INSURANCE AS A PRIVATE SECTOR REGULATOR AND PROMOTER OF SECURITY AND SAFETY: CASE STUDIES IN GOVERNING EMERGING TECHNOLOGICAL RISK FROM COMMERCIAL NUCLEAR POWER TO HEALTH CARE SECTOR CYBERSECURITY

By

John E. Gudgel

A Dissertation
Submitted to the
Graduate Faculty
of
George Mason University
In Partial Fulfillment of
The Requirements for the Degree
of
Doctor of Philosophy
Public Policy

Committee:

_____ Gregory D. Koblentz, Chair

_____ Laurie A. Schintler

_____ A. Trevor Thrall

Eric J. Novotny, External Reader

_____ John S. Earle Program Director

_____ Mark J. Rozell, Dean

Date: _____ Spring Semester 2022
George Mason University
Fairfax, VA

Insurance as a Private Sector Regulator and Promoter of Security and Safety: Case Studies in Governing Emerging Technological Risk From Commercial Nuclear Power to Health Care Sector Cybersecurity

A Dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at George Mason University

By

John E. Gudgel
Master of Science
George Mason University, 2009
Master of Science
University of Colorado, Boulder 1985
Bachelor of Science
Colorado School of Mines, 1980

Director: Gregory Koblentz, Professor
Schar School of Public Policy

Spring Semester 2022
George Mason University
Fairfax, VA

DEDICATION

This work is dedicated to my loving wife, Dorothy, my daughter Jackie, my future son-in-law Ellison, and my four dogs: Max, Molly, Woody, and Winston. Without their love and support, I would not have been able to get through this. I love you all!

ACKNOWLEDGEMENTS

I would like to thank my dissertation committee – Dr. Greg Koblentz, Dr. Laurie Schintler, and Dr. Trevor Thrall for their support and guidance throughout this long process. I would also like to thank my external reader, Dr. Eric Novotny for agreeing to review this work and providing me with really great and helpful comments. I also got indispensable support from Dr. Audrey Kurth Cronin who gave me the initial idea for this dissertation, and mentored me along the entire way. I also recognize and appreciate the help that other members of the faculty and staff of the Schar School gave me over the past ten years. Finally, I would like to thank my wife Dorothy for her incredible patience and support, especially during the dissertation writing process. I could not have finished this without all of your help. Thank you so much!

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

Literature Review Acronyms

APT Advanced Persistent Threat
CGL Commercial General Liability
CIA Confidentiality, Integrity, Availability
CISO Chief Information Security Officer
CNE Computer Network Exploitation
EP Exceedance Probability
FEMA Federal Emergency Management Agency
GAO General Accounting Office
GDPR General Data Protection Regulation
HIPAA Health Insurance Portability and Accountability
IDS Interdependent Security
ILS Insurance Linked Securities
ISO Insurance Service Office
IOT Internet of Things
MCP Managed Cybersecurity Providers
MPL Maximum Possible Loss
NAIC National Association of Insurance Comm.
NIST National Institute of Standards and Technology
NRC National Research Council
OPM Office of Personnel Management
PII Personally Identifiable Information
PCI Payment Card Industry
PRA Probabilistic Risk Assessment
P&C Property and Casualty
SME Small- and Medium-Sized Enterprises
TRIA Terrorism Risk Insurance Act
USCERT US Cybersecurity Emergency Response Team

Nuclear Industry Acronyms

ACRS Advisory Committee on Reactor Safeguards
AEC Atomic Energy Agency
AIC Atomic Insurance Committee
ALARA As Low as Reasonably Achievable
ANI American Nuclear Insurers
BWR Boiling Water Reactor
EBR-1 Experimental Breeder Reactor Unit 1
ENO Extraordinary Nuclear Occurrence
ERF Engineering Rating Factor
Gw Gigawatt
IAEA International Atomic Energy Agency
INPO Institute of Nuclear Power Operations
IPE Individual Plant Examinations
JCAE Joint Committee on Atomic Energy
Kw Kilowatt
LER Large Early Release
LOCA Loss of Coolant Accident
MAEP Mutual Atomic Energy Pool
MAELU Mutual Atomic Energy Liability Underwriters
MAERP Mutual Atomic Energy Reinsurance Pool
Mw Megawatt
NED Nuclear Engineering Department
NEIL Nuclear Electric Insurance Limited
NIRA Nuclear Industry Reinsurance Association
NIRB Nuclear Insurance Ratings Bureau
NML Nuclear Mutual Limited
NPP Nuclear Power Plant
NRC Nuclear Regulatory Commission
NSO Nuclear Service Organization (NEIL)
NWPA Nuclear Waste Policy Act
PRA Probabilistic Risk Assessment
PRDP Power Reactor Demonstration Program
PRDC Power Reactor Development Company
PRLR Power Reactor Liability Rating (ANI)
PWR Pressurized Water Reactor
SFP Secondary Financial Protection
SL-1 Stationary Low-Power Reactor
TMI-2 Three Mile Island Unit 2

Hazardous Waste Acronyms

AIG American International Group
APE Absolute Pollution Exclusion
ASTM American Society for Testing and Materials
BI/PD Bodily Injury and Property Damage
CAAA Clean Air Act Amendment of 1990
CCC Contractor Cleanup Cost
CGL Commercial General Liability
DHHS Department of Health & Human Service
DOJ Department of Justice
EDF Environmental Defense Fund
EIL Environmental Impairment Liability Insurance
EPA Environmental Protection Agency
ERA Environmental Risk Assessment
ERAS Environmental Risk Analysis Systems
ESA Environmental Site Assessment
FWQA Federal Water Quality Administration
GAO General Accounting Office
HRS Hazard Ranking System
IOS International Organization of Standards
ISO Insurance Service Office
LPL Lender Pollution Liability
NEPA National Environmental Policy Act of 1970
NPL National Priorities List
OPC Occidental Petroleum Corporation
OSHA Occupational Safety and Health Administration
OTA Office of Technology Assessment
P&C Property & Casualty
P&I Property & Indemnity
PCL Post-Closure Liability
PLI Pollution Liability Insurance
PLIA Pollution Liability Insurance Association
PRP Potentially Responsible Parties
PSM Process Safety Management
RCRA Resource Conservation & Recovery Act
RMP Risk Management Program
SARA Superfund Amendments and Reauthorization A
TSDF Treatment, Storage, and Disposal Facilities

Healthcare Cyber Acronyms

APT Advanced Persistent Threats
BA Business Associate
CAP Corrective Action Plan
CDS Clinical Decision Support
CIA Confidentiality, Integrity, and Availability
CMP Civil Monetary Payments
CMS Centers for Medicare & Medicaid Services
CPOE Computerized Physician Order Entry
CPRA California Privacy Rights Act
DCC Defense & Cost Containment
DHHS Department of Health and Human Services
DLS Dedicated Leak Site
DOJ Department of Justice
EHR Electronic Health Records
EH Eligible Hospitals
EP Eligible Practitioners
FDA Food & Drug Administration
GAO General Accounting Office
GDPR General Data Protection Regulation
HCAD Healthcare Cyber Attack Database
HIE Health Information Exchange
HSB Hartford Steam Boiler
IOC Indicators of Compromise
IOT Internet-of-Things
III Insurance Information Institute
MFA Multi-Factor Authentication
MGA Managing General Agent/
MGU Managing General Underwriter
NAIC National Association of Insurance Comm.
OCR Office of Civil Rights
PHI Private Health Information
PRC Privacy Rights Clearinghouse
PKG Packaged Policy
RaaS Ransomware-as-a-Service
RRG Risk Retention Group
SA Standalone Policy
SIR Self-Insured Retentions
SME Small- and Medium-sized Enterprise
SRA Security Risk Assessment
TDC The Doctors Company
TMC Tokio Marine Holdings
TTP Tactics, Techniques and Procedures
WHO World Health Organization

ABSTRACT

INSURANCE AS A PRIVATE SECTOR REGULATOR AND PROMOTER OF SECURITY AND SAFETY: CASE STUDIES IN GOVERNING EMERGING TECHNOLOGICAL RISK FROM COMMERCIAL NUCLEAR POWER TO HEALTH CARE SECTOR CYBERSECURITY

John E. Gudgel, Ph.D.

George Mason University, 2022

Dissertation Director: Dr. Gregory D. Koblentz

Insurance has been described as "a technology of governance beyond the state" (Ericson et al. p. 33). This dissertation will explore how both public and private insurance mechanisms can govern emerging technological risks by regulating and incentivizing private-sector security and safety behavior. Specifically, this study will seek to explain how insurance - an economic device for equitably transferring the risk of a loss, from one entity to another - can drive risk management and protection improvements at firms who acquire coverage. To answer this question, this study will use case studies to examine the role that insurance has played in managing and enhancing safety and security in three emerging technological risk regimes including commercial nuclear power, environmental pollution, and healthcare sector cybersecurity. It utilizes a mixed-methods multiple comparative case study approach to explore the key research question: "How can insurance promote better safety in emerging technological regimes?" Both qualitative and

quantitative evidence is presented including a new comprehensive database - the Healthcare Cyber Attacks Database (HCAD) - documenting over 5600 breaches against healthcare entities and sub-entities over the period 2005 to 2021. The key finding derived from this evidence supports the main hypothesis that “Insurance can improve the safety posture of firms engaged in emerging technologies.”

Chapter 1: Introduction

I. Introduction to the Problem

One of the challenges of our modern society is how best to proactively manage risks associated with emerging technologies. In this dissertation, "emerging technologies" are defined as scientific or technical innovations which are generally new, and are characterized by their novelty, relatively fast growth, prominent impact, and uncertainty regarding their future development and risks. Examples of contemporary emerging technologies include robotics, 3-D printing, autonomous vehicles, augmented reality, and artificial intelligence. What all of these technologies share is their connection to another older emerging technology, network computing or "cyber", which has been around since at least the 1970s, but continues to evolve and have its own inherent risks. Further, while all of these technologies have military and other public-sector applications, the vast majority are developed, manufactured and used by private-sector entities. Thus, managing emerging technological risk is primarily a private-sector responsibility.

Addressing specifically the issue of managing cyber risk, in its 2009 *Cybersecurity Policy Review*, the Obama Administration suggested that the private sector needed a compelling "business case" to incentivize it to invest in its own cybersecurity, and that would have spillover effects that could enhance the cybersecurity of other public and private entities (The White House 2009). Soon after, Vint Cerf, considered one of the

founders of the Internet, wrote that the term "cyber-safety" should be used when exploring the risks associated with network computing (Cerf 2011, p. 60), and went on to suggest that insurance might be one mechanism for managing private sector cyber safety (Cerf 2011, p. 67). This dissertation will explore the concept of managing emerging risk "safety," and the "compelling business case" for incentivizing private-sector safety behavior will be a solution that has existed for millennia, ***insurance***.

II. Background of the Study

Insurance has been described as "a technology of governance beyond the state" (Ericson et al. p. 33). Over thousands of years, insurance has been an effective business mechanism for managing emerging risks. Insurance often drives the development of safety standards and the dissemination of risk management best practices. It also acts as a private sector regulator that determines what activities are societally acceptable or "insurable" and what activities are not. In the past, many emerging technological risks, such as the development of commercial nuclear power, have been considered "uninsurable" due to the level of uncertainty regarding the magnitude and frequency of potential financial losses. However, over time, the insurance industry, in collaboration with other public and private entities and mechanisms, has managed to find a way to make "uninsurable" emerging technological risks "insurable."

A. The Insurance Framework

The literature review constructs an insurance framework for assessing, managing and insuring emerging technological risks. The key to insurability is having sufficient capital capacity to cover potentially catastrophic losses. Part of the insurance underwriting

process is to determine how best to spread the risk so as to minimize the impact on any single business unit, should a large loss occur. Insurers can spread the risk across their own portfolio, share the risk with other carriers, or find alternative financial instruments including reinsurance, risk pools, and insurance-linked securities. Under a worst case scenario, the government can intervene to provide backstop coverage for risks that the private-sector is unable to insure.

Under the insurance framework, insurers use the underwriting process to evaluate the risks associated with insuring a client and assess their eligibility for coverage. Underwriters gather client risk and exposure data, analyze the potential risks, determine what coverage (if any) will be offered, and the premium cost. Underwriters classify clients into appropriate risk classes composed of individuals and companies with similar risk characteristics. As part of the underwriting process, insurers assess and monitor customer behavior, rewarding good behavior with lower premiums, or penalizing bad behavior by charging higher premiums or denying coverage.

Through policy mechanisms including deductibles, copays, sub-limits and exclusions insurers can also require clients to retain a meaningful portion of the financial exposure and internalize some of the risk. They can also cancel coverage if a client violates the terms and conditions of the policy.

Insurers can also proactively manage firm risk behavior by educating them on best practices and encouraging them to participate in risk-reduction training by offering discounted premiums for course completion. Insurance also play a role in establishing safety standards for new emerging technologies. For example, insurance has played a

major role in the development of zoning regulations in flood areas, safety features in automobiles and fire protection in high-rise buildings.

Thus, through its ability to gather and analyze data, monitor and influence client behavior, encourage the development of safety standards, and in some cases enforce societal rules, insurance does play a significant role as a powerful private–sector regulator.

B. Other Mechanisms for Managing Emerging Technological Risk

This dissertation recognizes that there are many mechanisms other than insurance that can significantly influence the risk behavior of firms engaged in emerging technologies.

Federal and state regulations are one of the most obvious mechanisms. Regulations have the power of government behind them to force firms to adhere to safety standards primarily through licensing requirements, as well as civil or criminal penalties for violations. However, there are several problems with relying on regulations in managing emerging technological risk. First, government regulations often take years to develop, and likewise are hard to change once in place. For rapidly evolving technologies, this is extremely inefficient. Second, regulation typically results in an emphasis on meeting basic minimum standards, rather than striving to adopt and improve upon best practices. Third, regulations are primarily reactive and punitive rather than proactive and positive. Positive reinforcement is generally more effective at incentivizing good behavior because firms naturally prefer reward to punishment. Finally, regulations tend to be limited by

geographic jurisdiction. Thus for technological risks like cybersecurity that transcend national boundaries, safety issues may not be adequately addressed.

Another mechanism for managing the risks associated with emerging technologies is litigation. Entities that are harmed by a new technology can sue other entities for damages. The fear of litigation can be a major motivator for good safety behavior. However, like regulation, litigation can be lengthy, and often does not result in desired outcomes. Litigation is also costly, highly punitive, and can have geographic limitations as well.

Firms can also self-regulate and self-insure. Generally, well run companies know that it is not good business practice to harm customers, and subsequently make safety part of their business model. Such firms invest in safety measures and, in some cases, may set aside funds in "captives" to cover any risk-related losses. However, many firms involved in emerging technologies are start-ups with limited capital and, reasonably want to prioritize investment in development. Nearly all firms make cost-benefit analysis when deciding how to allocate limited capital funds. Firms also want to satisfy investors by maximizing profits. Thus, while well intentioned, most firms need external, unbiased third-parties including regulators and insurers, in order to optimize both performance and safety.

Interestingly, there is a synergistic relationship among regulation, litigation and insurance in helping to promote firm safety. Some regulations of emerging technological risks specify mandatory insurance as a condition of licensure. Compliance with regulations can be required by insurers as a term and condition of coverage, and non-

compliance can be evidence of negligence in litigation cases. Defense and settlements of litigation, and payment regulatory fines, are often a part of insurance coverage, and financial protection from these costs is a primary driver for entities to seek indemnity. This synergistic relationship will be discussed in later case studies.

III. Purpose of the Study

The purpose of this dissertation research is to examine over time the relationship between the primary variable ***safety*** and the primary independent variable ***insurance*** at firms engaged in business activities involving emerging technological risk.

As previously noted, insurance has been a tool for managing risk for thousands of years. It is an essential part of the global economy that has helped facilitate the diffusion of new technologies in many diverse fields including shipping, aviation, nuclear power, construction and genetic engineering. Arguably, without insurance, many projects would not get off the ground.

However, while there have been numerous theoretical papers written on insurance influence on private sector activities, there been few empirical studies demonstrating how insurance impacts firm behavior. The primary reason for this is that insurance is a private-sector business, and much of the data on insurers and their clients is proprietary. However, in the United States, insurance is a regulated business, and insurers that are "admitted" to do business in a state are required to file information on their products with state regulators, who in turn share this information with the National Association of Insurance Commissioners (NAIC). NAIC then posts this information through its public System for Electronic Rates & Forms Filing (SERFF) website. NAIC also collects data

from insurers on various types of insurance policies and claims that can be made available to researchers. For example, since 2016, NAIC has been collecting data on cyber insurance policies, and this data is used in this dissertation's healthcare cyber case study.

One limitation of the NAIC data is that it primarily covers recent activity submitted by regulated domestic carriers. Structured data prior to 2000, from foreign carriers, and from unregulated specialty insurers is largely unavailable. Thus NAIC has almost no insurance data on the two other regimes studied in this dissertation – commercial nuclear power and hazardous waste treatment. However, both of these regimes are regulated respectively by the Nuclear Regulatory Commission (NRC) and the Environmental Protection Agency (EPA), and all firms from both regimes are required to annually file proof of financial protection with their regulatory authority. Thus data on these regimes, while unstructured, is available for empirical analysis.

IV. Nature of the Study

The dissertation will be primarily exploratory in nature and utilize a mixed-methods multiple case study approach to explore the key research question and hypothesis. Specifically, it will explore the role public and private insurance mechanism played in helping clients manage the risk associated with three emerging technology regimes: 1) commercial nuclear power, 2) chemical and hazardous waste disposal, and 3) healthcare-sector cybersecurity. Each of these emerging risk regimes were not only influenced by private-sector insurance, but also liability concerns and public sector regulatory mechanisms that allowed for the technology's dissemination, while also managing

private-sector risk and public safety. The lessons learned from these case study experiences will then be applied to strategies for developing insurance coverage and other risk management mechanisms for future emerging technology regimes.

V. Research Question & Hypothesis

The goal of this research is to examine the relationship between safety and insurance at firms engaged in a number of emerging technological environments, over time. For the purpose of this study the dependent variable ***safety*** is defined as managing risks resulting in a reduction in either the frequency or magnitude of losses. The primary independent variable to be tested is ***insurance*** as defined by the number and type of policies taken up by firms engaged in the emerging technology, as well as a number of other insurance factors including insurer type, risk factors, annual premiums, coverage levels, deductibles, copays, and whether coverage is mandatory within that technological regime. Thus, the primary research question addressed by this research is:

RQ1: "How can insurance promote better safety in emerging technological regimes?"

The primary hypothesis to be tested is:

H1: "Insurance can improve the safety posture of firms engaged in emerging technologies"

To test this hypothesis, this research will examine insurance in three emerging technology regimes with a focus on issues such as:

1) What insurance policy mechanism (e.g., premium differentiation, coverage limits, etc.) are best at managing firm safety behavior?

2) How do insurance entities (e.g., shareholder owned, mutual, risk pools, reinsurers, etc.) interact and how can they best manage emerging technology risks?

3) What factors and conditions contributed to the development and adoption of insurance and can similar processes be used in the development of insurance for future technologies?

4) To what extent has insurance driven the definition of safety, the development of standards and adoption of safety measures in emerging technological regimes?

5) What other safety mechanisms, such as regulation and litigation, influence firm safety and how do they affect and interact with insurance safety activities?

VI. Data Analysis, Validity & Reliability

All three of these regimes share characteristics including a high degree of uncertainty, initial lack of actuarial data, potential for catastrophic losses, exclusion from Property & Liability (P&L) and Commercial General Liability (CGL) policies, and the belief that they were "uninsurable." There are also significant differences including the size of the populations, the nature of the risks, the availability of data, the involvement level of regulators, the degree of litigation, and the evolution of insurance coverage from initial availability to the present day.

Both similarities and differences allow for cross-case study comparison. To facilitate comparison, each case study is organized chronologically and in a similar manner, with guidance from the insurance framework and other elements of the literature review. Both qualitative and qualitative data was collected for each case study from multiple institutional sources including the NRC, EPA, Department of Health & Human Services (DHHS), and Congressional records sources including the HathiTrust Digital Library. All data is organized and stored using NVIVO and Excel spreadsheets. This use of multiple authoritative sources using replication logic and a standardized case study data gathering and storage protocol provides construct, internal and external validity to the research

design, as well as reliability that future researchers can replicate the findings and conclusions.

VII. Significance of the Study

This study is significant for several reasons. First, as previously noted, while there have been numerous theoretical papers written on insurance effects on private sector activities, there been few empirical studies demonstrating how insurance impacts firm behavior. Specifically, this dissertation uses both qualitative and quantitative data to empirically demonstrate the correlation between insurance and firm risk management and safety behavior.

Second, this dissertation also highlights the utility of insurance as a non-governmental regulator of private-sector behavior. In this era of partisan divide, having a non-governmental option for regulating firm behavior is important. Insurance is also a well-established mechanism for managing firm risk, and provides positive proactive incentives for firms to improve their safety capabilities.

Finally, for each case study, there are significant lessons learned that are highlighted at the end of each chapter. Significant findings relate to the importance of mandatory financial protection, the role of catastrophic events, the methods used to spread and internalize risk, and the interrelationship among insurance, regulation and litigation in optimizing safety. Most important, the risks in all three regimes evolved over time, requiring insurers to modify their coverage and adapt their underwriting practices.

VIII. Assumptions and Limitations

Assumptions and limitations exist based on the research design due to challenges in gathering and analyzing data in each of the studied regimes.

For the case study on commercial nuclear power, only U.S.-based commercial reactors were included in the population studied. Reactors outside of the U.S. and non-commercial reactors including research reactors owned and operated by governments, research institutions and universities were not considered even though some are covered by the insurance regime. The secrecy surrounding nuclear power and proprietary nature of commercial nuclear power was another limiting factor in gathering data. While data exists on insurance coverage for commercial nuclear power, much of the data is unstructured in insurance policies and other documents. The data record on both liability and property coverage is also far from complete, requiring interpolation or focus on specific reactors or operators, over a limited period of time.

For the case study on hazardous waste facilities, while there are over a million sites subject to RCRA and other environmental regulations, this dissertation research focuses on around 1800 larger sites designated by EPA as Treatment, Storage and Disposal Facilities (TSDFs). Like commercial nuclear power, data on insurance for hazardous waste disposal operations is also highly proprietary. While there are data from the EPA on environmental inspections, financial protection audits, and violations, there is only limited data linking insurance coverage to specific hazardous waste TSDFs. There is also limited data on the evolution of the environmental insurance regime from its near collapse in the late-1980s to its revival through specialized non-admitted carriers in the

2000s to the present day. Since specialty environmental insurance is primarily provided by non-admitted specialty carriers, NAIC does not have policy filings or other structure data covering this category of risk. Subsequently, the analysis relies on visual observations related to the structured EPA data, annotated with publicly available policies and other data from some specialty carriers made available through those carrier's public websites.

Arguably, the data used for the U.S. healthcare cyber study is the most complete and interpretable. It includes structured data from both the DHHS Office of Civil Rights (OCR) Breach Portal (https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf) covering the period 2009 to present, as well as structured data on insurance policies from NAIC covering the period 2016 to 2020. Structured data enabled the more rigorous use of quantitative analysis than in the first two case studies. However, these data also have limitations, and several assumptions were made in creating the quantitative models. The primary limitation is in the data from the OCR Breach Portal that only includes breaches of unprotected (unencrypted) data involving 500 or more records. Thus, breaches of encrypted data or those involving less than 500 records are not included. To compensate for this limitation, additional data was collected from state and other breach portals that often included such data, as well as a survey of media that cover healthcare breaches. This added an additional 1400 records to the Healthcare Cyber Attack Database (HCAD) – a new database used in the quantitative analyses.

Several assumptions were made in the healthcare quantitative analyses. First, the number of cyber policies allocated for each healthcare sub-entity (SUBCODE) is based

on the population of firms in that sub-entity derived from the 2018 U.S. Census Statistics of U.S. Businesses (SUSB 2018) and from insurance take-up rates from Marsh Analytics covering the period 2015 to 2020. The Marsh Analytics data has gained validity through its use in a 2021 U.S. General Accounting Office study on cyber insurance (GAO 2021). It is assumed in the regressions, that policy uptake for most healthcare entities is evenly distributed across healthcare sub-entities over the period 2015 to 2020, interpolated using the 2018 SUSB data. However, there were several exceptions made to this distribution. It was assumed, based on the literature that large healthcare entities with 500 or more employees had 100 percent insurance take-up. Also, it was assumed that federal facilities have no private insurance, and that a few sub-entities including medical equipment makers, state and local governments, suppliers, and medical schools fall into other non-healthcare SUSB classifications for population purposes.

Another assumption made in the regressions looking at the magnitude of cyber-attacks is that the primary measure of consequences is records compromised (AttRec). While this measure is the most widely reported, there are other measures of consequences including litigation settlements, ransom paid, property damage costs, and losses due to business interruption. While some of these tangible costs are captured in HCAD, they are not used in the quantitative analyses primarily because the record is only partial and often unavailable for many sub-entities.

IX. Organization of the Remainder of the Study

Following this Chapter 1 Introduction, the remainder of this dissertation is organized as follows. Chapter 2 is the Literature Review outlining four areas of concentration

including an overview of the insurance framework, descriptions of the primary characteristics of cybersecurity risk, the development of the U.S. cyber insurance market, and the political economy of cybersecurity and cyber insurance. Chapters 3 reviews the Methodology and Research Design that was used for this dissertation. Chapter 4, 5, and 6 are then the case studies developed to explore the role of insurance in promoting safety and managing risks for firms involved in three regimes: 1) commercial nuclear power, 2) hazardous waste disposal, and 3) healthcare cyber activities. Chapter 7 is the Conclusion including cross-case study analysis with policy recommendations and proposals for future research.

Chapter 2: Literature Review

This literature review consists of four areas of concentration. The first develops a theoretical framework based on insurance as a private sector regulator of emerging technological risk. The second defines the primary characteristics of cybersecurity risk and describes current cybersecurity risk management strategies. The third looks at the development of the U.S. cyber insurance market, the types of coverages offered, and the mechanisms that cyber insurers use to manage client cyber safety. The fourth area looks at the political economy of cybersecurity and cyber insurance, and provides additional theoretical background on how cyber insurance can help drive private sector cybersecurity investment and adoption of best practices.

I. Insurance, Insurability and Emerging Technological Risks (A Theoretical Framework)

This section discusses the nature of insurance and insurance risks. It also discusses the historical development of insurance and insurance products, and the role that the insurance industry plays in encouraging economic development, spurring technological innovation, and managing societal change. Theoretical concepts of insurability and potential public and private mechanisms for insuring seemingly uninsurable risks are outlined.

A. What is Insurance and Insurance Risk?

Insurance is an economic device for equitably transferring the risk of a loss, from one entity to another, in exchange for a premium (RANDmark40 2016). It is a form of risk management primarily used to hedge against the risk of loss associated with "uncertain events," reducing the uncertainty of the risk via pooling or other insurance mechanisms. Lloyd's of London notes that there "must be uncertainty as to whether the relevant event(s) may happen at all or, if they will occur (e.g., death) as to their timing" (Lloyds 2016). Conceptualized broadly, "risk" is "the potential for realization of an unwanted, negative consequence of an event" (Rowe 1977, p.24). A "loss" or "claim" is a realization of a risk. From an insurance perspective, there are various ways to categorize risks. They can be classified based on their causes – either natural or manmade. The former would include risks associated with natural phenomena such as hurricanes or earthquakes. The latter would include risks associated with infrastructure (e.g. bridges), industrial activity (e.g. refineries), or new technology (e.g. AI).

Tel-Aviv University risk management scholar Baruch Berliner in a 1985 paper developed a framework for analyzing the limits of insurability based on the relative size, frequency, distribution, and correlation of risks (Berliner 1977, pp. 313-329). In this paper, Berliner noted that the utility of insurance is that it allows individuals or small firms with very few large risks (such as a house or car) to transfer a portion of that risk to one or more professional risk carriers (e.g., insurance companies). The risk carrier can then spread risk across its portfolio or even split it with other carriers, making a large risk for a client into a smaller risk for the carrier(s).

Risks can also be classified based on their predictability and the potential impacts. Policy scholar Howard Kunreuther in a 2002 paper (Kunreuther 2002) , used probabilistic risk assessment (PRA) to evaluate a set of events that could produce a given dollar-value loss, determined the resulting probabilities of exceeding losses of different magnitudes, and then constructed Exceedance Probability (EP) curves (Figure 2.1) for each set of scenarios. Based on this analysis, he then developed a classification of risks based on the degree of ambiguity and uncertainty (Figure 2.2). Potential impacts can be further subdivided into tangible losses for which a monetary value is assigned and intangible losses, such as societal disruption or reputation, for which a specific economic cost cannot be assessed. For insurance coverage purposes, risks can also be classified as "first party" which directly affects the insured, and "third party" that influences other people or businesses, and that often result in third-party liability claims. Further, first or third party impacts can also have correlated effects that cascade downstream and disrupt seemingly independent systems.

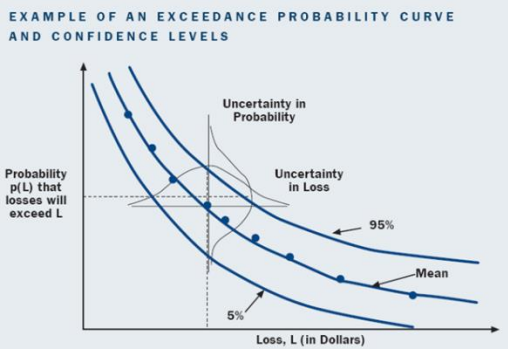


Figure 2.1: EP Curve (Kunreuther 2002)

CLASSIFICATION OF RISKS BY DEGREE OF AMBIGUITY AND UNCERTAINTY

Probability	Loss: Known	Loss: Uncertainty
Well-Specified	*Case 1* p, L Life, auto, fire	*Case 3* p, UL Playground accidents
Ambiguous	*Case 2* Ap, L Satellite	*Case 4* Ap, UL Earthquake, bioterrrorism

Figure 2.2: Classification of Risks (Kunreuther 2002)

B. The Insurance Industry – Role and History

In 2017, the global insurance market took in nearly $4.9 trillion in premiums equivalent to over 6% of global GDP, making it arguably the world's largest industry (IIIA 2019, p. 5). The U.S. insurance market represents 28.15% of total world premiums, with premium revenue of nearly $1.4 trillion or over 7.1% of U.S. GDP (IIIA 2019, p. 1). Further, these numbers do not include insurance industry profits from investment income or revenue from extra-insurance activities like reinsurance. Based on this economic prowess and its recognized expertise in managing risk, the insurance industry is in a strong position to influence private and public strategies regarding emerging threats.

Insurance plays a major role in a healthy economy. It enables money to become a means of communication within the economy by allowing problems to be expressed in terms of costs and time (SwissRE 2013, p. 11). It also allows businesses to separate operating capital from risk capital, freeing up funds to expand into new product lines and markets. The insurance sector has helped to facilitate the diffusion of new technologies in diverse fields including shipping, aviation, commercial nuclear power, construction and genetic engineering. Insurance can also help to define what technological and environmental changes are economically and socially acceptable. Insurance companies can, through the withholding of insurance coverage, compel developers of new technologies to apply a version of the "precautionary principle" that holds that every time there is individual or societal risk of harm that is not fully understood that exceptional precaution be taken before it is released (Dahlstrom et al. 2003, p.394). Thus while

insurance can spur development it can also encourage a more cautious approach. Without insurance, many projects would not get off the ground.

Insurance can also act as a private-sector regulator by determining what risks are acceptable (insurable) and what risks are not. Canadian scholar Richard Ericson describes insurance as "a technology of governance beyond the state" (Ericson et al. p. 33). London School of Economics Professor Bridget Hutter notes that insurance involves three aspects of regulation: 1) information gathering as part of risk surveillance, 2) behavior modification, and 3) third party enforcer such as fulfilling state requirements for all drivers to have automobile liability insurance (Hutter 2006, p. 5). As part of the underwriting process, insurers can assess and monitor customer behavior, rewarding good behavior with lower premiums, or penalizing bad behavior by charging higher premiums or denying coverage.

Insurance companies also play a role in establishing standards and educating clients on good business practices. For example, insurance has played a major role in the development of building codes in seismic locations, safety features in cars, and fire protection standards for houses and high-rise buildings. Insurance companies can also encourage client risk-reduction training, such as driver's education, by offering discounted premiums for course completion.

Many forms of insurance evolved out of the expansion of commerce and the development of new technologies. For example, during the late 1680s, Edward Lloyd opened a coffee house that soon became the meeting place for merchants wishing to insure cargoes and ships, eventually evolving into the Lloyd's of London marketplace for

marine and other specialty types of insurance (RANDMark40). Lloyd's of London wrote the first aviation insurance policy in 1911 and the first satellite insurance in 1965 (Crowley & Freeman 2016). The invention of the gasoline-powered automobile by Karl Benz in 1886 inevitably led to the first driver fatality from a collision in 1898 and, subsequently, the issuance of the first automobile liability insurance policy that same year (Onge 2008). In 1927, Massachusetts became the first U.S. state to have mandatory car liability insurance and today it is required in all U.S. states (IIIA 2019, pp. 92-93).

Finally, many insurance products were developed as a result of catastrophic events, concerns about insurability, and the impact of natural and manmade disasters. The 1906 San Francisco earthquake may have had the most profound effect on the U.S. insurance market. The earthquake and subsequent fire caused hundreds of millions of dollars in damaged – losses which threatened the solvency of many U.S. insurance companies (SwissRE 2013, p. 27). The correlated nature of the damage caused considerable confusion over whether losses were covered under fire insurance or excluded as damaged caused by an uninsured force majeure. The extent of the damage made insurers rethink the potential size of losses and highlighted the significant need for additional sources of capital to cover losses for future catastrophic events. The limits of insurability have been tested on many occasions and, in response, the insurance industry, private companies and governments have developed various mechanisms to absorb the financial shock.

C. Insurability and Emerging Risk

Insurance companies provide financial indemnity for losses arising from a specific set of causes, and there are insurability criteria that they use to determine the magnitude

of potential losses that can be transferred and the types of risks that can be insured. There are actuarial criteria including the estimated probability, frequency and independence of loss occurrence; and the average and maximum total loss likely associated with an event. There are also market-driven criteria including the level of premium required, the amount and duration of coverage, and the capacity of the insurance company to absorb the potential loss. Insurance is a business decision that involves assuring that the insurance company makes a profit while not assuming unacceptable risk that can cause insolvency. There are also other non-actuarial criteria including avoiding too high-risk clients (adverse selection) or clients able to manipulate the risk (moral hazard). Finally, political or legal concerns can influence insurability decisions.

Insurers use the process of underwriting to evaluate the risks associated with insuring a client and assessing their eligibility for coverage. Underwriters gather client risk and exposure data, analyze the potential risks, determine what coverage (if any) will be offered, and the premium cost. Underwriters classify clients into appropriate risk classes composed of individuals and companies with similar risk characteristics. The purpose of underwriting is to protect the insurance company from adverse selection of high-risk clients by identifying any moral hazard that might cause them to provide coverage at an unacceptable level or price. The underwriting process also works to determine the right mix of risks to add to a company's portfolio including assessing whether the risks are sufficiently independent so that the company cannot be hit too hard by a single loss event or by a cascading catastrophic loss. Thus, using underwriting, insurance companies pool

together a large number of acceptable independent risks, spread across a diversified portfolio, with minimal likelihood of a large number of correlated or costly claims.

Over time, insurance for new types of risks typically go through three phases of development (Young et al. 2016). During the first nascent phase, there is virtually no data on the risk, and insurers use their normative judgement to determine premium rates. To limit their exposure, insurers charge inordinately high premiums for a limited amount of coverage. There is no standard underwriting procedure or policy language. During the second phase, the insurer has paid numerous claims against policies and has gained some insight into actual losses (actual experience). Premiums are determined using both historical quantitative data and normative behavior assessments. The risks become more predictable, premiums level off, and underwriting procedures and policy language becomes more standardized. During the final phase, costs associated with the risk are well understood, and insurers rely on actuarial tables to determine premiums, risk categories, and coverage levels.

One way to measure emerging insurance market maturity is through measures of insurance industry profitability such as the loss ratio. The loss ratio measures the total incurred losses in relation to the total collected insurance premiums. In a nascent market, emerging risk insurance can be highly profitable because of high premiums, but the loss ratios can vary widely as some insurers experience unexpected losses. As the market matures, average loss ratios typically edge up as insurers gain a better understanding of the risk and are able to provide more competitive premiums. Loss ratios less than 70% are considered acceptable, with average loss ratios falling into the range of 40 to 60%.

During the final maturity phase, the loss ratios edge even higher as the risks become well understood and insurers are able to balance fair premiums vs. known costs.

One type of risk that is of particular concern to insurance companies is associated with emerging catastrophic (or systemic) events. Emerging catastrophic risks are characterized by their high level of unpredictability, potential for large-scale correlated losses, increasing occurrence, and lack of historical precedents (actuarial data) to determine reliable risk estimates (Castellano 2010, p. 395). London School of Economics Professor Giuliano Castellano believed that the increase frequency and impact of such large-scale disasters was directly attributable to the "growing interconnections between people, markets and networks together with the development of new technologies" (Castellano 2010, p. 391). An emerging catastrophic risk can be a single very large crisis that, by its sheer magnitude, impacts all or most entities in a system; or it can be an event of any size that sets in motion a cascade of correlated negative consequences that ultimately affects most or all of a system (Kaufman & Scott 2003, p. 371). A good example of a recent large-scale catastrophic crisis with cascading effects is the 9/11 terrorist attacks that not only destroyed the World Trade Center but also unsettled the world economy through disruption of airline travel, tourism, etc. However, catastrophic risks do not have to be sudden but rather can evolve slowly over time. Examples of these "creeping" catastrophic risks include global climate change and environmental pollution (e.g. Love Canal).

Based on these criteria, most emerging catastrophic risks are considered "uninsurable" by most insurance companies. Many insurability factors including

randomness, acceptable maximum possible loss, absence of client moral hazard, and availability of actuarial data are not satisfied as a result of the risk's size and uncertainty (Berliner 1985, p. 329). For this reason, insurers exclude such risks from their property and casualty (P&C), and comprehensive general liability (CGL) policies. This would include low frequency/high impact risks such as those associated with nuclear power and terrorism (Figure 2.3). However, through the implementation of various insurance industry products, insurance-like mechanisms, financial instruments, and government policies, such "uninsurable" risks have become more or less "insurable."

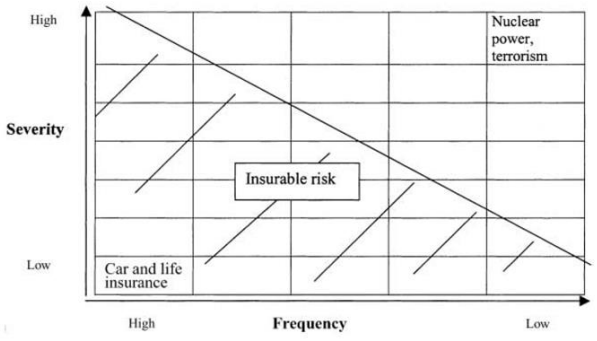


Figure 1: Insurability of risk

Figure 2.3: Insurability of Risk Based on Event Severity and Frequency (Dahlstrom et al. 2003)

Legal scholar Christian Lahnstein in a 2004 paper stated that "insurability criteria usually specified for private insurance are questionable, and can be refuted at once with facts…all too many insured risks can be regarded as non-random on the one hand, or not estimable on the other" (Lahnstein 2004, p.515). Lahnstein goes on to note that monetary limits define the boundaries of insurability and that emerging risks such as terrorism are insurable, but only within the scope of limited capital capacities (Lahnstein 2004, p. 516). Thus, capital capacity is a key element of how much emerging risks can be insured.

Insurers that have more capital capacity are able to insure more risks and absorb more shock if a catastrophic loss occurs. Capital capacity can come from internal net assets or from external sources of capital including financial markets. Most individual insurers do not have sufficient internal assets to cover large catastrophic losses. Thus, they need to consider alternative capital sources to assure that they have sufficient funds to cover losses from catastrophic events (Kleindorfer & Kunreuther 1999, pp. 178-179).

One of the most common mechanisms for expanding the capital capacity of insurance companies is reinsurance. First developed during the late-19th century, reinsurance is basically "insurance for insurance companies" where the insurer or "cedent" pays the reinsurer a premium in order to transfer or "cede" some of the risk. This allows the ceding insurance company to offer higher protection to policyholders in excess of what would be their normal solvency limits. The reinsurer in turn is able to pool different risks from numerous insurance companies and spread the risk as widely as possible across multiple business lines and alternative financial instruments.

Like insurance companies, a reinsurance company's ability to absorb capital losses is not unlimited and is set by the amount of internal and external capital available. Many reinsurance policies are "excess loss arrangements" where the reinsurer provides a set amount of coverage (e.g., $100 million) when an insurer's losses exceed a set amount (e.g. $300 million). These arrangements provide the insurer with an additional layer of protection while capping the reinsurer's maximum possible loss. However, reinsurers can experience solvency problems when an event affects multiple covered insurance

company clients or when a series of events results in multiple separate claims. Reinsurers faced both of these scenarios in the 9/11 attacks.

In order to expand their capital capacity and protect themselves from catastrophic losses, reinsurers also pursue alternative financial tools including "retrocession" (reinsurance for reinsurers) and "sidecar reinsurance" where a limited liability company takes a share of the risk in exchange for a share in the profit or loss of the insurance activity (Castellano 2010, pp. 400-401). Another alterative financial mechanism is insurance-linked securities (ILS) including catastrophe bonds (CAT-Bonds) that allow reinsurers to transfer some of the risk to capital investment markets in return for higher than average bond yield returns. Reinsurers also transfer high-end risks to hedge and pension funds (Radetzki & Radetzki 2000, p. 188).

Private companies can also act on their own behalf to protect themselves from catastrophic risks. Many Fortune 500 companies have formed offshore "captives," a form of self-insurance where companies set aside "rainy-day" funds typically in tax havens, such as Bermuda or the Cayman Islands to help pay for catastrophic liabilities should they occur. Many companies in the same industry have also bonded together and formed wholly owned joint liability or risk sharing mutual pools where all operators contribute and help to cover catastrophic losses when they occur. Examples of such "indemnity clubs" include the American Nuclear Insurers (ANI) and Nuclear Electric Insurance Limited (NEIL) pools formed following the 3-Mile Island incident, and the Pollution Liability Insurance Association (PLIA) formed by over 40 chemical companies in the mid-1980s in the wake of Love Canal. The advantage of such pools is that there are no

annual premiums since contributions are only required if an incident occurs. Participants from the same sector share similar risks and often have expert knowledge about those risks compared with insurers or other market actors who do not belong to that sector (Faure & Fiore 2008, p. 302). Participants also readily share information on specific risks since all are equally liable if an incident occurs. Thus, all pool participants have collective economic responsibility for safety and real economic incentives to prevent accidents in order to minimize their individual costs.

Finally, governments can make capital available to cover catastrophic losses. They can provide coverage "ex ante" as the insurer or reinsurer of last resort, or "ex poste" where they provide relief to victims of catastrophes through direct compensation or low cost recovery loans. As the ex-ante primary "insurer of last resort," governments provide temporary or permanent coverage during times of market failure when private insurers are unwilling or unable to provide indemnity. Examples of government provided indemnity include the ***National Flood Insurance Program (NFIP)*** established by Congress in 1968, and the ***California Earthquake Authority (CEA)*** formed in 1996 following the Northridge earthquake. Governments can also be the ex-ante reinsurer of last resort. Under this scenario, insurance companies are typically required to provide some level of coverage for specific catastrophic events and pay the government a premium for catastrophic coverage exceeding a set amount. Thus, government reinsurance replaces private sector reinsurance for a specific type of risk. Examples of government reinsurance programs include coverage under the ***Terrorism Risk Insurance Act (TRIA) of 2002***, and the mandatory second-tier of indemnity coverage provided by

the U.S. government to commercial nuclear power plant operators authorized by the ***Price-Anderson Act of 1957***.

There are both positive and negative aspects of ex ante government insurance intervention. On the positive side, the availability of government insurance and reinsurance helps to resolve, at least temporarily, the "uninsurability problem" – the unwillingness of insurance markets to provide catastrophic coverage (Faure & Fiore 2008, p. 375). The availability of government catastrophic coverage allows technological and economic development that might otherwise be stifled by the lack of private sector coverage. Government ex ante coverage can also help to stabilize insurance markets following major disruptions, such as occurred immediately following 9/11. This can allow private insurance and reinsurance markets time to gather data, reassess risk, and establish appropriate coverage levels and premiums.

However, while ex ante government intervention can help alleviate the uninsurability problem, it can also lead to negative consequences. In some instances, government insurance competes with private sector insurance. If the premium is subsidized, it can create an unfair market advantage to the public sector product. This can "crowd out" private sector insurers from entering the market, especially if the government premium is well below the market value associated with the risk (Jaffee & Russell 2005, p. 4). Government dominance can also eliminate the market incentives of private insurers and reinsurers to develop additional capacity, or to invest in new capabilities (Brown et al. 2002, p. 8).

One way to generate sufficient capital needed to deal with emerging catastrophic risk and with the issues associated with government intervention is to combine both public and private insurance mechanisms into an overall multilayered solution. As discussed in Chapter 4 and 5 such an approach was used in managing commercial nuclear power indemnity risks in the 1950s, and controlling environmental pollution liabilities in the 1980s.

II. Cyber Risk Management

This section analyzes the components of cyber risk and the role that risk management strategies, including risk transference, play in promoting cyber safety at US firms.

A. The Nature of Cyberspace

Cyberspace is complex and enigmatic. It has been described as a "rich chaotic realm" (Cronin 2013, p. 29) and "a complex man-made environment…(where) human adversaries are purposeful and intelligent" (Nye 2011, p.20). One element of cyberspace, the Internet, has been portrayed by Google's Eric Schmidt as "the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had" (Schmidt 2010).

Uncertainty is a key characteristic of cyberspace. It is often difficult to determine if a system failure was caused by bad software, human operator error, accident, mechanical malfunction, or deliberate cyber action. Martin Libicki referred to this characteristic as "non-obviousness" (Libicki 2012, p.89) – the ambiguity that can cause confusion, hesitancy and, sometimes, inappropriate response to a perceived cyberattack. Further, the

extent of harm attributed to a cyber event may remain forever uncertain to both the target and the attacker. A 2009 National Research Council (NRC) report concluded that due to the complexity of cyber-attacks, "outcomes are highly uncertain" and therefore "cannot be reliably predicted" (Owens et al. 2009, p.20). Cyber-attacks often go undetected for long periods as demonstrated by the cyber intrusions on the Office of Personnel Management (OPM) systems in June 2015.

Cyber-attacks are also characterized by their speed, stealth, and seeming ability to transcend national borders. They can be launched from anywhere in the world at any time – at the push of a button, or under predetermined conditions on specific dates in the future. Oftentimes, the target does not know they have been hit until long after the hack has occurred. Likewise, even if an attack is detected, the hackers can hide their identity through "spoofing" their IP address or by obscuring the true origin of an attack by hopping through a series of compromised computers to reach their target (Geers 2010, p. 301). The attacker can also "false flag" the attack, placing the blame on an innocent third party. Through this anonymity, cyber-attacks are conducted with plausible deniability by both the attacker and the state in which they operate (Owens et al. 2009, p. 20). For this reason, cyberspace is often characterized as having no national borders determining legal jurisdiction (Krepinevich 2012, p.45).

Another characteristic of cyberspace is the low barriers to entry. The technology required is widely available, inexpensive, and easy to obtain, allowing cyber-attacks to be initiated by any person or organization that has access to a computer, network connectivity, and some basic computer skills. These low barriers to entry mean that

individuals and small groups can inflict significant damage with asymmetric impacts on larger well-connected states and organizations.

Jason Healey in reviewing the history of cyberattacks noted that cyber incidents tend to fall into two categories – "either widespread but fleeting, or persistent but narrowly focused" (Healey 2013, 14). University of North Carolina scholar Nir B. Kshetri in developing a cyber conceptual framework classified cyberattacks as either "targeted" or "opportunistic" and noted that "Whereas minimal skill is needed for opportunistic attacks, targeted attacks require more sophisticated skills" (Kshetri 2005, p.541).

Finally, another important cyberspace characteristic is its rapid and accelerating evolution, both in size and complexity. As of July 2020, there were an estimated 4.66 billion active Internet users worldwide encompassing nearly 60 percent of the global population up from around 3 billion users in 2015. This rapid growth is being fueled by the rapid diffusion of mobile technology and access to social media. In addition, by the end of 2021, there were nearly 13 billion Internet-connected "things" including consumer intelligent personal assistants, smart medical devices, industrial sensors, and military drones – and this number is expected to grow to more than 27 billion Internet of Things (IOT) devices by 2025 (Sinha 2021). This treasure trove of valuable data, as well as the many new ultramodern devices, networks, and storage technologies represent novel vulnerabilities that new sophisticated threat actors can exploit using state-of-the-art tools and techniques. These intelligent adversaries can also quickly adapt their TTPs to thwart innovative technological security defenses erected to detect, protect and respond to their malicious cyber activities.

B. Cybersecurity Vulnerabilities

Cyber-attacks are implemented by exploiting vulnerabilities in the target's endpoint devices, computer systems, networks, human-related activities, and cyber defenses. Per Richard Danzig: "The beginning of wisdom about cyber systems is to understand that vulnerability is inherent in the technology" (Danzig 2014, p. 9). These vulnerabilities arise from a variety of causes. A 2014 NRC report noted that vulnerabilities can be introduced in software code by accident ("a bug"), intentionally by design (e.g. "a backdoor") or by a configuration error in the target system (Clark et al. 2014, p.45). Cyber attackers often exploit "zero-day" flaws that are unknown or software vulnerabilities that have not been "patched" by program manufacturers. The interaction of code with other programs increases the overall number of possible flaws and a system's overall vulnerability. The combination of errors allows hackers to gain unauthorized access to systems.

There are also other types of vulnerabilities that cyber attackers exploit. Richard Clarke and Robert Knake identified five major vulnerabilities in the Internet that enables cyber-attacks including its addressing system, routing protocols, minimal use of encryption, interconnectedness that allows rapid malware spread, and its decentralized design focused on openness, not security (Clarke & Knake 2010, pp. 73-85). They also point out the increasing interconnection and vulnerability of US critical infrastructure, much of which is owned and operated by the private sector (Clarke & Knake 2010, p. 145). This problem was first highlighted by the President's Commission on Critical Infrastructure Protection or "Marsh Commission" in 1997 which concluded that the

interlinkage of critical infrastructures had created "a new dimension of vulnerability, which…poses an unprecedented national risk" (PCCIP 1997, p. ix).

Another source of vulnerabilities is the global supply chain. Per the DOD in 2011: "Most information technology products used in the US are manufactured and assembled overseas. The reliance of DoD on foreign manufacturing and development creates challenges in managing risk at points of design, manufacture, service, distribution, and disposal" (DOD 2011, p. 3). Vulnerabilities in foreign components can then enable cyber penetration of the host system.

Finally, there are human vulnerabilities where people either unwittingly or deliberately expose a system to attack. Human mistakes are arguably the greatest vulnerability – a 2014 IBM study found that 95 percent of cyber incidents investigated recognized "human error" as a contributing factor (IBM 2014, p 3). Human errors include system misconfiguration, use of easy-to-guess passwords, lost laptops, and disclosure of information via email or "double clicking" an unsafe URL. Oftentimes threat actors will use social engineering techniques such as phishing to trick human targets into revealing IDs, passwords and other system access information.

Thus, vulnerabilities are pervasive throughout software and hardware components, exposed by human weaknesses, and spread through the interconnectedness of cyberspace. They provide attackers with the opportunity to gain unauthorized access to systems and to implement a "threat" that can adversely affect individual, organizational, national, and international security.

C. Cybersecurity Threats

"Cyber threat" is a term repeatedly used in policy statements and literature that can be confusing. It is often used interchangeably with cyber vulnerability without clear understanding of the difference. Peter Singer gave an example of a vulnerability being when you leave your house unlocked, where a threat is when someone decides to enter the house to steal property, cause damage, or attack an occupant. He states that the "defining aspects of threats are the actor and the consequence" (Singer & Friedman, p. 37). Per the 1997 Marsh Commission Report, "A threat is traditionally defined as a capability linked to hostile intent" (PCCIP 1997, p.14).

Cyberspace's low barriers to entry empower many state and non-state threat actors to exploit an even greater number of public and private targets. Further, there are many different types of threat actors, and they have a variety of motives for their attacks. *Cyber criminals* are individuals or organizations who engage in cyber-attacks for monetary gain. *Cyber spies* use computer network exploitation (CNE) to hack and steal proprietary or classified information to gain a competitive, political or military advantage. Finally, there are the nation-state *cyber warriors* and the non-state *cyber terrorists* who undertake cyber-attacks in support of their strategic objectives.

Three fundamental principles of information security are confidentiality, integrity, and availability (CIA). Cyber threats maliciously compromise one or more of these principles and one way to classify cyber-attacks is by determining which of these three principles is threatened. *Confidentiality* is a set of rules that restricts access to secret or private data to only authorized users. If a system suffers a loss of confidentiality, then

data has been disclosed to unauthorized individuals. *Integrity* is the assurance that data is trustworthy, accurate, and consistent throughout its entire life cycle. Loss of integrity means that an unauthorized entity has modified or destroyed data or programming code. *Availability* is the guarantee that data and systems are accessible by authorized users when needed. Denying access is a common form of cyberattack.

Of particular concern to the US government, military, and large corporations are *advanced persistent threats* (APTs) – coordinated teams of specialized experts that have the resources to escalate and maintain a cyber operation against a specific target. The 2014 NRC report characterized APTs as "technologically sophisticated (i.e., advanced), hard to find and eliminate (i.e., persistent)" and "highly focused on a particularly valuable target," in contrast to other threats that seek targets of opportunity (Clarke et al. 2014, p. 50). Due to the "advanced" nature of these attacks, most APTs are associated with states especially China, Russia, and the US, or large cybercrime gangs such the Russian Business Network. Their "persistence" often allows these groups to extract large amounts of data over long periods without detection. Many APTs are profiled by their tactics, their target selection, and overall mode of operation including preferred hacking tools and code, and sequence of commands used in implementing their attacks.

Another threat of particular concern to US policymakers is possible cyber-attacks on critical infrastructure. Protection of critical infrastructure was the focus of the 1997 Marsh Commission report which found "Our infrastructures are exposed to new vulnerabilities— cyber vulnerabilities—and new threats—cyber threats" (PCCIP 1997, p. vii) and concluded that the "threat of infrastructure attacks therefore has the potential for

strategic damage to the United States" (PCCIP 1997, p.24). The Marsh Commission then conclude that, because the infrastructures are mainly privately owned and operated, "critical infrastructure assurance is a shared responsibility of the public and private sectors," (PCCIP 1997, p. xi).

In February 2013, citing unspecified "repeated cyber intrusions into critical infrastructure" the White House issued ***Executive Order 13636*** **(EO 13636)** ***Improving Critical Infrastructure Cybersecurity*** that ordered the National Institute of Standards and Technology (NIST) to develop a framework to reduce cyber risks to critical infrastructure (The White House 2013). In response, NIST in February 2014 issued its *Framework for Improving Critical Infrastructure Cybersecurity* (NIST 2014) that outlined a risk management approach to cybersecurity.

D. Cyber Risk and NIST Risk Management Framework

The US Cybersecurity Emergency Response Team (USCERT) defines risk as "The potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences" (US-CERT 2015). It is often expressed by the risk equation:

Risks = Vulnerabilities x Threats x Likelihood x Impact or R = f(V, T, L, I)

Thus in order to truly understand cyber risk you need to understand cyber vulnerabilities, cyber threats, the likelihood of a cyber event occurring, and the level of harm that would be inflicted. Given these factors' uncertainty, the ability to determine cyber risk is even more challenging. Deirdre Mulligan and Fred Schneider in their paper "Doctrine for

Cybersecurity" noted, "lack of information about vulnerabilities, incidents, and attendant losses makes actual risk calculations difficult." Further, regarding losses they observe, "Companies and individuals do not know how to value (i) confidentiality of information, (ii) integrity of information, or (iii) the pain of dealing with recovery from an attack's effects" (Mulligan and Schneider 2011, p.73).

Further complicating the risk calculation is the interdependencies that exist among different types of cyber systems and critical infrastructure that can increase the possibility that rather minor disturbances can cascade into much more substantial cross sector failures. Jason Healey in a 2014 paper believes in the expansion of the risk management horizon beyond individual organizations to include what he calls the "seven aggregates of cyber risk" including "counterparties and affiliates, supply chain and outsourcing agreements, upstream infrastructure, external shocks and other risks" (Healey 2014, p. 2).

One method for organizations to deal with risk challenges is to implement a risk management strategy that includes processes to inform and prioritize decisions regarding cybersecurity, and reduce expected losses from cyber-attacks. Mulligan and Schneider note that "absolute cybersecurity is cost prohibitive" and by adopting a risk management strategy firms "admit that all vulnerabilities are not equal, that one should focus only on vulnerabilities whose exploitation (i) is sufficiently likely to occur based on perceived threats and (ii) could enable expensive (by some cost measure) system compromises" (Mulligan and Schneider 2011, p. 73).

In February 2014, NIST released the first version of its Framework for Improving Critical Infrastructure Cybersecurity that provided a "prioritized, flexible, repeatable,

performance-based, and cost-effective approach" for managing critical infrastructure cybersecurity risk (NIST 2014, p. 3). Per the NIST Framework, organizations can manage risk in different ways, including accepting, avoiding, mitigating, or transferring the risk (NIST 2014, p. 5).

In some instances, organizations may accept cyber risk deemed to be low or moderate, depending on particular situations or conditions. Thus, risk acceptance may be an appropriate risk response when an identified risk is within the organization's risk tolerances. Avoiding risk involves identifying potential vulnerabilities and threats, and implementing appropriate cyber-attack prevention measures such as the firewalls and anti-virus software; or choosing to limit participation by enacting strong access controls or air gapping their systems.

Mitigation is another strategy for dealing with cyber risks. Mitigation is defined as "the act of making a condition or consequence less severe" or "lessening the force or intensity of something unpleasant" (Dictionary.com 2016). Thus, it should be used in situations where a risk or hazard cannot be avoided. It can include "damage control" or allowing a system to "fail gracefully." FEMA defines mitigation as "effort to reduce loss of life and property by lessening the impact of disasters" but then expands the definition with "Mitigation is taking action now—before the next disaster—to reduce human and financial consequences later" (FEMA 2016). Thus, per FEMA's definition, mitigation includes risk analysis, preparedness and planning.

A final NIST Framework strategy is to transfer the risk. Risk transfer typically takes place when a firm wants to liability and responsibility to other firms, often by paying a

premium to insurers in exchange for protection against a financial loss. Risk transference reduces neither the impact nor the likelihood of harmful cyber events occurrence. However, companies willing to insure cyber risk can require firms to go through a risk assessment and implement best practices in return for preferred pricing. Thus, risk transfer can positively influence cybersecurity behavior provided it makes "business sense" from the perspective of both the insurer and the insured.

III. Cyber Insurance

This section provides information on the U.S. cyber insurance market including historical development, economic drivers, current market and coverages provided. It then provides details on how cyber insurance processes including audits and risk assessments, underwriting, risk categorization, premium differentiation, and policy mechanism help to manage client cyber safety. This information, along with that in the previous section (Cyber Risk Management) will be referenced extensively in the healthcare cyber insurance case study (Chapter 6).

A. Cyber Insurance Background & Breach Cost Drivers

Cyber insurance has been defined as "the transfer of financial risk associated with network and computer incidents to a third party, the insurance company, in exchange for a premium" (Toregas & Zhan 2014, p.6). Coverage for cyber-related casualty and liability events is not new. Cyber-specific insurance coverage has been available in the US for over 30 years. The first insurance products for cyber loss appeared in the 1980s as specialty coverage for IT errors and omission liability (CyRiM 2019, p. 35). During the 1990s, as the Internet evolved and more firms did business online, cyber-crime also

flourished. In response, the International Computer Security Association offered the first cyber-attack "warrantee" as part of its TruSecure security certification service (PropertyandCasualty.com 1998). Soon after, several insurance companies partnered with technology companies (e.g., Marsh/AT&T), and began to offer "hacker insurance policies" covering first-party losses and offering security solutions as part of a total risk management solution (Majuca 2005). Then, in 2000, American International Group (AIG) began offering its NetAdvantage suite of cyber insurance products covering both first- and third-party losses up to a limit of $25 million (PropertyandCasualty.com 2000).

As businesses increasingly depended on electronic data and computer networks to conduct their daily operations, the number and severity of data breaches increased, and the type and sophistication of cyber-attacks evolved. In November 2020, Cybersecurity Ventures estimated that the global cost of cybercrime in 2021 would be US$6 trillion, up from US$3 trillion in 2015, and rising to US$10.5 trillion in 2025 (Morgan 2020). Further, the Ponemon Institute in collaboration with IBM Security has estimated that the average total cost of a cyber breach in 2020 globally was US$3.86 million with the United States having the highest national average total cost at US$8.64 million (Ponemon/IBM 2020, p. 23). The average total cost of a data breach can vary considerably from industry to industry based on a number of factors.

First, the degree of cyber regulation experienced by an industry can have a major impact on breach costs. In particular, firms in the healthcare, energy, and financial industries are subject to federal (e.g., HIPAA) and state (e.g., COPA) laws requiring adherence to strict risk management and breach reporting regulations, with breaches

sometimes resulting in long costly investigations and hefty fines. Second, the number and sensitivity of records involved in a breach can play a major role in total breach recovery costs. Large breaches involving sensitive records such as personal identifiable information and financial data can result in expensive class action litigation and settlements requiring costly credit monitoring and victim monetary restitution.

Another factor impacting the cost of a data breach is the size and cyber maturity of the breached firm. While large firms potentially have more records at risk, small and medium enterprises (SMEs) typically lack the technical staff and expertise to prevent and mitigate cyber-attacks. As a result, cyber breaches can go undetected and uncontained for long periods of time, significantly increasing the damage, sometimes with existential consequences for the small firm involved. Finally, the cost of cyber breach oftentimes depends on the type of attack and whether it is targeted at a specific firm or untargeted, affecting many companies in a similar manner. Untargeted attacks tend to be more universally disruptive, and are usually quickly resolved once detected. Conversely, targeted attacks often are more sophisticated, targeting specific assets, and taking longer and more money to resolve. For example, ransomware attacks involving the theft and/or encryption of critical data, in some cases requiring two separate ransom payments – one to return the data and another to provide the decryption key. As a result, the cost of ransomware attacks tends to be 2.5 times more expensive than other types of cyber-attacks (Coalition 2020, p. 8). This has created a demand for cyber insurance in order to transfer some of that risk.

B. Cyber Insurance Demand (U.S. Firms)

In 2020, global insurance broker Marsh reported that 47% of its US-based clients purchased cyber coverage, more than double the number of companies that purchased coverage in 2015 (GAO 2021, p. 1). This growing demand for cyber insurance is driven by increasing concerns about cyber risks. According to a 2019 survey conducted by Marsh and Microsoft, 79% of firms ranked cyber risk as a top-five risk concern up from 62% in 2017 (Marsh & Microsoft 2019).

This demand is also driven by a number of cyber risk factors including company size, the amount and sensitivity of data collected, its dependency on network systems for daily operations, and the extent the firm is subject to regulation. Firms that collect and store financial data such as credit card numbers, and personally identifiable information (PII) such as Social Security numbers and birth dates, have higher risks for cyber-attack, and are more likely to purchase cyber insurance. Many of these same companies make extensive use of networking technology in their business, and may also be subject to strict breach reporting and data protection regulations including HIPAA, GDPR, and the Payment Card Industry Data Security Standards (PCI-DSS). Thus in 2020, firms in the education (79%), hospitality (73%), and healthcare (67%) sectors have cyber insurance take-up rates much higher than the all-industry average (47%) (GAO 2021).

Major cyber events and new types of cyber-attacks have spurred increased demand for cyber insurance. For example, the 2020 COVID-19 pandemic has resulted in a surge in ransomware attacks, especially targeted at healthcare and educational facilities. This,

in turn, has created a wave in demand for extortion payment and data restoration cost coverage.

Companies in the same industrial sector often face similar cyber risks, from many of the same types of threat actors, and are therefore potentially exposed to comparable cyber losses. For example, firms involve in scientific research may be more susceptible to state sponsored hacking, data exfiltration, and the theft of trade secrets or intellectual property. This is illustrated by a North Korea-sponsored attempt to steal Covid-19 vaccine secrets from pharmaceutical company AstraZeneca using an email phishing scheme in November 2020 (Liu 2020).

Attackers can also target vulnerabilities within an organization's supply chain or critical infrastructure. They can infiltrate an organization via a unsecure vendor network connection, be infected by malware through a business associate's email, or have an attacker exploit a flaw in a suppliers hardware or software component. In December 2020, suspected Russian cyber spies infiltrated SolarWinds, a network monitoring software provider with over 300,000 clients including the U.S government and over 400 of the Fortune 500 companies (Clarke 2020).

Finally, there are innumerable untargeted attacks intended to harm any vulnerable system which can be found on a network. Sometimes attackers exploit new previously unknown vulnerabilities for which patches have not been developed and deployed. More often, attackers exploit known vulnerabilities where system owners have failed to install available fixes. These systems may also not have implemented proper cybersecurity protection technologies such as encryption, anti-virus software, firewalls, and data

backups. A good example of an untargeted attack was the WannaCry ransomware event in 2017 that impacted more than 300,000 computers in 150 countries, spreading through unpatched versions of Microsoft Windows, and causing up to $8 billion in economic losses (CyRiM Report 2019).

Ultimately, as a result of both ongoing targeted and untargeted attacks and the associated economic costs and other less tangible losses, firms have gradually demanded cyber insurance coverage to meet there general and more specific cyber risk transfer needs. In response, insurance companies have developed portfolios of cyber insurance products, procedures to assess and underwrite the cyber risk, policy terms and conditions to manage client cyber behavior, and services to help clients reduce cyber losses and manage ever evolving cyber threats.

C. Cyber Insurance Supply (Insurers)

According to the National Association of Insurance Commissioners (NAIC), in 2020 there were at least 620 domiciled (admitted) insurers and alien (non-admitted) surplus lines insurers writing cyber insurance policies in the United States. Combined, they sold a total of roughly $4.1 billion in direct written premiums with over 4 million cyber policies in force (NAIC 2021).

The market is divided into two types of products – “packaged” where the cyber coverage is part of a single policy for a variety of different coverage needs – and “stand-alone” policies that offer specialized cyber risk coverage tailored to the individual needs of a company. The Top 20 carriers selling both packaged and standalone policies combined, including Chubb, AXA and AIG, wrote over 83% of the market. Overall, the

market for cyber insurance, both in policies and direct premiums written, has nearly doubled since 2015 - making it one of the fastest growing segments in the insurance industry (NAIC 2021).

As a fairly new product, cyber insurance has been profitable. One key measure of profitability, total loss ratio, over the past four years has averaged between 32.4% and 66.9% (NAIC 2021). However, profitability is volatile and performance varies considerably across individual insurance companies. For example, in 2020, loss ratios among Top 20 domestic cyber insurance providers ranged from 25.8% to 114.1% (NAIC 2021).

The 2021 cyber insurance market can be described as both evolving and nascent. It is evolving because the take up rate for cyber insurance is still less than 50% and the nature of cyber risk continues to change. While there is actuarial data for the frequency and impact of some types of cyber events, due to the evolving nature of cyber-attacks, the half-life value of this data is short. The market for cyber insurance is still nascent primarily because there has yet to be a catastrophic event to hyper-drive demand and better define the maximum possible loss (MPL). While there have been significant events like NotPetya, with an estimated cost of up to $10 billion, it only had a limited effect on cyber insurance take-up, and losses for cyber insurers were small due to the lack of policy coverage (Guy Carpenter 2019). A 2019 report by the Cyber Risk Management (CyRiM) Project estimated a possible worst case scenario for a global cyber-attack propagated via malicious email to be between $85 billion and $193 billion (CyRiM 2019, p. 6). However, without a real precedent setting event defining the size and scope of

possible exposure, reinsurers have been unwilling to provide significant reinsurance capital; and without adequate reinsurance capacity, most primary cyber insurers still limit their maximum single policy coverage to no more than $100 million (CIAB 2019). Further, without a 9/11-type event, the US federal government has been unwilling to put forward a reinsurance backstop for cyber similar to the Terrorism Risk Insurance Act (TRIA).

Thus, while the cyber insurance market has seen significant growth and maturity over the past few years, its further expansion may be stymied by the uncertainty regarding the industry's ability to cover a worst case cyber event. Per Warren Buffet in 2018, "I don't think we or anybody else really knows what they're doing when writing cyber….We don't want to be a pioneer on this" …and anyone who claims to know the base case or worst case for losses is "kidding themselves" (Basak and Chiglinsky 2018).

D. Cyber Insurance Business Model, Insurability & Coverage

Cyber insurance is a business transaction between firms who seek to manage the risk of uncertain loss events and maximize their profits through the transfer of cyber risk, and insurers who seek a profit from premiums exceeding losses over time by spreading the cyber risk over time and across many clients. This transaction puts a price tag on cyber risk and can provide economic incentives for clients to adopt cyber risk reduction and safety measures.

Firms seeking cyber insurance want coverage for both potential first- and third-party financial losses, as well less tangible indirect losses arising from the malicious actions or carelessness of internal and external actors, including suppliers and other business

associates. They also want clearly defined coverage protecting essential domestic and global business activities, at an affordable price that conforms to their capital availability and business needs. SMEs, in particular, may also want insurers to help them manage their cyber risks.

Likewise, insurers view cyber insurance as a business opportunity with growth and high profit potential. In the US, hundreds of insurance carriers are selling millions of cyber policies and with a firm take-up rate of less than 50%, there remains considerable room for future expansion. High perceived profitability is attracting new entrants with limited cyber underwriting experience, who may underprice cyber risk and accumulate large unsustainable concentrations of cyber exposure. Insurers biggest fear is "tail risk"- low frequency, high impact events affecting many policyholders - that can generate a large number of high cost claims, wipe out many years of surplus premiums, and threaten the solvency of many insurance and reinsurance companies.

One immediate and ongoing risk of catastrophic losses relates to what is called "non-affirmative" or "silent" cyber – that is, the claim occurs within traditional P&C and CGL commercial policies. Back in the 1990s, many insurance companies covered cyber-related losses under their commercial "all risk" CGL, P&C, and other business policies. However, by the early-2000s, many insurers realized the growing cyber threat and began to exclude first and third-party damage caused by cyber events from their traditional policies. The problem is that there is a very blurry line between physical and cyber risk, and ambiguous policy language has created a great deal of confusion about what is covered and what is not. To deal with this problem, insurers are aggressively identifying

and eliminating non-affirmative cyber coverage in their portfolios and also pushing clients to subscribe to affirmative standalone cyber policies or cyber endorsements that are specifically design to address the main losses that normally result from data breaches and other malicious or accidental information technology failures (OECD 2017).

Currently, cyber insurance policies cover a variety of first-party and third-party loss exposures (Table 2.1). Supply, in sync with demand, seems to be most available for first-party losses incurred directly by the insured including costs associated with responding to breach of privacy events (e.g. customer notification, crisis management), data and software restoration, cyber extortion (e.g. ransom payments), business interruption (e.g. lost profits) and regulatory actions (e.g. fines and legal defense). Coverage is also available for certain potential third-party liability costs for defending against public or private litigation, judgments, or other rulings, as well as fines, fees, and settlements stemming from cyber-related lawsuits. This includes potential Internet media liability (e.g. defamation, libel, slander, and copyright infringement), network service failure liability (e.g. failure to protect), technical/professional services and E&O liabilities.

Table 2.1: Typical First- and Third-Party Cyber Insurance Coverage (Source: Risk Management Solutions)

Cyber Loss Coverage	Type	Description	Supply	Demand
Breach of Privacy Event	1st Party	Response costs including customer notification, crisis management, credit monitoring, public relations, etc.	92%	97%
Data and Software Loss	1st Party	The cost of reconstituting data or software that have been deleted or corrupted.	81%	91%
Incident Response Costs	1st Party	Direct costs incurred to investigate and close the incident to minimise postincident losses.	81%	N/A
Cyber Extortion	1st Party	Cost of expert handling for an extortion incident and ransom payment.	73%	94%
Business Interruption	1st Party	Lost profits or extra expenses incurred due to the unavailability of IT systems or data.	69%	68%
Regulatory Actions	1st Party	Covers cost to respond to governmental inquiries, inc. fines, penalties, legal defense, investigations or other regulatory compliance costs. Provided where it is legally permitted.	62%	67%
Reputational Damage	1st Party	Loss of revenues arising from an increase in customer churn or reducedtransaction volumes, which can be directly attributed to the publication of a defined security breach event.	46%	60%
Financial Theft & Fraud	1st Party	The direct financial loss suffered by an organisation arising from the use of computers to commit fraud or theft of money, securities, or other property.	23%	66%
Intellectual Property Theft	1st Party	Loss of value of an IP asset, expressed in terms of loss of revenue from reduced market share.	23%	56%
Physical Asset Damage	1st Party	First-party loss due to the destruction of physical property resulting from cyber attacks.	19%	31%
Internet Media Liability	3rd Party	Cost for investigation, defence cost and civil damages arising from defamation, libel, slander, copyright infringement, publication negligence in publication of any content in electronic media.	65%	63%
Network Service Failure Liability	3rd Party	Third-party liabilities arising from security events occurring within the organisation's IT network or passing through it in order to attack a third-party.	42%	N/A
Contingent Business Interruption	3rd Party	Business interruption resulting from the IT failure of a third party, such as a supplier, critical vendor, utility, or external IT services provider.	33%	72%
Technology Errors & Omissions Liability	3rd Party	Errors & Omissions (E&O) coverage for third party claims from failure to provide adequate technical service including legal costs and expenses resulting from a cyber attack or IT failure.	27%	N/A
Professional Services Errors & Omissions Liability	3rd Party	E&O coverage for third party claims relating to failure to provide adequate professional services including legal costs and expenses resulting from a cyber attack or IT failure.	23%	N/A
Director & Officer (D&O) Liability	3rd Party	Costs of compensating claims made against the firm directors & officers including for breach of trust or duty resulting from cyberrelated incidents from alleged misconduct or failure to act	13%	N/A
Death and Bodily Injury	3rd Party	Third-party liability for death and bodily injuries resulting from cyber attacks.	15%	10%

Coverage is often customized to a particular sector's or company's needs. For example, only firms that operate in data regulated sectors such as healthcare or financial require coverage for regulatory actions, and SMEs may only need limited coverage that they can purchase at an affordable price. Thus, the ability to design and market cyber insurance products with suitable target population coverage at an affordable risk-appropriate premium is a key element of cyber insurer market success.

E. Cyber Insurance Policies and Claims

Insurers manage client cyber risk and coverage expectations through policy forms and language that outline who is an insured, the insuring terms and conditions, what type of losses are covered, and what type of losses are excluded. The policy also defines the policy period, territory of coverage, premiums, limits and sub-limits of liability,

retentions, insured obligations, triggers, and other provisions/services designed to promote safe client cyber behavior.

For most of cyber insurance history, there were no standard policy forms. Each individual cyber insurer designed their own standalone and endorsement forms to meet their needs. This created a great deal of confusion among cyber insurance brokers, agents, and clients over covered losses, especially when comparing one company's coverage to that of another. However, in 2017-2018, the Insurance Service Office (ISO) released a series of standardized policy forms for large commercial clients (CY-00-00-18) and SMEs (LI-CY-2017-005) (NUCO 2018).

Much of the standard cyber insurance policy form[1] contains language and terms common to all types of insurance policies including named insured, policy period, dispute jurisdiction, certain general exclusions (e.g., nuclear materials), standard definitions, and certain duties of the insured (e.g. subrogation). The focus below describes aspects of the cyber policy which are different from other types of insurance policies.

Similar to other types of specialty insurance, cyber policies are almost always written on a claims-made and reported basis (vs. occurrence basis). This means that the policy only covers cyber events that occur and are reported during the policy period (typically one year) and for an optional extended period (typically no more than three years) after coverage ends. The policy usually contains a retroactive policy start date. If it is determined that a breach occurs before this date, even though it is detected and reported

[1] Information on standard cyber insurance policy language came from a 2019 sample policy SP 14 797 0119 used by cyber underwriter Coalition which writes policies for a broad range of brokers. Policy can be found at: https://apcybersolutions.com/wp-content/uploads/2019/02/Coalition-Cyber-Policy-Form-w-Endorsements-SPECIMEN.pdf

after this date, the incident is not covered. This protects the insurer from covering preexisting conditions for which no premiums were collected.

Unlike other types of insurance, cyber insurance coverage is often global, covering cyber risks for multinational corporations, as well as laptops and smartphones of company employees when they travel. The "triggers" for insurance coverage claims are based on internal or external cyber events - either intentionally caused by malicious threat actors or unintentionally resulting from unplanned system outages due to employee or supplier negligence (CyRiM 2019).

Oftentimes, the premiums, coverage limits, and retentions are stated in the policy upfront. Premiums for cyber insurance are typically much higher than for other types of insurance, averaging $8000 to $13,000 per million - a rate that can be three times more expensive than CGL and six times more expensive than P&C (OECD 2017). Another distinctive feature of cyber insurance is the aggregate limit, which is typically lower than other types of insurance, and the types of first- and third party coverage (e.g. cyber extortion, breach response, network security liability) that are unique to cyber. An estimated half of all global cyber insurance policies sold are for limits of less than $1 million; less than 10 percent of policies written globally are for aggregate limits over $10 million; and for a company to obtain cyber coverage of more than $100 million typically requires the construction of a complex tower of coverage involving many different insurance companies (CyRiM 2019, p. 6). Many firms ask for higher aggregate coverage limits at the time of policy renewal (Advisen 2020, p. 9). Retentions, that include deductibles, copays, and quota shares, are negotiable as part of the premium calculation

process, but typically range from 5 to 40 percent of the coverage limit. The policy then layouts what first- and third-party losses are covered during the policy period, what losses are not covered (exclusions), and later has a long list of definitions of both insurance and cyber terms used throughout the coverage/no coverage sections.

The losses covered align tightly with the first- and third-party coverage types selected. Common first party coverage include: 1) Breach Response, 2) Crisis Management and Public Relations, 3) Cyber Extortion, 4) Business Interruption and Extra Expenses, 5) Digital Asset Restoration, and 6) Funds Transfer Fraud. The policy can also include special conditions such as a waiting period of hours or days before business interruption compensation kicks in. Exclusion language is typically very broad to allow insurers flexibility to preclude a wide range of potential claims arising from insured illegal or unethical acts such as fraud by a senior executive or misrepresentation of the cyber risk on the insurance application (known preexisting condition). The intent is also to exclude coverage for uninsurable risks such as intellectual property losses, and risks that are insured in other policies. Often, cyber insurance is in excess to other insurance, meaning it only provides indemnity when other more applicable coverage is exhausted.

Finally, the cyber policy form details the obligations of the insured, the services that the insurer provides to help control and reduce losses, and the circumstances under which coverage can be cancelled or withdrawn. Key obligations of the insured include taking reasonable precautions to protect their IT and network assets, and their duty to promptly report actual or suspected cyber incidents that could give rise to a claim. Evidence

suggests that incidents that are longer to detect and report often have more severe consequences for both insurer and insured (Verizon 2020). As part of their policy obligations most cyber insurers provide pre-claim and post-claim assistance for forensics and other services to help mitigate losses. Either party can cancel coverage with 60-day notice.

According to NAIC, over 22,000 cyber insurance claims were filed with US carriers in 2020, nearly double the number from 2018, with three quarters being first-party claims (NAIC 2021). The average claim in 2020 was $51,960 for packaged policies and $86,964 for standalone – both up over 60 percent from 2019 levels (NAIC 2021). Somewhat muting these numbers is the fact that many firms with cyber insurance are hesitant to file claims. They fear that making the breach public could damage the firm's reputation, erode stakeholder confidence, and possibly lead to expensive litigation and regulatory fines. Failure to file the claim and make the breach public could actually make the situation worse, not only for the firm involved but also for their clients, business partners, and other firms who may have similar vulnerabilities and exposures. Thus, there are a number of unpredictable behavioral factors and outcomes that insurers need to consider when assessing and underwriting cyber risk, and managing client cyber safety.

F. Cyber Insurance Underwriting, Cyber Risk Management and Safety

When an insurer evaluates the cyber risk of a firm that wants to buy cyber insurance, the insurer needs to assess the cybersecurity maturity-level of the potential customer. Do they understand their cyber risks and are they protecting themselves from attacks? Are employees trained in good "cyber hygiene" practices to avoid breaches and do they have

a good response plan if an attack occurs? Do they have a security organization in place to respond effectively to cyber incidents, and is upper management committed to providing resources to address cyber threats?

Firms that have high cyber maturity typically use a combination of self-protection, self-insurance, and cyber insurance to protect themselves against cyber losses. Self-protection attempts to reduce the probability of security breaches by employing measures such as firewalls, anti-virus software, authentication, encryption, and intrusion detection systems. Self-insurance attempts to minimize losses caused by a security incident through set-aside funds ("captives") and through mitigation measures such as data backup systems and disaster recovery plans. After these measures, any remaining "residual" cyber risk that cannot be prevented or protected can be transferred to a third party insurer, provided that the insurer finds the risk to be acceptable ("insurable") at a risk appropriate premium that is fair and acceptable to the client.

Firms that have low cyber maturity may have little understanding or awareness of their cyber risk. They may have minimal preventative cybersecurity controls in place, and no security organization or plans to deal with a disruptive cyber event if it occurs. Such firms may be uninsurable, or provisionally insurable only if they implement a minimum cyber security practices outlined in its cyber policy. In fact, a recent survey of brokers and agents indicated that only about 37 percent of their clients had a proactive information security program covering the four key areas of prevention, detection, containment and response/eradication (CIAB 2019).

To determine client cyber maturity and insurability, insurers use a specialized cyber underwriting process to assess, classify, and quantify the cyber risk and, if applicable, calculate a risk appropriate premium to offer the client in exchange for a specified level of coverage.

The basic starting point for all cyber policies is for firms to complete a self-assessment, usually in the form of an application questionnaire.[2] The extent of the inquiry will vary greatly based on the firm's size, industry and business activities. Some applications have just a few questions, while others more than a hundred, and may require follow up customer meetings, audits, risk assessments, inspections, and even penetration testing. Given the volume of companies seeking coverage and the high cost of full scale risk evaluations, insurers want to spend their resources evaluating high profit clients, and quickly weed out uninsurable firms with no understanding of their cyber risks and high potential for breaches and costly claims.

At a minimum, insurers want to know the firm's business sector and activities, size of company (in revenue and number of employees), past experience with insurance and claimable cyber events, reliance on IT for business operations, and whether they have implemented basic cybersecurity protections such as anti-virus software, firewalls, and data backup. For very basic customers with low perceived risks, this may be sufficient for them to secure a flat rate cyber policy with coverage up to $100,000, with a deductible of $10,000, for an annual premium of less than $500 (Romanosky et al. 2019). The

[2] Information on the typical cyber insurance application questionnaire was gathered primarily from a RAND study entitled *Content Analysis of Cyber Insurance Policies: How do carriers write policies and price cyber risk?* (2019).

deductible, right to audit, and exclusions for failure to protect, all act as ways the insurer can control client moral hazard and adverse selection.

In cases where the client cyber business risk is significant and the client coverage needs are extensive, the insurer underwriting assessment will likely be much more comprehensive. First the self-assessment questionnaire will require that the applicant provide much more detailed information on their organization, operations, technology, and policies/procedures comprehensive. From organizational standpoint, underwriters will likely want to know about the firm's management; their cybersecurity risk management philosophy; the existence of an internal security group including whether there is a Chief Information Security Officer (CISO); and staff awareness and training on IT security. To assess the operation of a business, underwriters may require details on key clients, business partners, type and sensitivity of collected data, financial transactions (e.g., credit card processing), and IT security budget and spending. From a technology standpoint, underwriters may want details on the company's IT and networking infrastructure, technical security measures, encryption practices, and process for patching vulnerabilities. Finally, underwriters will ask about the availability of current cyber incident response and business continuity plans, the client's access control procedures, their internal and external privacy policies, their compliance with sector regulations, and their adoption of key cybersecurity standards. There may also be questions about specific sector or company risks.

After reviewing the applicant's self-assessment, the underwriter may determine if an external examination is required. This could include meetings between the insurer risk

assessment team and key applicant personnel such as the CIO. It could also include audits, threat analyses, and inspections conducted by the underwriting team or by a third party consultant. Audits might include review of financial records, security logs, regulatory compliance, and security practices. Vulnerability and threat analyses look at what hardware and software exposures might exist in the client IT systems and networks, and what internal and external actors or non-human threats might cause a system outage or cyber event. Inspections might focus on physical security issues like uncontrolled access to IT facilities or physical inspection and inventory of company computer devices to assure that none have been lost or compromised. Inspectors could also conduct unannounced penetration testing to verify the effectiveness of client security measures. Finally, given the dynamic nature of cyber risks, clients might partner with insurers and managed cybersecurity providers (MCPs) to assure that insured network assets are continuously monitored by experts to quickly detect and respond to attacks when they occur.

Based on the evidence collected, the underwriter then decides if coverage will be extended or rejected and, if extended, what the premium, coverage level, terms and conditions will be. They will also need to determine how this risk compares to other clients and how it would fit into their risk portfolio. Insurers do not want to over accumulate too many similar risks, such as from a single sector. They want to diversify and spread the risk so that no single event can cause a large loss. For this reason they may want to quota share the risk with other carriers, or cede some risk to reinsurers. Either option has a cost that needs to be factored into the premium calculation.

RAND Corporation in a 2019 study examined the premium calculations for approximately 235 cyber insurance policy filings from the states of New York, Pennsylvania, and California spanning the period 2007 to 2017 (Romanosky et al. 2019). The study found a wide variety of ways carriers compute cyber insurance premiums including a flat rate price usually used for smaller, low risk and low coverage level policies. Some carriers use cyber insurance schedules based on an applicant's base asset value or revenues, with modification factors based on the amount of the retentions (e.g., deductibles & copays), coverage levels, claims history, and waiting periods for business interruption (Romanosky et al. 2019, pp. 15-16). Some insurers also use a hazard rating factor (e.g., low, medium, high) based on the client's industrial sector or whether the firm is for profit or not for profit (Romanosky et al. 2019, p 16). The more sophisticated premium calculations, used by big insurers for larger corporate clients, applies basic security modifiers around broad categories of data protection such as privacy controls, network access controls, and having an incident response plan. Applicants are then ranked based on their scored cybersecurity maturity level (Romanosky et al. 2019, p 16). Other insurers also apply cybersecurity weighting factors, rewarding excellent security with as much as a 25% premium discount, and penalizing poor cybersecurity with as much as a 50% surcharge. Some carriers also applied similar credits and penalties at renewal for individual security attributes such as frequency of disaster recovery plan simulations, penetration testing, or cyber-attacks experienced during the policy period (Romanosky et al. 2019, p 17). All weighted factors are then used to compute a base rate modified by any insurer-focused security factors and applicant-selected criteria including

desired coverage types, coverage levels, and retentions. Finally, the insurer adds their profit margin, usually averaging between 25% and 35%.

Hence, the most sophisticated cyber insurance underwriting can use the risk assessments, conducted prior to policy inception and at annual policy renewals, to score individual cybersecurity attributes, rewarding good scores with discounts and punishing bad scores with premium surcharges or even policy cancellation. In 2021, the projected premium for a large corporate customer will be between $8000 and $13,000 per $1 million coverage (Willis 2020).

To improve client cyber awareness and safety and, at the same time, reduce the likelihood and severity of client claims, many insurers offer both preventative services to stop incidents from occurring, and post-breach incident response services to help minimize the negative impacts. Often these services are included as part of the cyber package at no additional charge.

Basic preventative services may include advice on choosing and implementing antivirus and firewall software, providing suggestions on improving network security, assessing privacy policies, reviewing incident response plans, and helping employees get necessary cybersecurity training. The rapid rise of ransomware attacks in 2020 caused a major increase in claims for covered extortion payments and data restoration costs. By providing clients with ransomware training materials and guidance, insurers are helping educate firm employees to recognize phishing emails and avoid ransomware infections. Further, if infection occurs, they are teaching clients how to best to respond to mitigate losses. Some insurers are also teaming with managed cybersecurity providers (MCPs) to

offer clients a package of services including software patching, anti-virus updates, 24/7 monitoring, and intrusion detection. Oftentimes insurers offer clients premium discounts and other incentives to get them to subscribe. Directing these services to policyholders promotes loss control and is a differentiator in marketing their cyber products.

Insurers also regularly offer post-breach response capabilities as an integrated part of their products. Many insurers have 24/7 breach reporting hotlines and in-house teams of cyber loss professionals who provide guidance through incident investigation and response, as well as post-incident remedial assistance. Many have also developed networks of external consultants to offer clients assistance with crisis management, public relations, legal issues, regulatory investigations, data recovery and business remediation. Recovery and remediation capabilities are particularly important since the length of time before a breach is discovered and remedied has a tremendous impact on the number of records lost and costs of recovery. These services also give insurers a degree of quality control over client incident management, making it easier for them to predict and manage the costs of cyber claims.

Thus, archival and logical evidence suggests that cyber insurance, if properly underwritten and administered, can be an effective, market-driven way to positively influence private sector cybersecurity and safety behavior. Cyber insurance puts a price tag on cyber risk and creates economic incentives for clients to adopt cyber risk reduction and safety measures. Through the application self-assessment questionnaire, firms become more aware of their cyber risks and are more likely to implement additional protective measures. The cyber insurance underwriting process can help uncover client

cybersecurity vulnerabilities, identify cybersecurity gaps, and provide suggestions for cyber safety improvements. Especially for SMEs with limited resources, these services can be an attractive cost effective way to bolster their IT security capacity.

IV. The Political Economy of Cybersecurity & Cyber Insurance

Much of scholarly debate of cybersecurity over the past twenty years has focused on the economic incentives for firms and individuals to invest in their own cyber protection and the impact that these decisions and various government actions have on societal network security.

In 2001, Cambridge University Professor Ross Anderson in a paper entitled "Why Information Security is Hard (An Economic Perspective)" outlined how many of the problems in information security can be explained "using the language of microeconomics" (Anderson 2001). In this paper, Anderson describes information security as a "Tragedy of the Commons" an economic theory originally proposed by Garrett Hardin where individuals acting independently and rationally in their own self-interest, behave contrary to society's interests by depleting some common resource (Hardin 1968). Anderson uses this analogy and the concept of externalities to explain the economic incentives for firms to sell insecure products filled with vulnerabilities, and for users to underinvest in the cybersecurity services needed to protect society as a whole.

In a 2003 paper, Howard Kunreuther and Geoffrey Heal co-authored a paper on what they called the interdependent security (IDS) problem where the risks faced by any one firm depends not only on its choices but also on those of all others (Kunreuther and Heal 2003). The authors found that IDS can result in positive externalities where one firm's

investment in information security can benefit other firms. However, this can cause other firms to underinvest in their own security – resulting in diminished security returns for all firms.

The fundamental starting point for most papers on the political economy of cyber insurance is that absolute technological cybersecurity protection is impossible. Subsequently, firms need to adopt risk management strategies that include mitigating the impact of cyber-attacks and transferring any residual risks to third-party insurers (Anderson 2001, Schneider 2002, Bolot & LeLarge 2009, Herath & Herath 2011, Pal 2012).

Due primarily to the lack of actuarial data to model the development of insurance markets and compute risk appropriate premiums, most scholars have employed an economic approach to analyze the supply and demand for cyber insurance products, and the costs and benefits of utilizing cyber insurance as a risk management tool. Many scholarly economic models have indicated that cyber insurance can incentivize the insured to invest in their own cybersecurity (Kesan et al 2005, Baer et al 2007, Bohme & Schwartz, Bolot & LeLarge 2009). An important economic driver to this investment incentive is insurer premium discrimination – clients that invest in their own cybersecurity are rewarded with lower premiums (Kesan et al. 2005, Bolot & LeLarge 2009, Pal & Hui 2013, Clark et al. 2014). Many scholars also advocate that cyber insurance will help to establish and spur the adoption of cybersecurity standards and best practices, and that this will in turn improve the cybersecurity of society as a whole

(Kesan et al 2005, Majuca et al 2005, Bolot & LeLarge 2009, LeLarge & Bolot 2009, Marotta et al. 2015).

Other scholars argue that there are many factors that could result in cyber insurance market underdevelopment or market failure, including information asymmetry between the insurer and the insured, the potential for moral hazard, and the interdependent and correlated nature of cyber-risks. Some economic models suggest that asymmetric information results in the adverse selection of high-risk clients who underpay for the insurance they receive (Schwartz et al. 2010). Asymmetric information can also cause a moral hazard problem where clients, knowing they are insured, behave recklessly and reduce their investment in self-protection, believing that insurance payments would offset any losses (Schwartz et al. 2010, Shetty et al. 2010, Pal 2012, Schwartz & Sastry 2014). To address potential information asymmetry and moral hazard issues, cyber insurers usually require applicants to undergo extensive risk assessments (Young et al. 2016). Several scholars have also concluded that insurers can overcome moral hazard problems by imposing deductibles, co-payments, and coverage limits that ensure that the insured suffers some loss in the event of a cyber incident (Gordon & Loeb 2003, Kesan et al. 2005, Pal 2012, and Young et al. 2016). In addition, Rainer Bohme created an insurance model demonstrating that premium discrimination could incentivize clients and IT providers to implement more diversified systems, reducing the monoculture threat of correlated losses (Bohme 2005).

Models have also been developed to examine how cyber risks might be spread across multiple entities to increase coverage and absorb losses following a catastrophic cyber

loss event. For example, a 2007 paper outlined an insurance model for insurance companies to decide on the number of optimum layers, to spilt large cyber risks in order to reduce the overall variance of the loss to individual insurance entities (Mukhopadhyay et al. 2007). Likewise, a paper by Zhao et al. in 2009 described how risk pooling arrangements and managed security services can complement cyber insurance and optimize cybersecurity self-protection investment (Zhao et al. 2009). There has also been considerable scholarly discussion on the need for greater cyber reinsurance capacity or other financial instruments to hedge against possible catastrophic losses (Baer & Parkinson 2007, Clinton 2012, Toregas & Zahn 2014, Tondel 2015, Young et al, 2016).

As demonstrated by Kunreuther and Heal, interdependent security can create externalities that can influence both a firm's decisions to implement self-protection and purchase cyber insurance (Kunreuther & Heal 2003). For example, firms that invest in antivirus software create positive externalities by preventing virus infections from spreading to other firms. However, these positive externalities can also cause other firms to "free ride" on other firms' security measures and subsequently underinvest in their own security, resulting in sub-optimal societal network security (Pal 2012). To manage cybersecurity investment inefficiency, many scholars contend that various public and private policy measures need to be implemented in order to internalize these externalities, allowing firms to benefit from good security and suffer the costs of bad security (Gordon et al. 2003B, Kesan, et al. 2005, Zhao et al. 2009, and Clinton 2012).

Consequently, economic models and scholarly papers discuss various public and private policy initiatives to internalize externalities, stimulate the cyber insurance market,

and improve private sector risk management practices. Kunreuther and Heal in their IDS research concluded that more research needed to be conducted on "the appropriate roles of the public and private sectors in developing strategies that include economic incentives (fines or subsidies), third party inspections, [and] insurance coupled with well-enforced regulations and standards" (Kunreuther & Heal 2003, p. 246). Bohme and Kataria suggested that government might want to make cyber insurance compulsory, at least for some companies like software providers or firms that sell products to the government (Bohme & Kataria 2006). Mandatory liability insurance helped drive car insurance market development, as well as deployment of automobile safety standards (e.g. seat belts and airbags). Subsequent research found that compulsory insurance can incentivize clients into making self-defense investments through premium discrimination - charging fines atop fair premiums to high-risk users, and providing rebates to low risk users (Hoffman 2006, Bolot & LeLarge 2009, Pal & Hui 2013). Further, Bolot and LeLarge also found that "without regulation, insurance (in a competitive market or with one monopoly) is not a good incentive for self-protection" (LeLarge & Bolot 2009, p. 2).

Several papers have gone on to suggest that mandatory breach reporting laws that publicly expose cyber incidents can help to drive the adoption of cyber insurance (Braunberg 2013, and Tondel 2015). In 2003, demand for cyber insurance surge in the US with the passage of the first state mandatory breach notification law in California (Marotta et al. 2015), and passage of a national breach law in the US or the EU could have a similar stimulatory market effect. There has also been substantial academic commentary on the need for government reinsurance, similar to that provided for

terrorism insurance under TRIA, to bolster the supply and coverage-levels of cyber insurance products (Baer & Parkinson 2007, Clinton 2012, Toregas & Zahn 2014, and Tondel 2015). Thus, many scholars believe that government needs to have a role in the development of the cyber insurance marketplace.

Chapter 3: Methodology & Research Design

I. Introduction

The purpose of this dissertation research is to examine the relationship between safety and insurance at firms engaged in a number of emerging technological environments, over time. For the purpose of this study the dependent variable ***safety*** is defined as managing risks resulting in a reduction in the frequency and magnitude of losses. Emerging technologies are scientific or technical innovations which are generally new, and are characterized by their novelty, relatively fast growth, prominent impact, and uncertainty regarding their future development and risks.

The primary independent variable to be tested is ***insurance*** as defined by the number and type of policies taken up by firms engaged in the emerging technology, as well as a number of other insurance factors including insurer type, risk factors, annual premiums, coverage levels, deductibles, copays, and whether coverage is mandatory within that technological regime. As outlined in the literature review, insurance can act as a private sector regulator, promoting the development of safety standards and adoption of best practices for managing emerging technological risks including those associated with commercial nuclear power, environmental pollution, and cybersecurity.

All of these emerging risks shared characteristics including a high degree of uncertainty, initial lack of actuarial data, potential for catastrophic losses, exclusion from

P&L and CGL policies, and the belief that they were "uninsurable." All of these emerging risks eventually found a path to insurability. However, before these risks were transferred, insurers needed assurances that the insured were taking appropriate safety precautions and investing in their own security to minimize the risk. This included adopting safety standards, conducting of risk assessments, applying best practices, and, if necessary, complying with government regulations. The question is whether insurance can improve safety and security in other emerging technological risk regimes. Thus the primary research question addressed by this research is:

"How can insurance promote better safety in emerging technological regimes?"

In answering the primary research question, this dissertation will take a broader perspective on insurance that encompasses not only insurance companies but also a variety of public and private financial mechanisms that can manage information asymmetries and "insure" emerging risks. Further, this dissertation will explore whether insurance experiences in various emerging technologies can be applied to future emerging risks by testing the primary hypothesis:

"Insurance can improve the safety posture of firms engaged in emerging technologies"

To test this hypothesis, this research will examine insurance in three emerging technology regimes with a focus on issues such as:

1. What insurance policy mechanism (e.g. premium differentiation, coverage limits, etc.) are best at managing firm safety behavior.
2. How do insurance entities (e.g. shareholder owned, mutual, risk pools, reinsurers, etc.) interact and how can they best manage emerging technology risks?

3. What factors and conditions contributed to the development and adoption of insurance and can similar processes be used in the development of insurance for future technologies?

4. To what extent has insurance driven the definition of safety, the development of standards and adoption of safety measures in emerging technological regimes?

5. What other safety mechanisms, such as regulation and litigation, influence firm safety and how do they affect and interact with insurance safety activities?

II. Research Design

This research will employ a mixed-methods approach, involving both qualitative and quantitative analysis, to explore how insurance promotes better safety in three emerging technologies: 1) nuclear risk at U.S. commercial nuclear power plants, 2) environmental risks at U.S. chemical and waste disposal facilities, and 3) cyber risk in the U.S. health care sector. This approach will involve the development of multiple comparative case studies to explore how insurance influenced security and safety behavior in past and present emerging technological risks, and how lessons learned might be applied to future emerging technological risks.

According to Robert Yin: "In general, case studies are the preferred method when (a) "how" and "why" questions are being posed, (b) the investigator has little control over events, and (c) the focus is on a contemporary phenomenon with a real life context" (Yin 2009, p. 2). All three are relatively contemporary phenomena. During the times when each technology emerged and safety was recognized as an issue, there was a lack of empirical data on the frequency and magnitude of potential technology-related events that could result in substantial tangible and intangible losses. All three cases initially had

issues with "insurability" of the risk that have, and will likely continue to have, an impact on the evolution of the technology in the future.

The three case studies were selected using John Stuart Mill's comparative "most-different method" or "method of agreement" where cases are selected that are as different as possible, except on the outcome of interest (the dependent variable), which is the same. In this dissertation, the dependent variable is ***safety***, and the primary independent variable is ***insurance*** with some additional independent variables including regulation, litigation, other characteristics of the studied entities, as well as measurements of the frequency and magnitude of potential loss events. The effects of these variables vary across case studies, and should help to increase the method's robustness. Any case study alternative explanations, assumptions, and limitations will be identified and discussed.

To allow for comparison, each case study is organized in a similar manner with guidance from the literature review. Each has an introduction defining the problem and a description of the initial history of each technology from a risk and insurance point of view. Next, each has a description of the political and economic variables influencing the development of the technology and the associated insurance regime, including the costs, benefits and primary risk factors. The evolution of the risk and the insurance regime is then explored culminating in the presentation of evidence of the role insurance played in promoting firm safety, and the lessons learned from that technology's risk and insurance experiences.

The primary units of analysis are US-based private-sector firms and equivalent public-sector entities, and the domestic facilities that they operate. One of the big

differences among the three case studies is the size of the populations sampled ranging from a little over a hundred U.S. commercial nuclear reactors, to thousands of hazardous waste sites, to hundreds of thousands healthcare firms and their facilities.

All case studies were conducted using a data collection protocol. The data from the various qualitative sources were coded and analyzed using NVivo, and the quantitative data using Microsoft Excel, ArcGIS, and Stata. All data came from publicly-available sources with no ethical issues requiring IRB approval.

The remainder of this chapter reviews the specific population attributes (constructs), sources, limitations, and data collection and analysis techniques used for each case study.

A. Managing Risk at U.S. Commercial Nuclear Power Plants – Methodology

Much of the data on insurance and safety for commercial nuclear power plants comes from the Nuclear Regulatory Commission (NRC) Agencywide Documents Access and Management System (ADAMS) – a library of unclassified documents, and from Congressional records, mostly provided by the HathiTrust Digital Library - a digital preservation repository. Key archival documents from the ADAMS collection include: 1) annual required proof of financial protection including annual premiums paid for liability and property insurance; 2) examples of how premiums were calculated using American Nuclear Insurer (ANI) Engineering Rating Factors (ERF) and Institute of Nuclear Power Operations (INPO) safety indexes, and 3) NRC Licensee Event Reports (LERs), Notifications of Violation (NOVs) and availability/capacity reports summarizing safety performance, incidents and infractions for individual reactors. Key Congressional documents include: 1) hearings conducted by the Joint Committee on Atomic Energy

(JCAE) and later committees; 2) Congressional testimony from insurers and operators on early nuclear insurance development and subsequent accidents; and 3) debate on the evolution of nuclear insurance through the lens of the Price-Anderson Act and its renewal.

There were several limitations in gathering and analyzing this data. First, nearly all of the data is unstructured, requiring its extraction from individual documents and its recording in an Excel spreadsheet for later review. A second challenge is that the U.S. nuclear insurance regime has changed numerous times since its inception in 1957. It has evolved from initial coverage provided by a large pool of private insurers with government reinsurance, to a regime that spreads collective risk among the plant owners through a mutual insurance pool and retrospective coverage. Thus insurers, methods of premium calculation, and risk factors have changed over time. Significant recent nuclear events including Three Mile Island, Chernobyl, and Fukushima accelerated these changes. These events and changes also accentuated the third challenge of extreme secrecy. Insurance coverage and safety information is considered sensitive and highly confidential. Insurer syndicates like ANI, and operator-owned mutual pools like Nuclear Electric Insurance Limited (NEIL) do not openly discuss the methods they use to evaluate safety and calculate premiums. Likewise, standards groups like INPO keep their peer-review plant inspections and safety ratings of its member companies hidden from public view. Occasionally, key details leak out, allowing for a patchwork mosaic connecting safety ratings, insurance premiums, and reactor safety performance.

The reliance on primary archival documents from US regulators and Congressional sources, stored in respected libraries, provides a high level of validity and reliability to the data. For this case study, *nuclear safety* is the primary dependent variable. It is defined by the frequency and magnitude of negative events as recorded through LERs and NOVs, as well as safety indexes created by the NRC, INPO and insurers (when available). The primary independent variable is premiums for liability and property coverage for specific reactors based on various risk factors. Some of these key risk factor variables include reactor location, type, age, power, availability, operating capacity, containment reliability, overall operating history, number of reactors on site, and population density near plant. Within the commercial nuclear power realm, federal regulations and the threat of massive litigation are also significant explanatory variables. They are offset, somewhat, by the internalization of the risk by plant operators through the mutual insurance pool and possible expensive contributions to retrospective coverage in the event of a major accident. The requirements for mandatory insurance as a condition of licensure also impacts operator safety behavior, since without insurance, the plant cannot legally be operated.

Given the limitations on data, premiums and safety results are presented visually using graphs and charts showing the potential correlation between insurer safety evaluations as quantified in premiums, and known safety measurements including INPO safety indexes, insurer ERFs, as well as LERs, NOVs, other violations, and inspection ratings as recorded by the NRC.

B. Managing Risks at U.S. Chemical & Waste Disposal Facilities –Methodology

Like the commercial nuclear power case study, most of the data for this case study comes from federal regulators and digital library archives. Once again, reliance on government and respected library sources provides a high level of validity and reliability to the data.

The primary regulatory source is the Environmental Protection Agency (EPA) and its Enforcement and Compliance History Online (ECHO) Database - more specifically from the Resource Conservation and Recovery Act Information System (RCRAInfo) data subset. RCRAInfo contains data on evaluations, violations, and enforcement activities for over 1.1 million hazardous waste facilities subject to RCRA regulations. The case study focuses on 1808 U.S. public and private chemical and waste Treatment, Storage and Disposal Facilities (TSDFs). Unlike the first case study, this data is stored in structured Excel (.csv) format. The EPA also has unstructured digital archival records on environmental laws and regulations.

The other primary data sources are non-EPA digital libraries including the HathiTrust, Lexus/Nexus, and insurance industry association archives including the Insurance Information Institute (III) and the International Risk Management Institute (IRMI). Key documents include: 1) Congressional hearing records on debate and passage of various environmental laws including RCRA and the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA) or "Super Fund," 2) verdicts and reviews of historic environmental litigation, and 3) copies of past and present environmental liability policies and methods for computing premiums.

The primary limitation in gathering and analyzing data was that a great deal of information on environmental insurance and premium calculation is proprietary, not readily available to public scrutiny. Compounding this problem is the fact that most environmental insurance is sold by "unadmitted" carriers as "specialty" or "surplus" policies that do not have to be filed with state regulators and shared with the National Association of Insurance Commissioners (NAIC) through their System for Electronic Rates & Forms Filing (SERFF).

One of the prominent features of this environmental regime is the synergistic relationship among regulation, litigation and private insurance. RCRA regulations mandate that all operators of TSDFs have proof of financial responsibility as a condition of permitting. Proof most often involves the purchase of insurance from a private carrier. Both federal and state regulators are responsible for safety inspections and also for audits confirming that financial protection is in place. The primary driver for the need for financial protection was the explosion of litigation following the discovery of hazardous waste under a residential community at Love Canal and eventually at thousands of other sites around the United States. The litigation nearly brought the insurance industry to its knees, with several prominent insurers, including Zurich and CIGNA, filing for bankruptcy reorganization. The experience motivated insurers to either withdraw from the market, or refocus their attention on specialty environmental insurance products with risk-appropriate premiums, based on environmental site assessments (ESAs) and other insurance risk management measures.

For this case study, ***environmental safety*** is the primary dependent variable. It is defined by the frequency and magnitude of negative events defined by RCRA and other EPA violations over the period 1980 to 2020. The primary independent variable is ***financial protection*** (insurance) as required under RCRA, and verified by federal and state regulatory audits. Over the 40-year period the ECHO data shows that federal and state regulators conducted 141,043 "evaluations" of TSDFs including onsite inspections, and over 22,0000 financial audits. During these evaluations they found 35, 716 safety violations including 2,681 financial violations for failure to produce adequate proof of financial protection. In addition, many safety violations occurred at federal- and state-operated facilities that are not required to have insurance or other proof of financial protection. Thus the RCRA data allows the comparison of the safety violation history of TSDFs with financial protection to those that do not.

The results are presented visually in a series of graphs, charts and a heat map. The number of safety and financial evaluations vs. safety and financial violations are compared by year and by state. Safety indexes were created showing the ratio of safety evaluation to safety violations by TSDF, and ownership type (private vs. government), and a financial protection index was created showing the ratio of financial audits to financial violations for private TSDFs by site. The index results for each TSDF are plotted using ArcGIS to a heat map showing the correlation between safety and financial protection by site and TSDF ownership type.

C. Managing Cyber Risk at U.S. Healthcare Firms – Methodology

The final case study focuses on cyber safety in the U.S. healthcare sector. Like the other case studies, it uses a retrospective descriptive analysis to allow historical comparison with other realms. However, in addition, this case study uses econometric modelling using Stata to determine if a correlation exists between cyber safety in the healthcare sector and the take-up of cyber insurance by healthcare sector firms.

The quantitative data comes primarily from two reputable sources. The first is the Department of Health and Human Services (DHHS) - Office of Civil Rights (OCR) Breach Portal which, through August 13, 2021, had a total of 4,171 breaches reported, exposing over 305 million records (OCR 2021) over a period beginning in 2009. This structured data, augmented with over 1400 additional healthcare breaches identified from media and other state and national breach portals, is used to create a new database – the Healthcare Cyber Attack Database (HCAD). As of August 31, 2021, HCAD (Appendix A) consists of 5,609 cyberattack incidents, affecting 392,370,978 PHI records that have occurred at public and private healthcare entities located in all 50 U.S. states, the District of Columbia, and Puerto Rico. The second major source is the National Association of Insurance Commissioners (NAIC) statutory Cybersecurity Insurance Filing Supplement, with data collected from 3,120 insurers over the period 2016 to 2020. NAIC requires U.S. domiciled insurers to report the following cyber insurance information:1) number and type of policies in-force, 2) direct premiums written and earned, 3) number and type of claims reported, 4) direct losses paid and incurred and 5) defense and cost containment expenses paid and incurred (NAIC 2020).

The retrospective descriptive analysis provides the background of cyber safety in the healthcare sector, including the major roles that regulation and litigation play in the demand for and development of cyber insurance for healthcare-sector firms. The data in the OCR breach portal, and subsequently in HCAD, came as a direct result of federal regulations requiring the reporting and posting of all cyber breaches of 500 or more records of "unsecure" (e.g. unencrypted) data from "covered entities," including healthcare providers and their business associates. While this federal regulation help create HCAD, it also is a limitation. Not included in the OCR Portal are breaches of less than 500 records and breaches involving encrypted data, including many ransomware attacks.

To deal with this missing data problem, other breach portals were tapped, including the Privacy Rights Clearinghouse (PRC) and the portals of several states including California, Maine, and Indiana. PRC is a structured dataset of over 9000 U.S. data breaches that occurred between 2005 and 2020, of which 4,581 are healthcare related. Unlike the OCR breach portal, PRC's data contains older events, as well as healthcare breaches affecting less than 500 individuals. To supplement the missing data on healthcare-sector ransomware attacks, a review was made of media sources such as such as HealthcareInfoSecurity.com, DataBreaches.net and Becker's Health IT, The review resulted in the discovery of 614 ransomware attacks which are housed in a separate dataset called HCAD-R (Appendix B). There was considerable incident overlap among the sources, and data edited to eliminate duplicates. A media search of Lexus/Nexus, DHHS and state breach enforcement sites and law journals also identified 253 civil

lawsuits and regulatory settlements involving over 200 healthcare providers and business associates housed in a separate dataset called HCAD-L (Appendix C).

This econometric model uses count panel data from HCAD (Appendix A) to examine the relationship between the take up of cyber insurance by U.S. healthcare sector entities and their management of cyber safety during the period 2015 to 2020. The panel consists of 15,144 observations from 2,524 healthcare entities over the six year period. It is very strongly balanced with no missing data. The healthcare-sector entities have been subdivided into 27 sub-entities (SUBCODE) representing all of the key healthcare provider types (e.g. Doctor, Hospital, etc.) and healthcare support companies (e.g. Admin, Medical Equipment).

There are two key dependent variables representing cyber safety. The first is ***Attacks*** denoting the number (frequency) of cyber-attacks experienced by each entity, each year. The second is ***AttRec*** representing the number of records impacted (magnitude) by each attack, each year. Each attack in the dataset is rated as either being internal or external (EXTHACK), and if external, whether it involved ransomware (RANSOM).

The key independent variable is INSPOL10K which is the estimated number of insurance policies issued each year for each sub-entity divided by 10,000. The estimate is based on the population of each sub-entity as derived from the 2018 U.S. Census Statistics of U.S. Businesses (SUSB 2018) times the take-up rates for policies by sector as determined by Marsh Analytics each year and used by the GAO in a May 2021 report (GAO 2021). The dataset also includes indicator variables denoting if the firm is large

with more than 500 full time employees (FTE500), public or private (PUBorPRIV), and whether it is non-profit or for-profit (NPFP).

The literature review discusses how cyber insurance, in theory, can incentivize the insured to invest in their own cybersecurity through insurer premium discrimination and other mechanisms – clients that invest in their own cybersecurity are rewarded with lower premiums and better terms and conditions. Conversely, some scholars argue that cyber insurance can cause a moral hazard problem where clients, knowing they are insured, behave recklessly and actually reduce their investment in self-protection, believing insurance will offset any cyber-attack losses. For example, evidence suggests that cyber insurance covering ransomware attacks makes it more likely victims will pay the ransom, and hackers will target clients with insurance for that reason. The literature and data from HCAD also suggests that certain types of healthcare entities might benefit more from cyber insurance than others. It is hypothesized in this dissertation that small healthcare sector firms with less than 500 employees might benefit more from cyber insurance safety incentives than larger firms. Further, many public sector entities (e.g. government) fully or partially self-insure. Thus, it is hypothesized that private for profit firms are more likely to be influenced by cyber insurance than public non-profit/not for profit entities. Based on the above description, the following hypotheses will be tested:

H1: Cyber insurance will have a small but significant impact on reducing the frequency & magnitude of cyber-attacks against healthcare sector entities

Given the growth in the number of cyber-attacks over the period 2015 to 2021, it is not unexpected that cyber insurance might have a negative impact on the frequency and

magnitude of cyber-attacks for some firms under certain circumstances such as ransomware attacks.

H2: Cyber insurance will have a more significant impact on reducing the frequency & magnitude of cyber-attacks against small private healthcare firms vs. large and/or public-sector entities

Small healthcare firms include individual practitioners such as doctors and dentists, most group practices, and business associates including administrative, suppliers, and diagnostic testing companies (e.g. labs, imaging, etc.). Large healthcare entities include health systems, insurers, hospitals, and those operated by local, state, and federal governments.

H3: Cyber insurance will have a more significant impact on reducing the frequency of non-ransomware and internal cyber-attacks than on ransomware and external hacks.

We test our hypotheses empirically using Poisson regression and negative binomial regressions. The descriptive statistics for these regressions is given in Appendix G.

The ***Attacks*** count data is Poisson-distributed with values each year ranging from zero to five. The first set of models was conducted using, if appropriate, ***xtpoisson*** with fixed-effect (FE), random effect (RE) and the "pooled" xi: Poisson models, with normal and robust standard errors (SE). In these models the sign (+/-) of the coefficients is of particular interest indicating if insurance significantly increases (+) or decreases (-) the log likelihood of ***Attacks*** holding other variables constant. Where appropriate the Hausman test was run to determine if FE or RE is most appropriate. For many of the models the indicator variables used are time invariant, making FE inappropriate. Models are run using with INSPOL10K, with combinations of FTE500, PUBorPRIV, NPFP, and various SUBCODES above to test Hypothesis #1 and Hypothesis #2.

Models were also run with EXTHACK and RANSOM to test Hypothesis #3. Running the models with robust standard errors controls for heteroscedasticity. Where appropriate, the Pearson Goodness of Fit (estat gof) and Variance Inflation Factor (estat vif) tests were run to test for model appropriateness and multicollinearity. Tests were also run for serial autocorrelation.

A series of regression analyses was then conducted to test the influence of insurance (*INSPOL10K*) on the dependent variable for magnitude of cyber-attacks (*AttRec*). The *AttRec* count data is over dispersed and it was determined that xtnbreg would be a more appropriate modelling technique to use. All models were run using xtnbreg with fixed-effect (FE) and random effect (RE). Once again, in these models, the sign (+/-) of the coefficients is of particular interest indicating if insurance significantly increases (+) or decreases (-) the log magnitude of attacks holding other variables constant. In all models the Hausman test was then conducted to determine if FE or RE is most appropriate. All models are run using INSPOL10K, with combinations of FTE500, PUBorPRIV, NPFP, and various SUBCODES to test Hypothesis #1 and Hypothesis #2 for attack magnitude as measured in records compromised. Where appropriate, test were then run to test the model's goodness of fit, for multicollinearity, and for serial autocorrelation.

The regression results are presented using formatted Stata tables with variable coefficients, standard errors, and other relevant data, starred where significant. Other data from HCAD-R (Appendix B), HCAD-L (Appendix C), and NAIC are presented in tables and graphs throughout the case study with descriptive discussion. There are also appendices describing the coverage (Appendix D) and risk management (Appendix E) of

key healthcare cyber insurers, and comparing insurer performance over the period 2016 to 2020 (Appendix F).

III. Conclusion

The next three chapters use the methodologies and research design described above to look at the role that insurance plays in promoting safety and managing risk in the realms of commercial nuclear power (Chapter 4), hazardous waste management (Chapter5), and healthcare cybersecurity (Chapter 6).

Chapter 4: Insurance as a Private Sector Risk Regulator & Promoter of Safety: Managing Risk at U.S. Commercial Nuclear Power Plants (Case Study)

I. Introduction

How has insurance promoted better safety in the commercial nuclear power industry and what lessons learned can be applied to other emerging technological risk regimes? This case study examines the role that insurance plays in helping to regulate, promote safety and manage risks for firms operating reactors at nuclear power plants (NPPs) in the U.S.

During the 1950s, commercial nuclear power generation was considered an ultra-hazardous activity with great uncertainty regarding the frequency and consequences of catastrophic accidents. For this reason, nuclear risk was initially considered "uninsurable" by lawmakers and insurance industry executives. However, given the strategic importance of the development of the "peaceful" uses of atomic power, in 1957 Congress passed the *Price-Anderson Nuclear Industries Indemnity Act* (P.L. 85-256 1957) that, with the collaboration of insurers and nuclear operators, established a nuclear insurance regime that has endured to the present day.

The key finding of this case study is that throughout the entire history of commercial nuclear power generation in the United State, insurance is a key variable in explaining the safety behavior of operators, regulators, and other institutions in managing nuclear risk, without which the industry, as we know it, might not exist. Further, the definition of

nuclear safety and the role of insurance in managing behavior changed over time, influenced significantly by major events.

Evidence presented in Section VII demonstrates the relationship between safety and insurance, using insurance liability and property premiums, and key measures of safety from the Nuclear Regulatory Commission (NRC), Institute of Nuclear Power Operations (INPO), and from nuclear insurance pools including American Nuclear Insurers (ANI) and Nuclear Electric Insurance Limited (NEIL)

The organization of the remainder of this case study is as follows. Section II describes the early history of the US commercial nuclear power industry prior to the enactment of the Price-Anderson Act, and the regulatory and insurance regime that developed to support their activities. Section III provides an overview of the political economy, risks and uncertainties related to the commercial nuclear power generation, and safety protections. The case study will then trace the process of nuclear insurance development and the evolution of nuclear safety through the lens of the Price-Anderson Act, including first enactment term (Section IV), and subsequent renewal periods (Section V and VI). Section VII continues with the current nuclear insurance coverage and safety roles of ANI and NEIL, and the U.S. government. It includes evidence on how insurers incorporate INPO indices, ERF, and NRC risk factors to calculate premiums and manage client safety behavior. Sections VIII and IX then conclude with an analysis of the question "How has insurance promoted better safety in the commercial nuclear power sector?" looking at how the lessons learned from this case study can be applied to future technological risk regimes.

II. Background Period before Price-Anderson Act (1946 –1957)

This section describes the period from just after World War II, including the political environment, secrecy concerns, desire to develop "peaceful uses" of nuclear energy including the generation of nuclear power, and the formation of the institutions to oversee this transition. It also includes initial concerns about the frequency and magnitude of a catastrophic accident, and the debate on creating nuclear insurance to protect power companies from liability.

A. Early Legislation and Regulation

Following World War II, the US military via the Manhattan Project had a monopoly on the ownership of nuclear materials and the technology needed for its production and use. However, there was a desire by Congress to capitalize on the Manhattan Project's $2 billion investment through the promotion of the peaceful uses of the atom, and by the scientific community to demilitarize the nuclear energy program and turn it over to civilian control. Still, on the eve of the Cold War, there were grave concerns that "atomic secrets" needed to be protected and nuclear materials needed to remain in government hands.

The result of this debate was the passage of the ***Atomic Energy Act of 1946*** (P.L. 79-585) that transferred control of the Manhattan Project to a newly-created civilian agency – the *Atomic Energy Commission* (AEC) – but banned the foreign transfer of nuclear technology and severely restricted private-sector use. The act also established the *Joint Committee on Atomic Energy (JCAE)*, a permanent joint committee of the US Congress responsible for oversight of the AEC, and with exclusive jurisdiction over "all bills,

resolutions, and other matters" related to civilian and military aspects of nuclear power. The AEC's primary purpose was to promote peacetime research and development of atomic energy. It was also given the power to issue licenses and to establish nuclear safety regulations. This conflicting role of being both the promoter and regulator of nuclear power would plague the AEC until its dissolution in 1975.

On December 20, 1951, at the AEC's National Reactor Testing Station in Arco, Idaho a small reactor known as Experimental Breeder Reactor No. 1 (EBR-1) produced the first electricity from atomic energy, enlightening four 200-watt light bulbs using steam generation. The test was a proof of concept for much larger and more powerful commercial NPPs to come.

However, a little less than a year later, on December 12, 1952, a less positive proof of concept occurred. On that day, a partial meltdown of the NRX reactor core at Chalk River, Ontario, occurred. The accident, which fortunately happened while the reactor was at low power, was caused by operator error compounded by a failure in the control rod safety systems (Jedicke 1989). While no one died or was seriously injured, some personnel were exposed to high levels of radiation which may have caused them future adverse health effects.

By the time Eisenhower had become president in January 1953, the atomic energy world had drastically changed. In 1948 the Soviet Union successfully tested its first atomic bomb; in 1952 the US successfully detonated the first full-scale thermonuclear device; the Cold War nuclear arms race was well underway; and America was immersed in the McCarthy-era Red Scare. Under this cloud of fear and uncertainty, the Eisenhower

administration decided on a dramatic shift in US policy from near-absolute atomic secrecy to a new strategy of openness where nuclear research was shared with other countries and private industry.

Soon after entering office, Eisenhower launched "Operation Candor," a public relations campaign with the express goal of explaining to the American public the risks and rewards of nuclear energy and the perils of the atomic age (White House July 1953). A key component of the campaign was a speech by Eisenhower to the UN General Assembly on December 8, 1953 entitled "Atoms for Peace" outlining a plan for the peaceful, controlled distribution of nuclear technology to all the countries of the world in exchange for agreement not to pursue atomic weapons (White House December 1953). The speech has been described as a "canny" strategy to promote the atom's peaceful uses while allowing the U.S. to develop more powerful atomic weapons – a propaganda move "aimed at winning hearts and minds before the Soviet Union could introduce a similar program" (Hicks 2014). In his speech, Eisenhower also proposed the creation of a new international agency to monitor nuclear proliferation, develop safety standards, and regulate trade in nuclear materials and technology. The ultimate result was the formation of the *International Atomic Energy Agency* (IAEA) in 1957.

On August 30, 1954, less than a year after the Atoms for Peace speech, Congress amended the Act of 1946 by passing the ***Atomic Energy Act of 1954*** (P.L. 83-703 1954) which ended the US government monopoly on atomic energy and for the first time allowed for a privatized nuclear energy industry. Section 103 of new Act gave the AEC authority to issue commercial nuclear licenses to private facilities "who are equipped to

observe and who agree to observe such safety standards to protect health and to minimize danger to life or property as the Commission may by rule establish." This included issuing construction permits and operating licenses to facilities for the generation of commercial power. Further, one of the conditions of licensure was that "the licensee will hold the United States and the Commission harmless from any damages resulting from the use or possession of special nuclear material" (Section 53e.8).

Under the *Atomic Energy Act of 1954*, private entities could now construct, own, and operate nuclear reactors for electric power production, subject to a strict AEC licensing regime. However, during hearings on the new atomic law, Francis McCune of General Electric first raised the issue of private sector liability and the need for insurance. He noted that the inability of private companies to acquire adequate insurance could be a serious roadblock to the growth of the atomic industry. He believed that private companies should acquire some nuclear hazards insurance from private insurers, but that the federal government should make some provisions for insurance above the limits available from private insurers in order "to protect both industry and innocent people against the kind of catastrophe we hope will never come" (JCAE 1954:335)

B. Concerns about a Catastrophic Accident - WASH-740 "Brookhaven Report"

In July 1956, the AEC enlisted the services of a group of scientists from the Brookhaven National Laboratory (BNL) to conduct the first comprehensive study of the theoretical likelihood and consequences of a major accident at a typical large nuclear power reactor. BNL would study a hypothetical 500 Mw reactor located about 30 miles from a major city. The postulated accidents would be timed to occur when the reactor's

fission product inventory would be at its maximum (USAEC 1957: 7). BNL explored three types of potential reactor accidents that could result in release of radioactive materials. The first was a "nuclear runaway" when the reactor becomes supercritical and all safety instrumentation fails. This can result in a core meltdown or vaporization of fuel elements and the release of fission products (USAEC 1957: 18). The second was a Loss of Coolant Accident (LOCA) caused by a break in the primary coolant circulating system or from a rupture of the reactor vessel. The third accident was a violent chemical reaction resulting in an explosion causing a containment rupture (USAEC 1957: 18).

Based on the three types of accidents, the estimates indicated that casualties might range from a lower limit of no injured or killed to an upper limit of about 3,400 killed and 43,000 injured. Theoretical property damages ranged from a lower limit of $500,000 to the worst case of about $7 billion. This latter figure was largely due to assumed contamination of land with fission products. For most scenarios, the total losses did not exceed a few hundred million dollars (USAEC 1957). Still, the maximum hypothetical property losses far exceeded the envisioned property insurance coverage, and did not include an estimate of liability compensation.

While the report generated alarmingly high consequences for a worst-case accident scenario, it was unable to estimate realistic probabilities since there was no methodology to do so. The report started out optimistically stating "experts all agree that the chances that major accidents might occur are exceedingly small" and "there will be few reactor accidents and that such as do occur will have only minor consequences" (USAEC 1957: vii). However, the major accident probability estimates ranged widely from one in

100,000 to one in a billion per year for each large reactor (USAEC 1957: viii). Some of the experts refused to give a number because they believed such estimates were "unknowable" (USAEC 1957: 5).

C. Formation of Insurance Pools & Initial Primary Nuclear Insurance Coverage

On February 1, 1955, less than six months after the enactment of the *Atomic Energy Act of 1954*, William Mitchell, the General Counsel of the AEC told the JCAE that "damages from a major [nuclear] accident, if one should occur, might well be beyond the capacity of most companies and communities to handle and cannot now be fully covered by insurance" (JCAE 1955: 59). The following month, at the request of the JCAE, the AEC established the Insurance Study Committee, a group of leading insurance company executives to study the feasibility of nuclear insurance and to make appropriate recommendations (Paulding 1967). The Committee released its final report in March 1956 (USAEC 1956), concluding that the nuclear liability risk was insurable, but only through nuclear insurance pools, spreading the risk of a small number of exposure units (i.e., reactors) over a large number of insurance companies.

In May 1956, three insurance risk pools were formed to provide nuclear industry coverage - two for liability coverage and one for property coverage. The first was *Nuclear Energy Liability Insurance Association (NELIA)* composed of 135 stock insurance companies offering protection against radiation liability hazards arising out of nuclear reactor operations. Each member company had a minimum coverage commitment of $25,000, with a total pool coverage capacity of $46.5 million (NELIA 1956: 3). The second liability pool was *Mutual Atomic Energy Pool (MAEP)* consisting

of two mutual companies - a primary underwriting syndicate, *Mutual Atomic Energy Liability Underwriters (MAELU)* which was reinsured by the *Mutual Atomic Energy Reinsurance Pool (MAERP).* The combined pool was comprised of 105 mutual insurance companies and had a total liability capacity of $13.5 million (AMRC 1956). This brought the total nuclear liability coverage offered by NELIA and MAEP to $60 million. Finally, a third pool was formed, *Nuclear Energy Property Insurance Association (NEPIA)* comprised of 189 stock insurance companies offering nuclear facility property coverage. This pool had a total insurance capacity of $65 million. Thus, the total nuclear coverage offered by the private sector in 1956 was $125 million spread over nearly 400 US insurance companies - the largest coverage amount ever offered in the United States (JCAE 1960: 529).

As part of their formation, the pools also developed a "specialized loss-prevention and inspection service which we have regarded as an absolute requirement for the protection of the public, the Government, and of our own companies" (JCAE 1960: 530). The casualty companies employed and trained a number of health physicists and engineers in nuclear problems, and also trained other scientists in radiation detection and safety. In addition, pool inspectors worked with facility operators to prevent damage to facilities, injuries to employees and to the persons and property of the public. They also cooperated with the AEC in enforcing its safety regulations. As a result, the pools gave operators of insured nuclear facilities inspection and loss-prevention services that they would find difficult, if not impossible, to get anywhere else.

For example, 90 years prior to these hearings, the Hartford Steam Boiler Inspection and Insurance Company (HSB) was founded – becoming "the first company in America devoted primarily to industrial safety" (MunichRE 2016). HSB developed the "Hartford Standards" that quickly became the specifications for boiler design, manufacture and maintenance. Not surprisingly, since boilers are a major component of reactors, HSB engineers were involved in the inspection of early nuclear reactor pressure vessels during the 1950s (White 1957), and continuing to the present day. Per MAERP chairman Hubert Yount: "Such services are part of the modern concept of insurance which includes not only the acceptance of risk of loss, but the prevention and control of loss" (JCAE 1960: 531).

However, despite the unprecedented amount of coverage, insurers, plant operators, and Congress realized that if a catastrophic accident occurred, it was likely not enough. Recognizing this dilemma, the nuclear industry's Atomic Industrial Forum formed an Atomic Insurance Committee (AIC), and contracted with Columbia University to conduct a study on the nuclear insurance problem. In its report the AIC concluded that "the magnitude of the risk is such that the potential liability cannot be covered by private insurance alone," and that "the financial protection problem calls for the establishment of some program by the national government" (Murphy 1957: 43). The report then recommended that Congress adopt a nuclear indemnity program outlined in a bill introduced by Sen. Clinton Anderson (D-NM).

III. Political Economy of Nuclear Power in the 1950s

This section discusses the political economy of nuclear power in the 1950s. It includes a brief overview of the benefits and costs of nuclear power, as well as the vulnerabilities, threats, and risks to nuclear reactors, and the measures employed to assure safety.

A. Benefits & Costs of Nuclear Power

Both the Atomic Energy Act of 1954 and Eisenhower's Atoms for Peace speech envisioned a variety of medical, industrial and other peaceful uses for nuclear energy where "this greatest of destructive forces can be developed into a great boon for the benefit of all mankind" (Eisenhower 1953). Foremost among these beneficial uses was "to provide abundant electrical energy in the power-starved areas of the world." AEC Chairman Lewis Strauss predicted in 1954 that electricity produced by commercial NPPs could become "too cheap to meter" (Strauss 1954). However, from the viewpoint of the US Government, the most important benefit of the peaceful uses of atomic energy was as a propaganda vehicle in the Cold War against the Soviets. As such, nuclear power was so vitally important to national security, US prestige and the public interest that its development and use superseded any costs and concerns, including public safety.

During the mid-1950s, there was limited knowledge on what it would cost to design, build and operate a commercial nuclear power generation facility. To solve this problem, the AEC invited four private sector consortiums[3] to submit proposals in a competition to design a nuclear plant that could both produce commercial electricity and also plutonium

[3] These four groups were: Commonwealth Edison Company and Public Service Company of Northern Illinois; Dow Chemical Co. and Detroit Edison Company; Monsanto Chemical Company and Union Electric Company; Pacific Gas & Electric Company and Bechtel Corporation.

that could be sold to the AEC for nuclear weapons. The declassified results were published in May 1953 (USAEC 1953).

A variety of different reactor types were proposed by the participants. The Con Edison consortium estimated that the construction costs for their 225 Mw capacity heavy-water-cooled reactor and plant to be $118 million (USAEC 1953: 62-63). This was substantially higher than for a conventional fossil fuel plant. The Monsanto proposal estimated costs based on the amount of electricity generated ($ per Kw), comparing the results to coal burning plants. While the cost of electrical generation was similar between nuclear and coal, the group was quick to note that coal plants have a "long history of safe operations" while there is "insufficient data to estimate the actual hazard to the workers or the public of such a plutonium-power-plant" (USAEC 1953: 62-63). Consequently, they did not include costs for liability insurance in their estimate.

B. Reactor Design, Vulnerabilities, Threats and Risks

Today, 85% of the world's nuclear electricity is generated from two reactor types developed in the 1950s – the pressurized water reactor (PWR) and the boiling water reactor (BWR) (World Nuclear Association 2018). Both types of reactors use water as a coolant and moderator, to slow the atomic reaction. A nuclear power plant consists of one or more nuclear reactors fueled primarily by enriched uranium arranged in tubes to form fuel rods, inserted into fuel assemblies in the reactor core. The more fuel assemblies in the core, the higher the reactor's power rating; and the higher the potential consequences of a nuclear accident.

All US commercial reactors are housed in an airtight, steel or concrete containment structure designed to protect those outside from the accidental release of radiation, and to guard the reactor from outside attack. In addition to the containment structure, nuclear plants are also equipped with multiple redundant safety systems to prevent and mitigate accidents. This includes systems to quickly shut down the reactor, stop the chain reaction, continue cooling, and monitor safety.

Since the 1950s, the biggest concern for nuclear reactors has always been the remote possibility of a core meltdown coupled with a loss of containment leading to a large early release (LER) of radiation to the nearby community. The most likely cause of a meltdown is a loss-of-coolant accident (LOCA) where the liquid used to cool a reactor core is lost. Threats that can exploit vulnerabilities and initiate LOCAs and other plant accidents can come from either internal or external sources. Internal threat sources include mechanical failures, internal fire or flooding, gas leaks, and accidents resulting from human operator error or sabotage. External threat sources include power blackouts, loss of service water, earthquakes, tsunamis, flooding, wind-events, accidental airplane impacts, and deliberate human attacks.

The *Atomic Energy Act of 1954* defines a “nuclear incident” as "any occurrence within the United States causing bodily injury, sickness, disease, or death, or loss of or damage to property, or for loss of use of property, arising out of or resulting from the radioactive, toxic, explosive, or other hazardous properties of source, special nuclear, or by-product material” (Section 11.q).

A radioactive release poses both individual and societal risks to public health and safety. Individual risks include the possibility of early fatalities, injuries and illnesses; as well as the potential for delayed or long-term "latent" health effects such as birth defects and deaths from radiation induced cancers. Since the evidence of harm is often not contemporaneous with exposure, it is often difficult to establish a causal link between the release of radiation and latent health effects. Further, cancers can be caused by multiple factors including smoking, diet and alcohol consumption, more likely linked to the disease than radiological exposure. Thus proving radiation from a nuclear plant is the sole cause of cancer versus other risk factors is virtually impossible. From a societal risk standpoint, a nuclear incident could cause a major disruption to the economy, and possibly irreversible damage to the environment. The economic impact could depend on factors such as population density, property values, and types of businesses that might be disrupted. The level of environmental damage and casualties would in turn depend on a series of unpredictable factors including the amount of fission products released, the weather conditions, and the geographic characteristics of the area where products are dispersed,

Victims expect to be compensated if they are harmed by a nuclear accident. In the US, state courts generally have jurisdiction over civil liability arising out of hazardous activities. State tort laws can vary considerably. Most require proof of fault and causation, and many entities can be held liable for an accident causing harm. As a result, liability compensation can be unpredictable. The radioactive cloud could drift across state and even international borders, creating the possibility of liability lawsuits in multiple

jurisdictions. Since state laws regarding nuclear liability were totally undeveloped, this left open the possibility that plant operators and other related parties could be held financially responsible for unlimited third-party damages. Thus, in 1954, liability problems were a major roadblock to commercial nuclear power development.

C. Defense-in-Depth, Design-Based Accidents and AEC Definition of Nuclear Safety

Much of the knowledge and experience of nuclear reactor safety in the 1950s evolved from the Manhattan Project and the expertise developed by chemical giant DuPont. In October 1942, DuPont was contracted to design and build a plutonium production plant. The location criteria required that the site be a minimum of 225 square miles and that no one be allowed to live within four miles of the facility for fear of a radioactive accident (Atomic Archive 2020). Subsequently, DuPont engineers decided that a site near Hanford, Washington best met the criteria, and soon after began construction of the Hanford Engineer Works, codenamed Site W (Atomic Archive 2020). Using their experience in designing other types of hazardous chemical production facilities, the engineers separated the reactor design into smaller, independent sub-systems and froze those designs early so that dependent systems could be designed around them.

This design concept evolved into the nuclear safety doctrine of "defense-in-depth," with multiple independent 'barriers' to prevent the release of radioactivity into the environment, and minimize the likelihood and consequences of an accident (Keller and Modarres 2005: 272). This defense-in depth philosophy required: 1) high quality "fail

safe" design with large safety margins to reduce the likelihood of malfunctions, 2) multiple automatic backup systems, 3) plant operation within predetermined safe design limits; and 4) continuous testing, inspections, and maintenance to preserve original safety design margins (Keller and Modarres 2005: 272-273).

The plant was surrounded by a population exclusion zone calculated using a plant isolation formula based on the reactor's rated power:

$$\textbf{Exclusion Area (miles)} = .01\sqrt{\textbf{Plant Power (Kw)}}$$

Thus, the 250,000 Kw Hanford B reactor required a 5-mile exclusion area (USNRC 2016: 7).

Due to the lack of quantitative data, the defense-in-depth safety margins were calculated using a deterministic qualitative approach based on engineering judgement. To test the reliability of the defense-in-depth concept, engineers used design-basis accidents (also called maximum credible accidents) to measure the effectiveness of barriers and systems and ensure plant safety. Using design-basis accidents, engineers postulated a number of "credible" plant events, such as a loss of offsite power, which could initiate an event or series of events leading to an accident.

Thus in the 1950s, the AEC came to define "nuclear safety" as the ability of the reactor to withstand a fixed set of prescribed design-basis accident scenarios qualitatively judged by experts as the most credible events that could occur in NPP operations (Keller and Modarres 2005).

IV. Initial Private Nuclear Insurance & The Price-Anderson Act

This section reviews the initial private sector pool coverage, including premium determinations, the Price-Anderson Nuclear Indemnity Act and the insurance framework that it helped establish, including the authorization of a $500 million government "backstop" indemnity, and the requirement that all commercial nuclear power plants have liability coverage consisting of the backstop and the maximum amount of primary coverage from the pools.

A. Initial Primary Insurance Risk Factors, Policies & Premium Determination

With the establishment of the nuclear pools and the maximum primary liability insurance capacity at $60 million, insurers next focused on determining the key risk factors, policy terms, conditions, and premium rates for various types of nuclear facilities (JCAE 1957: 119). The challenge for the bureaus was to develop "fair premiums" that covered ordinary losses and expenses, permitted the accumulation of reserves for catastrophic losses, and also provided a reasonable profit margin for pool participants (JCAE 1960: 531).

Each reactor was rated based on its individual characteristics. Early nuclear liability policies considered four key individual reactor risk factors for determining premiums: 1) type of reactor and containment 2) use, 3) power level, and 4) location and proximity to populations. These factors were used to determine a "base rate" for the first $1 million of coverage. After setting the base rate, the charges for additional millions were arrived at as percentages of this base premium. Estimates for early power reactors (Table 4.1) including Dresden #1, Indian Point #1, Elk River and Yankee Row showed that power

and population proximity were the primary risk factors considered in calculating premiums.

Table 4.1: Initial Premium Estimates – Early Commercial Reactors (JCAE 1957: 121)

Reactor	Dresden # 1	Indian Point #1	Elk River*	Yankee Rowe
Start Date	9/28/1959	3/26/1962	11/6/1962	12/23/1963
Reactor Type & Containment	BWR-GE (MARK 1)	PWR-B&W	BWR-AEC	PWR-WEST
Operating Power (Thermal Mwt)	700	585	58	600
Population within 10 miles	67,379	308415	0	0
Required Coverage	$60,000,000	$60,000,000	$17,550,000	$60,000,000
First $1 million (base)	$40,000	$40,000	$14,600	$20,000
Next $4 million (50% Base/$mil)	$80,000	$80,000	$29,200	$40,000
Next $5 million (20% Base/$mil)	$40,000	$40,000	$14,600	$20,000
Next $10 million (10% Base/$mil)	$40,000	$40,000	$11,023	$20,000
Next $20 million (5% Base/$mil)	$40,000	$40,000	$0	$20,000
Next $20 million (2.5% Base/$mil)	$20,000	$20,000	$0	$10,000
Estimated Initial Premium (1956)	$260,000	$260,000	$69,423	$130,000
Actual 1966 Premium	$233,000	$266,500	$0	$125,000
Estimated 10-Year Return Premium	$171,600	$171,600	$0	$85,800
Est. Government Indemnity Payment ($30/Mw/Yr.)	$21,000	$17,550	$1,740	$18,000
*Elk River was built under the second phase of the AEC's PRDP program, and became exempt from financial protection requirements (see p. 24)				

For example for a 600 Mw BWR, fully contained, located in a high value agricultural area, the base rate for the first $1 million of coverage would be $40,000, and the "provisional" annual premium for $60 million worth of coverage would be $260,000 (JCAE 1957: 87). The goal was to build up reserves quickly in case a catastrophic accident. The premium was "provisional" because a proportion of premium received was set aside in a reserve fund. For large risks such as commercial nuclear reactors, the proportion reserved was a maximum of 75 percent. These reserve funds would be used only for the payment of losses and loss expenses over a period of 10 years. Under an industry credit rating plan, during the 11th year, if the losses and loss expenses incurred (including reserves for unpaid losses and expenses) during the 10-year period were less

than the total 10-year deposits in the reserve fund, a refund would be made to first-year policy holders (JCAE 1960: 531). This procedure would be repeated annually so long as the rating plan remained in effect. Thus, through this plan, the policyholders could be rewarded annually with return premiums for safe behavior resulting in less than expected losses. During the first 10 years of coverage, no major liability claims were filed, and beginning in 1967, the pools began to reward policyholders with premium returns averaging 67 percent of the premium paid 10-years prior rising to nearly $1.4 million in returned premiums in 1973 (USAEC 1974: 7).

The bureaus also developed a standardize nuclear energy liability policy form outlining coverage terms, conditions, and exclusions (JCAE 1957: 100-107). The liability insurance covered any entity that might be liable for a loss. This included not only the reactor operator, but also plant designers and builders, equipment suppliers, the fuel fabricators, and even any outsider whose negligence result in damage. Each policy was written per reactor/reactor site, and the limit of insurance indemnity ($60 million) was for the lifetime of the installation.

Coverage was only for 3rd party bodily and property damage, and did not cover damage to the insured's property or liabilities covered by other insurance. The pools had the right to inspect the facility at any time (USAEC 1960: 12), examine the insured's records, and could suspend coverage should an engineer or inspector discover a dangerous condition with respect to a machine or vessel, and the insured did not comply with a request to take such vessel or machine out of service for correction. Given that some insurers were considered experts in the inspection of boilers, they participated in

the development of standards for the in-service testing of reactor structures under radiological conditions, and were sometimes invited by the AEC or the licensee to inspect nuclear boilers and provide recommendations on their safe operation (McClure 1968).

Likewise, the nuclear property insurance pool, NEPIA established the Nuclear Insurance Rating Bureau and developed an "all risk" policy to cover first party direct property damage to nuclear facilities not only from the nuclear hazards, but also conventional perils such as fire, vandalism, and normal power plant boiler and machinery exposures (McClure 1968: 112). The policy did not cover damage and bodily harm to third parties outside of the plant property. Thus, "all-risks" were contained within the insured property and, unlike third-party liability, these risks were considered "determinable" based on the replacement value of the assets.

For calculation of the annual premium, the ratings bureau came up with a formula starting with the standard rates for the fire and other property perils of a conventional steam plant, with a significant adder for the nuclear hazard factoring in reactor type, use, power level, and containment. The nuclear hazard adder resulted in a cost for nuclear power plant property insurance that was more than 250 percent higher than for conventional steam plants.[4] In addition, similar to other types of property insurance, NEPIA's policy had a 10 percent coinsurance requirement, as well as a negotiable deductible. Thus, with a claimable event, the insured would be responsible for up to 10% of the coverage maximum plus an additional cost for the deductible. This could

[4]An example given by NEPIA during 1957 hearings was for a 600 Mw plant with premium of $198,000 per year for $40 million worth of property insurance vs. $74,000 per year for a conventional plant. The composite rate was $0.495 for each $100 of property coverage of which $0.315 was to cover the nuclear hazard (JCAE 1957 pp. 141-142).

incentivize owners to adopt safety measures in order to avoid costly copay and deductible expenses.

Thus by 1957, the insurance pools had come up with processes for determining rates for the limited amount of first-party and third-party insurance coverage they were willing to make available. However, it was also clear that the amount of liability insurance available from private insurers was considered inadequate, and that the government needed to provide additional indemnity to cover losses in the event of a catastrophic accident.

B. Price-Anderson Act of 1957 Debate & Passage

The government indemnity was a hot topic of debate during the 84th Congress 2nd session. This importance was underscored by the fact that during this session, no less than five indemnity bills were introduced. Ultimately only one pair of bills H. R. 12050, introduced by Rep. Melvin Price (D-IL), and S.4112, introduced by Sen. Clinton Anderson (D-NM) — collectively called the Price-Anderson bill - was reported out after JCAE hearings in July 1956 (JCAE 1956).

During the bills debate, controversy arose regarding the granting of a construction license to the Power Reactor Development Company (PRDC) to build a new type of commercial reactor – a breeder reactor – at a site in Laguna Beach, Michigan. The proposed PRDC breeder was of the same type of reactor as the EBR-1 that first generated electrical power. But, on November 29, 1955, EBR-1 suffered a partial meltdown – raising concerns that the fast breeder reactor design was unsafe (Mazuzan and Walker 1984: 127-128). Given this controversy leading into the 1956 election season, the

decision was made not to call up the Price-Anderson bill during the 84th Congress (Mazuzan and Walker 1984: 120-121).

In January 1957, Price and Anderson reintroduced their bills respectively to the House and Senate, and hearings were scheduled for late-March. During the first day of JCAE hearings, extensive discussions took place on the Brookhaven Report and the need for government indemnity protection. AEC Chairman Lewis Strauss testified in detail about the Brookhaven Report findings. He noted "the chances of a person being killed in any one year by a reactor accident would be less than 1 in 50 million." However, despite the "exceedingly small" chances of a major accident, he urged that "indemnity legislation to safeguard against even the small contingency of a reactor accident be passed during this session" noting that "public will and public confidence would be strengthened by this protection" (JCAE 1957: 13).

During the hearings, the cost for the $500 million government indemnity was debated, eventually being set at $30 per year per megawatt of thermal energy (MW_{th}). Thus, the annual government indemnity premium would be $21, 000 for Dresden 1 (700 MW_{th}), a reactor then under construction. Testimony by Francis McCune, vice president at General Electric brought the issue of government indemnity to the forefront. McCune announced that if indemnity legislation did not pass in Congress during the current session that all work by GE on Dresden I would be halted. He then went on to state that "I don't believe there will be any market for the civilian products of atomic energy unless the liability problem is solved" (JCAE 1957: 148).

The JCAE voted the bill out of committee on May 9, 1957. With no opposition in the Senate, and little debate in the House, the Price-Anderson Act, amending the Atomic Energy Act of 1954 was signed into law on September 3, 1957 with the following key insurance provisions:

1. **Mandatory Coverage:** All licensees as a condition of all licenses issued between August 30, 1954 and August 1, 1967 would be required to have financial protection.

2. **Required Indemnity & Premium Payment:** The government would provide up to $500 million in indemnity to cover all reasonable costs associated with a nuclear incident including investigating and settling claims and defending suits for damage. All licensees would be required to sign an indemnity agreement and pay annual premium of $30 per Mw.

3. **Maximum Coverage:** All licensees operating facilities with a rated capacity of 100 Mw or more were required to have the maximum amount of financial protection available from private sources. Such financial protection could include private insurance, private indemnities, self-insurance, other proof of responsibility, or a combination of such measures.

4. **Limit of Liability:** The aggregate liability for a single nuclear incident shall not exceed the sum of the $500 million indemnity together with the amount of private financial protection ($60 million) required of the licensee or contractor (total liability capped at $560 million).

V. First Eighteen Years of Price-Anderson Act (September 2, 1957- December 31, 1975)

This section discusses the US commercial nuclear power industry and nuclear insurance during the first eighteen years of the Price-Anderson Act. As originally enacted, the Price-Anderson Act was considered temporary legislation with the indemnity only applying to licenses issued through August 1, 1967. Yet in 1967, Congress renewed the Act and indemnity for another 10 years covering new licenses through 1976. During this period, the commercial nuclear power industry grew but initially at a much slower

pace than anticipated, sparking controversy between private nuclear insurers and the AEC. Several nuclear accidents in the US resulted in property damage and casualties requiring primary insurance compensation. . However, no liability claims were made requiring Price-Anderson indemnity coverage. New risk assessment techniques were developed to more quantitatively assess the probability and consequences of a nuclear accident. Further, with renewals of the Price-Anderson Act in 1967 and 1976, major changes were made to private insurance and the indemnity, transferring more of the nuclear accident risk to operators, making them internalize more of the social costs.

A. Initial "Commercial" Nuclear Power Growth and Pool Insurance Concerns

When the insurance industry established the nuclear liability and property pools creating an unprecedented amount of coverage, they did so with the expectation that many new large-scale private NPPs would be built. They planned to put 70 percent of expected premiums into pool reserves (McClure 1968: 292), thus having sufficient funds readily available to cover at least one significant loss event. Soon after the Price-Anderson Act passed, the liability pools also agreed to administer the government indemnity, handling claims if needed (McClure 1968: 276). However, the anticipated post-enactment nuclear boom didn't immediately happen. The main reason was a government initiative known as the Power Reactor Demonstration Program (PRDP).

The first stage of the PRDP was announced by the AEC in January 1955. Under the PRDP initiative, the AEC partnered with power companies to promote nuclear power research and development, drive nuclear plant design and construction, and demonstrate the economic benefits of nuclear power generation. The Atomic Energy Act of 1954

Section 169 specifically forbade the AEC from subsidizing the construction or operation of licensed nuclear power facilities "except under contract or other arrangement entered into pursuant to section 31" – dealing with "Research Assistance." Under the first stage of PRDP, the AEC provided R&D funds, waived fuel charges, provided other technical support, and also provided assumed legal liability. Thus PRDP plants did not require coverage from the nuclear pools.

In 1953, the AEC had already agreed to partner with Duquesne Light to build a 60 Mw "commercial" nuclear power plant at Shippingport, Pennsylvania along the Ohio River, 26 miles northwest of Pittsburg. Duquesne agreed to furnish the site, provide a staff to operate the plant, construct and maintain the conventional electric generating plant, contribute $5 million to the reactor section of the facility, and purchase the steam produced by the AEC-owned reactor. The AEC agreed to finance 90% of the reactor costs, build the reactor plant, supervise all nuclear operations, and assume legal liability for it (Beaver 1987: 346). Thus when Shippingport became the first commercial U.S. nuclear power plant to generate electricity in December 1957, it was operated and insured by the federal government

The first and second phases of the PRDP included smaller utilities that could not afford to finance and operate a reactor themselves. In these projects, the AEC, following the "Shippingport Model" financed and retained ownership of plants in Hallam, Nebraska (240 Mw), Elk River, Minnesota (58 Mw) and Piqua, Ohio (45.5 Mw). (Navigant 2013: 13-16). The government supervised nuclear operations and the small power utilities were

hired as federal contractors to run the plant, exempt from financial protection requirements, and thus not requiring pool insurance (P. L.85-256 Section 170(d)).

The nuclear pools objected to these arrangements. They argued that the government was interfering in the development of a private nuclear insurance market and feared that they would find themselves insuring so few commercial facilities that they would not achieve the spread of risk necessary for sound insurance. Further, they alleged that the AEC, in order to spur nuclear development, was substituting the federal indemnity for "a sound program for the inspection and prevention of loss" needed to protect the public health and safety (JCAE 1960: 148-149).

Ultimately, the AEC phased out the PRDP program, and private utilities began to announce plans to build NPPs without government assistance. However, by the time the Price-Anderson Act came up for renewal in 1966, the liability pools only insured seven relatively small reactors and had only about $11 million in reserves to cover a catastrophic loss (McClure 1968: 292-294).

B. IAEA & International Nuclear Safety Standards

Following President Eisenhower's "Atoms for Peace" speech in 1953, the United Nations convened a series of international conferences leading to the creation of the International Atomic Energy Agency (IAEA). Among the IAEA's key functions was to establish "standards of safety for the protection of health and minimization of danger to life and property" (IAEA 1989 Art. III). The IAEA began its safety standards program in 1958, and over the past 60 years produced hundreds of standards encompassing reactor

design, siting and engineering safety, operational safety, radiation safety, safe transport, and safe management of radioactive waste (IAEA 2018).

The IAEA also developed in 1992 an International Nuclear and Radiological Event Scale (INES) to provide a numerical rating that indicates the significance of nuclear or radiological events. The scale is rated on seven levels (Figure 4.1) with events considered in terms of impact on people and the environment (INES 2020). For example, the Chalk River event, if the INES scale had been created, would likely be rated a "4" being an accident with local consequences. For the remainder of this case study, any events referenced will include an estimated INES scale rating.

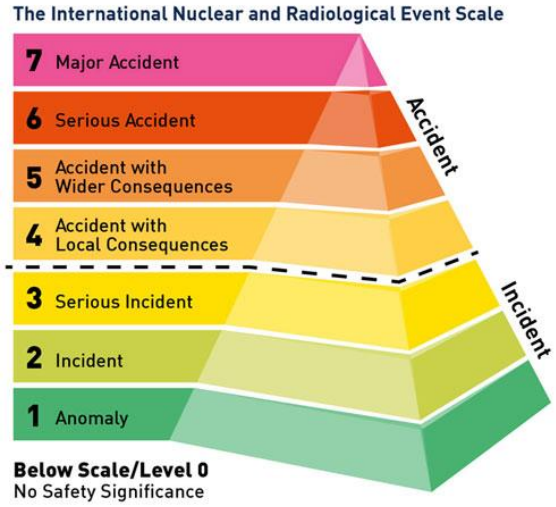


Figure 4.1: International Nuclear and Radiological Event Scale (INES 2020)

C. Nuclear Accidents: SL-1 (1961), Fermi (1967), and Browns Ferry Fire (1975)

During the first eighteen years of the Price-Anderson Act, several accidents occurred at both government and private nuclear reactor sites. None incurred private liability payments, but all three events influenced the private nuclear insurance development.

On January 3, 1961 the Stationary Low-Power Reactor #1 (SL-1) a U.S. Army experimental reactor located at the National Reactor Testing Station in Arco, Idaho suffered a catastrophic accident resulting in the immediate deaths of three servicemen. It is the only known nuclear reactor accident in the United States which resulted in immediate fatalities. The SL-1 was a small 3 Mw BWR designed to generate both electric power and building heat, a prototype for use at small remote Artic military outposts (Thatcher 2018). Because it was a low power experimental unit there was no containment building. It was known the central control rod should only be raised a few inches, and to raise it beyond its safe limit would cause a power excursion allowing the reactor to achieve prompt criticality. An AEC investigation found evidence that the central control rod had either accidently or intentionally been raised 20 inches (JCAE 1961: VI). This resulted in an excursion and steam explosion that propelled the control rod upward with enough velocity to impale one worker to the ceiling (Lochbaum 2018). The area within the reactor building was heavily contaminated with radiation levels over 1000 rads per hour. Fortunately, little radiation leaked from the building, so nearby communities were not affected. Retrospectively, the incident was rated a “4” on the INES scale as an accident with local impact..

On October 5, 1966 Detroit Edison's Fermi I nuclear power reactor in Laguna Beach, Michigan suffered a partial fuel meltdown during power testing. Fermi I was an experimental fast breeder reactor that, unlike water-cooled reactors, required the constant circulation of liquid sodium, an extremely volatile substance that can explode if exposed to water or outside air. Later investigation found that, at the time of the accident, a zirconium metal plate had broken loose, obstructing coolant flow, and causing approximately 1% of the fuel to melt. Radiation alarms immediately sounded, the containment building was immediately sealed shut, and over the next twenty minutes the operating crew performed an emergency shutdown. No one was injured and no radiation escaped. By all accounts, the safety mechanisms and containment performed as designed. Still it is unclear how close Fermi I came to a catastrophic accident. In his book "We Almost Lost Detroit," author John Fuller claimed that the fuel melt could have caused a "secondary criticality" igniting the volatile sodium coolant and creating a large explosion that could have breached containment and released large amounts of deadly radiation (Fuller 1975). However, critics claim the alleged dangers were grossly exaggerated. In any case, the accident resulted in over $20 million of property damage to the core, causing the reactor to be offline for nearly four years, and shutdown permanently in 1972.

On March 22, 1975, a major fire occurred at the Tennessee Valley Authority's (TVA) Browns Ferry Nuclear Power Plant in Athens, Alabama. The fire started around noon by workers using a candle to test for leaks along an electrical cable air seal. The fire spread along the cable insulation into an adjoining equipment room of the Unit 1 secondary containment building, burning for approximately 7 hours causing significant

damage to electrical systems used to control of Units 1 and 2, including the safety systems. The fire suppression system failed to work. Both the Unit 1 and Unit 2 reactors were manually shut down, and remained down for months following the incident (JCAE 1975: 4). The direct cost of the fire were estimated to be about $10 million, with indirect costs of providing replacement power running as high as $10 million per month (JCAE 1975A: 2).

In its report following the fire the NRC's Advisory Committee on Reactor Safeguards (ACRS) noted that "Since the TVA is self-insured in accordance with federal policy, its installations do not have the normal fire insurance surveillance used by private installations" Thus, Browns Ferry did not have property coverage from NELPIA and consequently did not have fire inspections from the property insurance pools. ACRS went on to recommend that TVA's fire protection team be "supplemented by an outside review agency to assure a broad and unconstrained evaluation of fire protection requirements" (USNRC 1976: 21).

Soon after the fire, representatives from NELPIA were invited in to conduct an independent fire investigation. Despite the fact that the plant underwent at least 209 AEC/NRC inspections prior to the fire, the NELPIA inspectors found nearly 40 issues potentially contributing to the fire and needing correction. During JCAE hearings in September 1975, the NRC admitted that their inspections only confirmed compliance with their regulations, only spot-checked cable separations, and did not specifically look at fire protection equipment (JCAE 1975A: 18).

NELPIA followed the Fire Underwriters recommendations for fire protection that exceed any NRC regulations. Subsequently, the JCAE recommended and NRC agreed that NELPIA should conduct all future fire inspections at TVA plants (JCAE 1975A: 11).

D. Nuclear Insurance & Government Regulatory/Indemnity Changes (1967-1977)

One of the main objections to the Price-Anderson Act was that it shielded the nuclear industry from the consequences of negligent behavior by removing the deterrent effect of unlimited liability. While financial protection would always be a precondition for licensure, it had always been the intent of the JCAE that the government indemnity would be phased out, and replaced with a purely private sector solution (JCAE 1965: 12). Further, the JCAE wanted the nuclear industry to internalize their risks in order to maximize the incentives for safe operations.

From inception, the commercial nuclear power operators internalized the cost of protecting their own property. They spent hundreds of millions of dollars to design, build and operate their plants, and they expected to profit from their investment. In the late-1960s, they could purchase up to $100 million of insurance from NEPIA and MAERP, but at a cost 30 to 40 times more than for conventional power facilities (JCAE 1965: 64), and even the maximum coverage might not cover a total loss. Also, there were deductibles, co-pays and loss of use expenses that they were responsible for. Further, unlike the nuclear liability pools, there were no rebates, no government indemnity, and no maximum out-of-pocket cost (JCAE 1965: 302). Thus, the potential uninsured losses could amount to hundreds of millions of dollars. Per a 1974 AEC report, “this potential loss alone should provide a significant economic incentive for safety” (USAEC 1974:

124). The utilities biggest complaint was the high premiums they had to pay to the nuclear property pools.

In 1973, in order to provide an alternative to NEPIA/MAERP, 14 operators created their own mutual insurance pool or "captive" called Nuclear Mutual Limited (NML). These operators, unhappy with monopolistic pool premiums and coverage, decided they could better manage their insurance risks themselves. To reduce rates, NML implemented retrospective premiums that would be assessed to all members to cover a portion of a loss to a single member.

As the number of commercial nuclear reactors increased during the late-1960s, NELIA and MAELU increased their maximum coverage levels. By 1968 there were 11 licensed commercial reactors and maximum coverage was raised to $82 million. It was raised again in 1972 to $95 million when there were 23 commercial reactors licensed to operate, again in 1974 to $110 million; and yet again to $125 million in 1975 with the licensing of 54 commercial reactors (USAEC 1974: 5). Each time the amount of private sector liability coverage increased, the government indemnity decreased by the same amount while keeping the limit of liability the same. However, public criticism of the indemnity as a subsidy to the nuclear industry was growing, and the JCAE asked the AEC to work with the industry and insurers to come up with private sector funded alternatives to the government indemnity.

In January 1974, the AEC produced a report examining various alternatives to the indemnity. One alternative proposed by the nuclear liability pools in August 1973 eventually gained favor. Under this plan, the indemnity would gradually be phased out

and replaced with a retrospective premium program, paid on a per reactor basis, that would only be collected in case of a major accident to cover the portion above the primary layer, up to the limit of liability.

Under the NELIA/MAELU retrospective premium plan, $305 million in coverage would be available in 1978, the first year of Price-Anderson Act renewal. This would include $125 million in primary insurance plus a retrospective assessment of $2 million per reactor for 90 reactors that were expected to be online by the end of 1977 ($180 million total). The premium would be collected by the pools from each operator only if needed to pay losses in access of primary coverage. Retrospective funds would increase by $2 million for each additional reactor added. The government indemnity would then decrease proportionally by the increased retrospective until eliminated. The AEC estimated that this would occur in 1984 when 218 reactors would be in operation. All projections had the number of reactors increasing to 400 units by 1990, increasing the funds available and the limit of liability to well over $1 billion (USAEC 1974, 57).

E. Probabilistic Risk Assessment (PRA) – Rasmussen Reactor Safety Study

In 1972, the chairman of the JCAE requested a new study looking at the probabilities and consequences of severe nuclear power reactor accidents. The request came in the wake of the growing anti-nuclear and pro-environmental movements, and to provide additional information to the JCAE in preparation for hearings on renewing the Price-Anderson Act schedule for 1974.

The study was conducted under the direction of Professor Norman Rasmussen of MIT. This research first used probabilistic risk analysis (PRA) techniques for the study of

core meltdown accidents in two commercial NPPs – Peach Bottom Unit 2 BWR in Delta, Pennsylvania; and Surry Unit I PWR in Gravel Neck, Virginia. The goal was "to make a realistic estimate of the risks and to provide perspective, to compare them with non-nuclear risks to which our society and its individuals are already exposed" (USNRC 1975: 1). To do this, Rasmussen's team tried to identify every accident sequence that mattered, its probability and potential consequences (Bartel 2016: 22). To map the accident sequences they used fault and event trees to define accident paths and their likelihood of occurrence. The Reactor Safety Study (RSS) released in October 1975 pioneered the investigation of nuclear safety issues from a risk perspective. It was a "proof of concept" for the application of risk assessment, establishing the procedures for quantitatively estimating the risk associated with credible low probability events.

The results found that accident probabilities were higher than previously believed but that the consequences to the public and the environment were significantly lower. For example, it estimated that the probability of a core melt accident was 1 in 20,000 per reactor per year, but that the accident would likely be contained with no fatalities or injuries, and less than $1 million in property damage. Under a worst case scenario, there would be 3,300 fatalities, around 33,000 injuries, and property damage of $14 billion – similar to the Brookhaven estimates - however with a probability of only one in a billion (USNRC 1975: 8-11). If a containment breach occurred, the RSS team using demographic and meteorological data was able to calculate the radiation pathways and effects on the nearby populations including early deaths and injuries, and latent radiation

illnesses. It was the first study to estimate the long-term health effects including the probability of latent cancer deaths based on the distance from the reactor accident.

However, the most controversial aspect of the RSS was comparison of nuclear risks to other man-made and natural risks including car accidents, or extremely remote risks such as a large meteor striking the earth. Critics believed that the study had a pronuclear bias, and by using comparisons allegedly prejudged the public's acceptable level of risk for nuclear energy.

F. Price-Anderson Act Extensions & Other Legislative/Regulatory Changes

During this period the Price-Anderson Act was extended twice, in 1965 and 1975, and amended in 1966 to include the concept of the Extraordinary Nuclear Occurrence (ENO). Also, in 1974, the AEC was abolished and replaced with a new Nuclear Regulatory Commission.

When the JCAE held hearings on the first extension of Price-Anderson Act in 1965 and 1966, they identified several key policy questions that needed to be addressed. First, should private insurers make available more nuclear liability coverage and, if yes, how much? Second, was the $500 million indemnity still needed? Third, should the amount of the governmental indemnity available under the Act be reduced as more commercial nuclear liability insurance becomes available? Fourth, should the Act require strict liability that is channeled to the nuclear operator? Finally, given the differences among the various state tort laws, should the federal courts have jurisdiction over nuclear liability cases? (JCAE 1965: 1-2, 12-13)

During the hearings, NELIA and MAELU jointly announced that they would increase the maximum combined liability coverage to $74 million per installation effective January 1, 1966. The JCAE was disappointed and asked why it could not be increased more. Over the first 8 years of coverage there had been no claims filed against covered nuclear reactors, and only two minor liability claims against shippers totaling $3,500 (JCEA 1965: 191). During this time, the AEC paid only one claim totaling $70,000 for a contractor death resulting from the SL-1 accident (JCAE 1965: 31). Despite this "unparalleled safety record" (JCAE 1965: 191) the liability pools were unwilling to increase coverage further because there was too few reactors to spread the exposure; and insufficient reserves to cover even one major accident (JCAE 1965:178).

NEPIA/MAERP also jointly announced that they would raise their combined maximum property coverage capacity to $74 million. However, since their inception in 1956, the property pools had far fewer risks to insure, and far more claims to pay. Over the first 8 years these pools handled 39 claims – with 16 involving nuclear materials including one costing over a million dollars (JCEA 1965: 208). They were also unwilling to raise their coverage limits. However the pools agreed that as more power reactors came online, coverage levels would likely increase.

Given the nuclear liability pools' refusal to substantially increase coverage levels, the nuclear industry advocated for extending the Price-Anderson Act government indemnity. Ultimately Congress voted on September 29, 1965 to extend the Price-Anderson Act for another 12 years (P.L. 89-210 1965). The only major change was to

reduce that amount of the government indemnity by any amount of private sector liability coverage above $60 million.

In July 1966 the JCAE convened hearings to address the issues not covered by the 1965 extension. Specifically debated was whether to establish a federal basis for liability, whether the operator should be held strictly and exclusively liable for accidents without regard to fault (waiver of defense), and whether there should be a statute of limitations on claims. Further, the JCAE was concerned about how claims would be adjudicated and funds would be apportioned and distributed in case of a serious nuclear accident exceeding the $560 million limit of liability.

To deal with all of these issues, the AEC proposed the concept of an Extraordinary Nuclear Occurrence (ENO) defined as any event causing a discharge or dispersal of radioactive material which it determines will result in substantial damages to persons or property offsite. When an ENO is declared by the AEC several things would happen. First, jurisdiction for any public liability arising out of ENO would be assigned to the federal district court in the district where the nuclear incident occurred. The district court then would have the authority to determine if the event might exceed the limit of liability and would adjudicate the disbursement of funds to settle victim claims. Further, if an ENO is declared, under the provisions of the indemnity agreement with AEC, liability would be channeled to the nuclear facility operator who would be required to waive any legal defenses relating to fault or negligence, oblige the operator to assume strict liability and accept a uniform 3-year statute of limitations for the filing of suits (JCAE 1966).

The concept of an ENO and its requirements were captured in Public Law 89-645 passed by Congress on October 13, 1966 (P.L. 89-645 1966). The Law amended the Price Anderson Act, and created a liability environment where victims of an ENO could be quickly and fairly compensated, and which was aligned with international nuclear liability compensation norms.

In 1973, an energized environmental movement filed several lawsuits in federal court challenging the constitutionality of the Atomic Energy Act of 1954 which gave the AEC its authority to simultaneously promote and regulate the nuclear industry. Subsequently, in November 1973, hearings began on the proposed Energy Reorganization Act, an amendment to the Atomic Energy Act of 1954 that would abolished the AEC. In its place two new agencies would be created: the Energy Research and Development Administration (ERDA), to develop and promote energy sources; and a Nuclear Regulatory Commission, to independently regulate the nuclear industry. As noted during the hearings "there has been almost uniform agreement among those who have studied the problem that a separate regulatory commission for nuclear matters should be established (US Congress 1973: 57). As AEC Chairman Dixy Lee Ray noted "the new organization would eliminate the appearance of regulatory and developmental conflicts in administering the nuclear energy program" (US Congress 1973: 158). The ***Energy Reorganization Act of 1974*** (P.L. 93-438) passed the House and Senate with almost unanimous consent, and was signed into law by President Ford on October 11, 1974 and, as a result, the NRC came into existence, and the AEC ceased to exist on January 19, 1975.

Also in 1975, Congress again renewed the Price-Anderson Act for another ten years. The bill included the nuclear pools' proposal to replace the government indemnity with a system of retrospective premiums. The new bill kept the limit of liability the same at $560 million. However, this limit could increase if the aggregate of primary and retrospective coverage ever exceeded $560 million, at which point the government indemnity would be completely phased out. One provision added was that in the event of an incident exceeding the limit of liability, "Congress will thoroughly review the particular incident and will take whatever action is deemed necessary and appropriate to protect the public from the consequences of a disaster of such magnitude" (P.L. 94-197, Section 6). Thus, the new Act set in motion the process for transferring the government indemnity costs to private sector operators. However, it still left open the opportunity for the government to intervene if more funds were needed. The extension was approved by Congress and signed by the President, going into effect January 1, 1976.

VI. Last 45 Years of Price-Anderson Act (January 1, 1976 to Present)

Over the next forty five years the Price-Anderson Act was extended three more times in 1988, 2002, and 2005. During this period the NRC refined the PRA process, the nuclear industry established a new domestic safety standards body, and the nuclear insurance regime further evolved including the phase out of the government indemnity, increases in the limit of liability, coverage for new types of hazards, and changes to nuclear pools structure to adapt to the political and economic climate. Most important was the impact of three accidents: 1) Three Mile Island (1979), 2) Chernobyl (1986), and 3) Fukushima (2009).

A. Three Mile Island Unit 2 Accident - Middletown, Pennsylvania (March 28, 1979)

The Three Mile Island Unit 2 (TMI-2) nuclear power reactor located on the Susquehanna River in Middletown, Pennsylvania went into commercial operation in December 1978. At the time of the accident, Three Mile Island was home to two NPPs, TMI-1 and TMI-2. The two plants were jointly owned by three subsidiaries of the General Public Utilities Company (GPU).TMI-2's PWR was designed to generate 800 Mw of electricity, and the two plants produced enough electricity to supply the needs of 300,000 homes (Kemeny 1979: 82-83).

Around 4 a.m. on March 28, 1979 the initiating event occurred at TMI-2 leading to what the NRC has described as "the most serious incident in U.S. commercial nuclear power history." (USNRC ONRR 2016: 1).The event was triggered when an equipment failure prevented the main pumps from feeding water to the steam generators that remove heat from the reactor core. This caused the generator and reactor to automatically shut down, resulting in an increase in pressure in the primary reactor system. The pressure increase triggered the opening of a relief valve designed to vent excess steam. The valve opened properly, venting the steam, but failed to close when pressure decreased, creating an opening in the primary coolant system. Gauges in the control room indicated that the valve was closed and, as a result, the staff was unaware that water was pouring out of the open valve – the reactor was experiencing a small-break LOCA. The situation was made worse by the operators who misinterpreted the rising water level and actually reduced how much water was being pumped into the system. The LOCA and this action starved the reactor core of coolant causing it to overheat. The situation went undetected for over

two hours and, over time, nearly half of the reactor's fuel melted. Further, with the valve still open, radioactive gasses vented into the containment building.

Eventually, operators discovered the open valve, regained control of the coolant system, and over 16 hours were able to reduce core temperatures and stabilize the reactor. However, the crisis was not over. Hydrogen gas, created by chemical reactions in the melting fuel, escaped into the reactor containment building and formed hydrogen bubble at the top of the reactor pressure vessel. There were widespread fears that the bubble might explode, rupturing the pressure vessel and possibly breaching the containment building. To relieve some of the pressure, the utility began venting some of the gas from the system into the atmosphere. By this time, the accident was getting a considerable amount of press coverage and each burp of steam was increasing public anxiety. In reality, the vented steam contained very little radiation.

Given the atmosphere of growing uncertainty on March 30th Pennsylvania Governor Richard Thornburgh advised pregnant women and preschool-age children to evacuate the area within a 5-mile radius of the plant. By April 1, four days after the accident began operators succeeded in reducing the concentration of hydrogen in the containment building. Later that day, President Carter visited the site, demonstrating to the public that the immediate danger had passed. In its aftermath, the President formed a commission to investigate the accident. The commission, chaired by Dartmouth President John Kemeny, was charged with conducting "a comprehensive study and investigation of the recent accident." The Kemeny Report was released on October 30, 1979. One key finding was that "while the major factor that turned this incident into a serious accident was

inappropriate operator action, many factors contributed to the action of the operators, such as deficiencies in their training, lack of clarity in their operating procedures, failure of organizations to learn the proper lessons from previous incidents, and deficiencies in the design of the control room" (Kemeny 1979: 11).

Fundamentally, the Kemeny Commission recommendations initiated the process for redefining the concept of nuclear safety and the way government and private industry managed nuclear risk. Specifically, they stated that there was too much reliance on technology and regulations, and too little attention paid to the human aspects of safety. They observed that after many years of nuclear power plant operating experience with no evidence of any public harm, the belief that NPPs were safe grew into a conviction. They also believed that there was a preoccupation in the nuclear establishment with safety systems and technology, and a mistaken perception that compliance with complex regulations was the equivalent of safety. Indeed, the Commission noted that "once regulations become as voluminous and complex as those regulations now in place they can serve as a negative factor in nuclear safety" (Kemeny 1979: 9).

It was generally agreed that there had been little appreciable radiation released from the TMI-2 accident, and that there would likely be negligible effects on the physical health of individuals. There were no immediate deaths or physical injuries from the incident. Later health studies found no evidence that the accident was linked with additional deaths from leukemia or other cancers (Hatch et. al.1990: 397-412). The Kemeny Commission concluded that the most serious health effect of the accident was mental stress – especially for those living nearest to the plant (Kemeny 1979: 13). The

TMI-2 accident also had direct financial cost to the utility owners for plant damage and loss of use, and to nearby residents whose lives were disrupted. Following the accident, at least seven class action lawsuits were filed against the utility owners and the reactor manufacturer, with each suit seeking the maximum limit of $560 million.

At the time of the accident, the insurance pools provided a maximum of $140 million in primary nuclear liability coverage. The pools eventually paid 3,170 claimants $1.4 million for living expenses and lost wages (USNRC 1983: 1-6). Soon after, the NRC determined that TMI-2 was not an ENO because there was negligible offsite release of radiation and no clear evidence of harm to people or damage to property. With no ENO, there was no channeling of liability or waiver of defense by TMI-2's operators, and the liability claims were litigated in court. Consolidation of most suits led to a September 1981 settlement. Under the settlement, the pools paid $20 million into a Court managed fund for economic harm to businesses and individuals within 25 miles of TMI-2, and $5 million for the establishment of a Public Health Fund (Clements 2018: 20). But, contested claims continued for another 25 years with a total of $71 million being spent by the pools when finally settled in 2004.

The actual cost to cleanup TMI-2 was around $1 billion. Approximately $300 million less deductible was covered by pool property insurance, a third was covered by the licensee, while the remaining amount was provided by the DOE and other entities (Clements 2018: 20). As a result of the TMI-2 accident, the NRC established new regulations that require licensees to maintain a minimum of $1.06 billion in onsite property insurance at each reactor site.

Soon after the TMI-2 accident, the NRC suspended the licensing of power reactors for a year and turned its attention to determining the TMI-2 lessons learned, reassessing the meaning of "nuclear safety," and applying that knowledge to establishing new nuclear safety goals. The suspension disrupted operator and insurer plan to phase out the indemnity and replace it with retrospective coverage. Per the plan, by 1990 it was expected that around 400 NPPs would be in operation, producing a retrospective coverage layer of about $2 billion. The suspension of licenses undermined this basic assumption needed for retrospective coverage growth.

In May 1979, the NRC established the Lessons Learned Task Force to examine all facets of the accident, identify the causes, and determine what actions were needed before new operating licenses would be issued (USNRC 1981: 656-657). The principal conclusion of the Task Force was that, although the causes of the TMI-2 accident stemmed from many sources, the most important lessons learned fell in a general area they called "operational safety." They acknowledged that in the past the overwhelming emphasis in NPP safety had been on producing a safe design, and not enough placed on safe operation. Bluntly put, there was "no such separate things as safe design and safe operation. A good design can be unsafe if put into the hands of a poorly qualified and trained operations organization" (USNRC 1979: 2-1). Further, the most important recommendation that the Task Force "cannot stress enough" was "the importance of a safety goal in achieving a balanced regulatory perspective" (USNRC 1979: 4-2).

B. NUREG Series Reports on Nuclear Safety Goal (1979 to 1983)

In June 1979 the NRC established a committee to look at the safety goal issue. The first step was the release of a plan for developing a safety goal (NUREG-0735) made available in October 1980 (USNRC October 1980). Under NUREG-0735's basic principle "a general degree of safety is established as a goal and rules are made and licensing actions taken with that goal in mind" (USNRC October 1980: 1). One key plan milestone was the publication entitled *An Approach to Quantitative Safety Goals for Nuclear Power Plants* (USNRC October 1980B*)*. The approach included setting safety criteria based on social and political risk, and outlining the technical tasks needed to determine whether the safety criteria have been met.

The safety criteria included four decision rules including: 1) limits on the frequency of occurrence of certain reactor hazardous conditions, 2) limits to harm to individuals including early and delayed deaths, 3) limits on the overall societal risk of early or delayed death, and 4) an "as low as reasonably achievable" or "ALARA" approach with a criterion that included both economic costs and a monetary value of preventing premature death (USNRC October 1980B: 53). The ALARA criterion was highly controversial since it proposed a marginal value of $1 million per delayed cancer death averted and $5 million per early death averted (USNRC October 1980B: 10). Ultimately, after a series of reports, workshops, and public comment periods, the NRC in May 1983 released NUREG-0880 entitled *Safety Goals for Nuclear Power Plants*. (USNRC May 1983) The safety goals included two qualitative safety goals:

1. Individual members of the public should be provided a level of protection from the consequences of nuclear power plant operation such that individuals bear no significant additional risk to life and health.

2. Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks from generating electricity by viable competing technologies and should not be a significant addition to other societal risks.

There were also two quantitative design objects covering individual and societal mortality risks:

3. The risk to an individual in the vicinity of a nuclear power plant of prompt fatality from a reactor accident should not exceed 0.1% of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed.

4. The risk to the population in the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one percent (0.1%) of the sum of cancer fatality risks resulting from all other causes.

And finally, a benefit-cost guideline and plant performance design objectives:

5. The benefit of an incremental reduction of societal mortality risks should be compared with the associated costs on the basis of $1,000 per person-rem averted.

6. The likelihood of a nuclear reactor accident that results in a large-scale core melt should normally be less than one in 10,000 per year of reactor operation.

C. New Institutions & Industry Safety Performance Standards

In the aftermath of the TMI-2 accident, sweeping changes occurred in the US nuclear industry. The accident created a public relations nightmare for nuclear utilities, increasing public fear and distrust, and threatening the continued existence of their plants and the future of US nuclear power generation. Under these circumstances, the utilities recognized the need for more self-regulation and better management of individual reactor risks. As a result, the utilities created several new institutions to develop safety standards, establish performance benchmarks, administer safety inspections, enact training

requirements, conduct nuclear safety research studies, perform individual plant risk assessments and, when necessary investigate accidents.

1. Institute of Nuclear Power Operations (INPO)

The Kemeny Commission recommended that the nuclear industry "establish a program that specifies appropriate safety standards including those for management, quality assurance, and operating procedures and practices, and that conducts independent evaluations" (Kemeny 1979: 68). In response, the industry in December 1979 established the Institute of Nuclear Power Operations (INPO) with the mission to "promote the highest levels of safety and reliability – to promote excellence – in the operation of commercial nuclear power plants" (INPO 2020).

After its formation, INPO developed performance indicators and began to conduct plant evaluations, visiting each plant about every 18 months. INPO conducted evaluations by sending teams of about 15 INPO personnel and peer evaluators to the plant for two weeks. As part of the evaluation, INPO assigns an index number for each reactor ranging from 0 (poor) to 100 (superior), and then ranks each reactor site from Category 1 (exemplary) to Category 5 (requires special attention and assistance) (USDOE 1986: D4-5). The index is based on ten performance indicators first reported on by utilities to INPO in 1985 (Pate 1986: 61). When INPO developed these indicators, it realized that NPPs with high availability, low personnel radiation exposures, and few significant events, forced outages and unplanned scrams, were generally well managed, more reliable and expected to have higher margins of safety (Pate 1986: 61). Their goal

was to create clear measures of safety performance allowing each plant to be compared with its peers.

Plant evaluation reports are considered highly confidential, and initially are only given to the plant operator (Georgia Court of Appeals 1999). However, the operator is encouraged to share the results with the NRC. Also, since the evaluations are conducted by peer review, any findings of deficiencies are shared with other INPO members, creating peer pressure to improve performance (Rees 1994: 108-109).

Scholar Joseph Rees has described INPO as a very secretive private regulatory bureaucracy that exercises "quasi-governmental functions" including major regulatory tasks delegated to it by the NRC. These include how the industry trains its workers, collects and analyzes operating experience, and how it should operate and maintain NPPs. INPO also issues highly secretive Significant Operating Experience Reports (SOERs) that describe truly significant problems that urgently require additional action by the utilities, including “mandatory” recommendations (Rees 1994: 128). Per Rees, INPO officials believe that their organization’s confidential relationship with NPPs, “like a doctor dealing with her patient” is critical to its ability to carry out its mission (Rees 1994: xi), justifying the public secrecy of SOERs, the INPO index and its annual NPP rankings. Recognizing INPO’s ability to collect and screen event information, the NRC in 1982 issued Generic Letter 82-04 (USNRC 1982) endorsing utility use of INPO’s *Significant Event Evaluation and Information Network* to confidentially share operational experiences.

2. Nuclear Electric Insurance Limited (NEIL)

After the TMI-2 accident, the NRC required all commercial nuclear facilities to carry a minimum of $1.06 billion in property coverage to cover the licensee's obligation to stabilize and decontaminate the reactor and site after an accident. Also, the TMI accident resulted in the uninsured loss of electrical generation capacity, forcing TMI's owner in 1979 to pay up to $35 million per month for replacement power (Kimball 1982: 321). To fill this need, the nuclear utilities in 1980 established a new mutual insurance company called Nuclear Electric Insurance Limited (NEIL). NEIL's first party nuclear property and power outage policies insure NPPs and their generating units for physical losses, decontamination expenses, and costs associated with electric power generation interruptions caused by both nuclear and non-nuclear events.

Over time, NEIL established an operating subsidiary named Nuclear Service Organization (NSO) to perform engineering, loss control and claims functions. NSO also conducts plant evaluations on boilers and other equipment, and fire risk assessments at insured plants. However, it is NEIL's relationship with INPO that has the most impact on nuclear safety. Early in the formative years of INPO and NEIL, officials from both organizations as well as from the NRC believed that the extension of NEIL insurance coverage would be tied to compliance with INPO standards of performance. As such, NEIL insurance would be used as a regulatory tool, and a utility's insurance could be revoked if it failed to implement INPO safety recommendations.

This plan was never implemented. It was believed that revoking insurance could be financially catastrophic to a utility – "kind of like having a nuclear bomb in your arsenal"

(Rees 1994: 94). However, as specified in the annual policy renewal forms, NEIL requires INPO membership as a condition of insurability, and makes the insured consent to the release of all INPO final plant evaluations as soon as they are available (NEIL 2018). NEIL uses INPO plant evaluation ratings as a factor in setting insurance premiums – giving member utilities a 10 percent credit for being rated INPO Category 1 plant. Further, insured plants must pay an immediate penalty of up to 25 percent of the annual premium if the plant is rated INPO Category 5. Further, NEIL has the right to automatically cancel coverage if INPO membership is suspended or cancelled (NEIL 2018). Thus, some elements of plant insurability and premium rates are dependent on compliance with INPO best practices and positive inspection results.

3. American Nuclear Insurers (ANI)

Around this same time, the nuclear liability insurer NEL-PIA changed its name and became American Nuclear Insurers (ANI). Like NEIL, ANI established a Nuclear Engineering Department (NED): consisting of staff nuclear engineers and health physicists whose major purpose was to provide technical assessment to the underwriters and minimize losses to both ANI and MAELU insured assets. Unlike NEIL and NSO, ANI and NED focused on how to reduce third-party liability losses and external risks by conducting inspections independent of both the NRC and INPO. They developed special expertise in monitoring and managing plant performance particularly in regard to the environmental release of radioactive materials, compliance with regulations, and reducing the number and severity of safety events.

Like INPO, ANI established an index for measuring and comparing reactor emission and safety performance – the Engineering Rating Factor (ERF). Based on the ERF, the performance of reactors of similar type were compared and used to establish annual premiums, rewarding the best performers and punishing those with the worst ratings. Thus the ERF can lead to a 20% credit or a 30% debit on premiums. These adjustments are reflected in the following year's calculation of the plant's advanced premium. Thus, ANI loss control expertise complemented and strengthened the safety efforts of NEIL, the NRC, and the nuclear industry as a whole.

D. Chernobyl Nuclear Disaster

The Chernobyl Nuclear Power Plant is located in northern Ukraine about 20 km south of the border with Belarus and 140 km west of the border of the Russian Federation. At the time of the accident in April 1986, these three present-day countries were part of the Soviet Union (USSR). About 115,000 people lived within 30 km of the plant. Kiev, the capital of the Ukraine with a population of over 2 million people, is located 130 km south of Chernobyl. The Chernobyl plant consisted of four 1000 Mw graphite-moderated RBMK-1000 BWRs. The reactors were only equipped with rudimentary emergency shutdown systems and, per Soviet safety protocols, had no containment structure to control radioactive releases if an accident occurred (O'Tool 1978).

The Chernobyl accident occurred on Saturday, April 26, 1986 at 1:23 a.m. during an experimental test of the electrical control systems. As part of the test, the technicians deliberately lowered the reactor's power level and shut off the plant's emergency cooling

system. Compounding their error the operators removed all but a few of the control rods and disconnected the automatic rod control system. Within seconds there was a heat buildup in the core. Further, when the shift manager attempted an emergency shutdown, a flaw in the system caused a power surge that overheated the reactor, and resulted in a series of gas explosions that blew off the roof of the reactor building, created a fire, and released radioactivity into the atmosphere. Two workers died as a result of these explosions. Emergency crews responding to the accident used helicopters to pour sand and boron on the reactor debris to stop the fire and additional releases of radioactive material. However, the fire continued to burn for another ten days. The explosions and fires released more than 5% of the radioactive reactor core into the atmosphere. At least 134 onsite responders were exposed to high levels of radiation and were later diagnosed with acute radiation syndrome (World Nuclear Association 2020) - 28 of these responders would later die. On April 27, the town of Pripyat was evacuated; and by May 14th the entire population within a 30-kilometer radius of the plant was moved to safety.

The Chernobyl accident was the first NPP disaster in which nuclear contamination occurred on a global scale. The accident caused the largest uncontrolled radioactive release into the environment ever recorded for any civilian operation, and large quantities of radioactive substances were released into the air for about 10 days. It was retrospectively rated a “7” on the INES scale as a major accident. Radiation traveled across the Pacific with measurable amounts eventually detected in all countries of the northern hemisphere (UNSCEAR 2008: 47). Over 116,000 people were initially evacuated and another 220 000 were relocated in subsequent years. All of the initial 30

fatalities and approximately 300 radiation-related injuries occurred at the reactor site. No off-site casualties occurred in the immediate accident aftermath. However, there were major concerns about the long term health effects of radiation exposure, especially for the 530,000 registered "liquidators" involved in cleanup activities. The Chernobyl Forum estimated that among the 600,000 people receiving significant exposures there would be a higher cancer rate translating into about 4000 more deaths above expected levels (Chernobyl Forum 2008: 15). The total economic consequences of the disaster are also difficult to calculate. The costs to contaminated former-Soviet republics included the direct damage caused by the accident; expenditures for sealing of the reactor and mitigating the consequences in the exclusion zone; costs for resettlement of people and construction of new housing and infrastructure to accommodate them; disposal of radioactive waste; and indirect costs related to loss of agricultural land use, and loss of power generation from the Chernobyl nuclear plant. One report estimated the total cost to Belarus alone to be $235 billion (Belarus Foreign Ministry 2009).

E. Probabilistic Risk Assessment (PRA) & Risk Informed Regulation

Throughout the 1980s and1990s, the NRC and private sector through the use of PRAs strove to improve the process to determine the likelihood and consequences of a nuclear accident. In 1983, the NRC released a report (NUREG-2300) outlining the procedures for utilities to follow to perform PRAs at their facilities (ANS and IEEE 1983).

In follow up to NUREG-2300, the NRC released *NUREG-1050* providing guidance for the use of PRA in regulatory decision making (USNRC 1984). It outlined three levels

of nuclear risk: Level 1 PRAs estimated the frequency of accidents that cause reactor core damage; Level 2 estimated the frequency of accidents that release radioactivity; Level 3 estimated the consequences including injuries and damage to the environment after a radioactivity release.

In 1985 the NRC released a policy statement on severe reactor accidents. It recommended PRAs for all existing NPPs and future reactor designs (USNRC 1985). This recommendation became formalized in November 1988, when the NRC released *Generic Letter 88-20* (USNRC 1988) requesting that all commercial nuclear power licensees perform Individual Plant Examinations (IPEs) to identify plant-specific vulnerabilities. In response, nearly all licensees performed Level 1 & 2 PRAs to assess the likelihood and consequences of a severe accident to their specific plant. The detailed results along with NRC staff evaluation reports, and technical evaluation reports for each IPE were made publicly available. Thus, each IPE was viewable by the insurance members of ANI, and by the utility members of NEIL.

Prior to the release of the IPE results, the NRC issued a policy statement on its commitment to use PRA in nuclear regulatory matters (USNRC 1995). Thus, risk assessments would inform, regulatory decisions. Building on this statement, the NRC subsequently released a series of plant-specific risk-informed regulatory guides dealing with decision-making, inspections, testing, licensing, and quality assurance (USNRC 2002). Thus the NRC was moving from a "one-size fits all" approach to safety regulations to a safety regulation path focused on the meaningful risks associated with a specific plant design, components, systems, and operational practices.

F. Nuclear Industry Evolution: New Political Economy of Nuclear Power

In 1980, noted Harvard political scientist Graham Allison was asked by the President's Nuclear Safety Committee to conduct a study with the goal of developing a realistic diagnosis of the problem of nuclear power in the United States today. The Report began with the "Director's Dilemma"- if you were a director of a US utility company, would you vote in favor of building a new nuclear power plant? The answer was "probably not." Unless something drastic was done there would be few new orders for NPPs, more cancellations, substantial safety problems for current plants, and a defeat of what had been US policy for over three decades.

The report stated that the NRC's complex licensing procedures had doubled the cost and the time needed to put a plant into operation. Further, the deluge of new regulations after TMI-2 was overloading operators, creating confusion, and ultimately lowering overall safety (Allison et. al. 1981: 27). The report proposed fundamental changes to the governance of nuclear power. Key to this new governance system was to shift focus from complex technology-specific regulations to a regime where the private sector was principally responsible for the safety of their plants, and operator interest in safety are identified, enhanced and encouraged (Allison et. al. 1981: 41-42).

Analysis of the TMI-2 accident showed that it was the reactor's owners and the nuclear industry that suffered the most financially from the disaster. A new viewpoint emerged that the possibility of large financial losses from nuclear accidents would provide a strong incentive for utilities to build and operate plants with very low risk to the public. Evidence suggested that safe plants had the highest availability and lowest long-

term costs. Therefore, the utility interest and the public interest in safety were coincident. Further, it was argued that greater use could be made of the utility's self-interest in regulation if the relationship between the NRC and the nuclear industry were less adversarial and more cooperative in nature (Starr and Whipple 1982).

In 1998 the NRC produced a detailed report (Bailey et al. 1998) concerning the condition of the nuclear industry, the availability of private insurance, and the state of knowledge on nuclear safety at that time. Since 1980, little had changed. No new licenses for nuclear reactors were issued during this period. Construction on 8 new plants was competed, but also 10 reactors were prematurely retired (Bailey et al. 1998: 333).The number of operating reactors reached a peak of 116 in the early 1990s, only to decline to 110 by mid-1998. The NRC predicted that no new units would be added in the foreseeable future. Further, due to reactor aging, deregulation, and other economic factors, the NRC predicted additional early reactor retirements.

The commercial nuclear power industry continued to have an outstanding safety record. With approximately 2,000 years of operating experience, the U.S. industry had only one significant accident, TMI-2, and it had caused no identified fatalities. PRAs being conducted by the utilities under the IPE program continue to indicate that the chance of another major accident was one in 10,000 years (or more), and that such an accident would likely not cause fatalities due to containment and other safety systems in place. In addition, the NRC in the 1980s implemented the Systematic Assessment of Licensee Performance (SALP) program to grade each reactor's operational, maintenance, and engineering performance based on inspections, audits, and event reviews. SALP

along with PRA/IPEs provided the nuclear insurers additional information to augment INPO's and their own assessments of each reactor's individual safety risk.

Around 2005, the U.S. commercial nuclear power industry experienced a revival including the granting of new construction licenses, renewing of many operating licenses, and approving many plants to generate electricity at higher power levels. By 2013, 5 new reactors were under construction, and another 10 proposed projects were in various stages of NRC licensing review (Navigant 2013: 5, 52). In addition, 73 reactors had their operating licenses extended an additional 20 years, and another 24 units were under review or planning to renew. Further, by 2013 the NRC had approved 146 reactor power uprates, providing 6.8 Gw of additional US generating capacity (APS 2013: 2).

There were several reasons for this revival. First, since the TMI-2 accident in 1979, the US nuclear industry had a nearly perfect safety record with no major events. This sustained superior performance allowed plant's to operate at an average capacity of nearly 90%, provided extensive operating experience and significantly reduced operational and maintenance costs (Navigant 2013: 5). From 1995, NPPs had a lower production cost per megawatt per hour than all fossil fuel-based generating plants (Navigant 2013: 63). For new plants, the NRC simplified the licensing process, allowing operators to apply and receive combined "one-step" construction and operating licenses. This eased the regulatory burden, eliminated some construction delays, and shortened the time period between breaking ground and revenue-producing operations. Thus, by the mid-2000s, the economics of nuclear power generation was turning more favorable.

As part of the Energy Policy Act of 2005 nuclear power was considered a clean energy technology eligible for loan guarantees and other subsidies for construction of new plants. As of December 2020 there are 94 operating nuclear power reactors on 56 sites, in 28 states (with a combined total capacity of 96.55 GWe (EIA 2022). In 2018, the first utilities began to submit applications for extending operating licenses to 80 years under the NRC's Subsequent License Renewal program. Despite this progress, several impediments remained to nuclear power's renewed growth. Economics remains a key factor in nuclear power plant operations.

Even with the opportunity to extend their operating licenses for an additional 20 years, some plant operators are finding the costs to retrofit their plants to meet license renewal safety requirements to be prohibitively high. As a result, over the past six years, 8 nuclear reactors have been shut down and another 10 reactors currently in operation are at risk of closure due to economic challenges. Since 1957, 31 US commercial nuclear reactors have been shut down, nearly all prematurely before the expiration of their 40-year license. Often these early shut downs were precipitated by accidents arousing public nuclear safety concerns and triggering new safety regulations that required similar reactors to undergo expensive retrofits. The quintessential example of such an accident occurred in March 2011 when an earthquake and series of large tsunami caused an INES Category 7 accident at the Fukushima Nuclear Plant in Japan.

G. Fukushima Prefecture Nuclear Disaster

The nuclear disaster that occurred in Fukushima prefecture in 2011 was unprecedented and had a profound effect on US nuclear operations, liability, insurance

and safety. Unlike Chernobyl, it involved fully-contained reactors, equipped with modern safety systems, operated under full power, and located in a densely populated area. While there were no immediate deaths or injuries, there was a breach of containment, widespread contamination, large population displacement, and over $100 billion in economic damage, Thus in many ways, the Fukushima event paralleled the worst-case predictions of the Brookhaven, RSS and other PRA studies.

Like the US, Japan had nuclear liability legislation requiring utilities to have JPY 120 billion (US $1.1 billion) per reactor in financial protection, and strict liability that was channeled directly to the reactor operator. Unlike the US, there was no liability limit and operators were fully responsible for damages. In the aftermath of the event, a new catastrophic liability compensation model was developed involving funds from the operator, contributions from other Japanese nuclear operators, and government support through the sale of special bonds.

Several injuries to plant workers were attributed to hydrogen explosions, and several workers received radiation doses that exceeded Japanese lifetime radiation exposure legal limits. Over the years the Japanese government awarded compensation to four workers who developed leukemia and cancers, and in 2018 recognized the first radiation death – a worker who died of lung cancer (Meixler 2018). The economic cost of the Fukushima accident is estimated to be trillions of yen. Industries particularly impacted included agriculture, fishing, and tourism.

The entity that suffered the biggest economic loss was TEPCO, the owner and operator of Fukushima. TEPCO had both property and liability insurance provided by the

Japanese nuclear pool, and heavily reinsured by the global pools. However, coverage was denied as earthquakes and tsunamis were specifically excluded. Thus, TEPCO was fully liable for all third party damages resulting from the disaster, as well as the decontamination and decommissioning of its plant. In May 2011, TEPCO and the Japanese government came to an agreement whereby the state would provide support to compensate all third parties affected by the accident and also to help TEPCO cleanup and decommission the Fukushima site. The agreement included the formation of a new state-sponsored institution, the Nuclear Damage Compensation Facilitation Corporation (NDF) to expedite payments to victims. NDF established a compensation fund with financial backing provided through the issuance of JPY5 trillion (US$62 billion) in special government bonds, and contributions from other nuclear operators, similar to the retrospective premium program in the US. In return, TEPCO agreed to not set an upper limit to compensation and to establish a plan to repay the government for its assistance.

The financial burden quickly grew. Eventually in June 2012 TEPCO's shareholders voted to sell 50.11% of voting shares to the Japanese government for JPY 1 trillion – thus essentially placing TEPCO under state control. As of 2017 the costs had risen to JPY 22 trillion (US$191 billion) including JPY 16 trillion from TEPCO, JPY 4 trillion by other nuclear operators, and JPY 2 trillion from the Japanese government (World Nuclear Association 2019).

The accident had a chilling effect on the nuclear industry in the US. Plans for new nuclear plants that had been announced in the period 2007 to 2010 were withdrawn, and several existing plants were closed in 2013. Questions were raised about the reliability of

the NRC's use of PRAs, especially in regard to estimates on the frequency of major reactor accidents. There were also concerns about whether the financial protection provided under Price-Anderson was sufficient to cover damages caused by a similar event in the United States

H. Price-Anderson Act Extensions & Evolution of Nuclear Insurance

Over the period 1976 to the present, the Price Anderson Act has been extended twice more in 1988 and 2005. Also during this period, the U.S. nuclear insurance market consolidated into two primary carriers – ANI for liability protection, and NEIL for property coverage.

When debate began on the third extension of the Price-Anderson Act in June 1985, it was conducted by the Senate Subcommittee on Energy Research and Development. Long before then, in August 1977, the JCAE had been abolished. Over the period from the Acts enactment in 1957 to the 1985 hearings, there had been a total of 112 claims reported to the nuclear insurance pools resulting in $43 million in third-party liability payments and $488 million in first-party property settlements – nearly all of which were associated with the TMI-2 accident (US Senate 1985: 26-27). No claims or payments had ever been made against the Price-Anderson federal indemnity or its retrospective replacement. The US commercial nuclear power industry continued to have an exceptional safety record compared with other energy sectors. There had been no fatalities compared with over 6,000 deaths due to US coal mining accidents over the same period (US Senate 1985: 16). However, soon after debate began, the Chernobyl accident occurred. It had a

profound effect on the US public's perception of nuclear safety, further dampening prospects for new NPP construction and accelerating the pace of reactor retirements.

On March 4, 1987 Rep. Morris Udall introduced the Price Anderson Amendment Act (H.R. 1414). The bill passed the House on July 30th, just ahead of the August 1, 1987 expiration date. This proposed legislation stalled in the Senate over the issue of unlimited liability. Eventually the Senate passed an amended version of H.R. 1414 on March 18, 1988, and it was signed into law by President Reagan on August 20, 1988.

The *Price-Anderson Amendment Act of 1988* (P.L. 100-408 1988) contained several new elements. It extended the Act through August 1, 2002. It raised the limit of liability to $7.34 billion based on $200 million of primary insurance and $7.14 billion of secondary coverage. The bill also authorized an automatic adjustment to retrospective premium every 5 years to take into account the effects of inflation. The extension also consolidated the claims of all nuclear incidents, not just ENOs, under federal jurisdiction, and eliminated the 20-year claims statute of limitation. The Congress also committed to providing "full and prompt compensation" to the public for all liability claims resulting from a nuclear disaster.

During most of the 1990s, the primary liability coverage level provided by ANI and MAELU/MAERP stayed the same at $200 million per reactor site. Seventy percent of reactors were located on multi-unit sites. Locating more than one reactor at a site allowed utilities to reduce operating costs by consolidating resources. They also saved money on primary insurance with the premiums on the second and third reactor on a site being discounted by eighty percent or more vs. the first reactor. Under the Industry Credit

Rating Plan, the utilities received up to 75 percent of premiums paid back after 10 years - more than $209 million in rebates since 1957. Despite these discounts and rebates, the utilities objected to what they considered exorbitant premiums for coverage resulting in minimal claims. Over 40 years of coverage since 1957, the utilities had paid over $1.9 billion in premiums, and the liability pools had only paid out $141 million in indemnity and expenses – a loss ratio of less than 7.5 percent. Nearly half of those payments were for TMI-2 settlements and expenses. Even with the $209 million in rebates and amounts put away in reserves, the insurers were making a healthy profit.

However, one accident on the scope of Chernobyl, would likely wipe out all profits dating back to 1957. Despite this possibility, in 1991, the utilities demanded and received a 20% reduction in their premiums from ANI and MAEP, and an additional 15% reduction in 1992. In 1995, the utilities demanded a further reduction in premiums, and also asked that some of the risk be ceded to NEIL. ANI agreed, however MAEP members felt that significant concessions had been made, and that further reductions would not be in their interests. Thus they voted to end participation in the nuclear liability program and exited the market in 1997. By 1998, ANI had ceded nearly 70% of its liability exposure to NEIL and foreign pools. In return, NEIL and foreign pools ceded ANI some of their exposure creating a global nuclear insurance community which spread the risk over a broad financial base (Bailey et al. 1998: xviii).

As mandated by the 1988 extension, the secondary retrospective premium was increased every five years for inflation based on the Consumer Price Index, rising to $75.5 million per reactor in 1993, and to $83.9 million per reactor in 1998. At that time,

the total secondary coverage was $9.23 billion ($83.9 million x 110 units) and the limit of liability was $9.43 billion. ANI managed the secondary program charging $7,500 per reactor in administrative fees. In the event of an accident requiring maximum secondary coverage, ANI would collect $10 million per reactor per year until the $9.23 billion limit of liability was satisfied.

In 1988, as a condition of licensure (10 CFR 50.54), each power reactor site was required to carry a minimum of $1.06 billion in property insurance to stabilize and decontaminate the reactor site in the event of an accident. This minimum coverage consisted of $500 million in primary coverage and a minimum of $506 million in excess coverage. At that time this primary and excess coverage could be obtained from NEIL, NML, ANI/MAELU, or a combination of all three. Each year, every operator was required to provide proof of coverage for all of their sites. Most operators secured the maximum amount of property coverage - $1.525 billion including over $1 billion in excess – typically with anywhere from a $1 million to $10 million deductible.

Unlike nuclear liability coverage which was essentially a monopoly of ANI/MAELU, the competition between NEIL/NML and ANI/MAELU drove coverage levels up and premium prices down. NEIL/NML annual reports indicate that the amount of their available coverage rose from $1.325 billion in 1988 to as much as $3 billion in 1998. Meanwhile, the cost of coverage dropped from approximately $3.3 million per billion of coverage in 1988 to $1.2 million per billion of coverage in 1998 (NEIL 2013: 9). Because NEIL/NML property insurance covered “all-risks” their loss ratios were higher than for ANI/MAELU averaging 23% over the ten year period (NEIL 2002: 1),

but substantially better than most other lines of commercial insurance. Separate from Price-Anderson, NEIL/NMI established a retrospective plan to collect additional premiums from utility members in the event of a major accident, Throughout the 1990s, they built up a sufficient reserve to pay for two full policy limit losses without the need for retrospective payments (NEIL 2013: 9). In 1997, NML merged with NEIL, provided reinsurance to ANI, and also began to offer business interruption coverage of up to $490 million to members.

Thus, by the turn of the century, NEIL controlled the US market for nuclear property and business interruption insurance, and ANI had a virtual monopoly on nuclear liability coverage. Both managed a retrospective program in case of a major accident, provided reinsurance coverage to foreign pools, and ceded risk to each other and to non-US nuclear insurance carriers.

Congress began holding hearings on fourth renewal of the Price-Anderson Act on September 6, 2001. However, five days later, a non-nuclear event occurred that among many things disrupted the entire insurance industry and delayed renewal of the Act for four years.

On September 11, 2001, the insurance industry's views on the risk of terrorist attacks in the US materially changed. Prior to 9/11, terrorism in the US was considered a very rare and insurable risk. Consequently, insurers usually included terrorism coverage as part of their commercial property and casualty policies, oftentimes at little or no additional charge. This all changed immediately following 9/11 as insurers and reinsurers realized that they had grossly underestimated the probability and severity of a terrorist

attack on US shores. Losses stemming from the destruction of the World Trade Center and other buildings totaled about $31.6 billion, including liability and life insurance claims. Much of this cost was borne by reinsurers to pay off underlying insurance contracts (Castellano 2010: 400). Almost immediately, reinsurers worldwide began to impose new terrorism exclusion clauses. This prompted many insurers in the US to also exclude terrorism from property and casualty policies.

Unlike most insurers, the nuclear pools continued to insure their commercial nuclear power clients for first- and third-party damages caused by a terrorist attack. However, primary liability coverage was limited by ANI to one shared industry aggregate limit of $200 million per year in order to assure member companies and reinsurers that the terrorism exposure was quantified and capped. ANI also increased their premiums by 30%. The retrospective layer of coverage of over $9 billion also remained for acts of terrorism (US Senate 2002: 33). So up to the limit of liability terrorism was covered. Coverage above this amount would require special Congressional action.

Faced with this coverage dilemma, Congress in November 2002 enacted the *Terrorism Risk Insurance Act* (TRIA). Under TRIA, the US government became the "reinsurer of last resort" to cover losses associated with foreign acts of terrorism that occur on US soil. TRIA required insurance companies to offer terrorism coverage and, in return, provided a federal reinsurance "backstop" for losses from terrorist attacks. Thus, both the private and public sectors shared the terrorism risk. The insurance industry was responsible for the first $10 billion of aggregated losses. TRIA coverage was 90% of the

amount above the insurer's deductible, with coverage capped at $100 billion per year without additional Congressional approval (P.L. 107-297 2002).

ANI and NEIL managed terrorism coverage for their clients through an ""endorsement" that stipulated the limit of coverage for the industry per year to be the maximum available coverage for a single policy – thus $200 million primary and $9.1 billion secondary for liability, and $3 billion for property. The revised policies also included a disclosure on TRIA coverage, outlining what additional coverage might be available through the federal government (NEIL 2002).

The 9/11 attacks significantly heightened concerns about the security of U.S. nuclear plants. It was soon found that the planes that flew into the World Trade Center passed directly over the nuclear plant at Indian Point. A *London Times* story alleged that TMI was the intended target of Flight 93 that crashed into a field near the town of Shanksville, Pennsylvania (Rufford et al. 2001). Then, during his State of the Union address on January 29, 2002, President Bush noted "we have found diagrams of American nuclear power plants [in al Qaeda camps]." As a result, Congress focused their attention on updating the bill to provide for nuclear infrastructure physical security.

Up to 9/11, extension of the Price-Anderson Act seemed to be a virtual certainty. Congressional hearings held earlier in 2001 indicated broad bipartisan support in both the House and Senate, and renewal also had the endorsement of President Bush, the NRC, and DOE. Hearings were held in the Senate subcommittee on the bill, but it never made it to the Senate floor, and died in the 107th Congress. However, an amendment was added

to the 2003 appropriations resolution temporarily extending the Act to the end of 2003 (P.L. 108-117).

During the 108th Congress (2003-2004) no specific hearings were held to extend Price-Anderson, and the Act technically expired on December 31, 2003. Even without an extension, existing power reactors were grandfathered and would continue to operate under the Price-Anderson liability system, but any new reactors would not be covered. Subsequently, during Congressional hearings on the future of nuclear power, it was made clear that no new NPPs would be constructed without the Act's reauthorization (US Senate 2004: 40). Despite this problem, the insurance situation for existing power plants was improving. On January 1, 2003 ANI raised the level of primary liability coverage to $300 million, and in August 2003 the secondary retrospective premium was adjusted to $95.8 million per reactor for inflation. These changes raised the limit of liability to $10.4 billion for 105 reactors (US Senate 2004:40). Finally in 2005, sparked by rising costs of fossil-fuel electricity generation, concerns about climate change, and the development of "cleaner" and "safer" next-generation nuclear reactors, Congress passed the *Price-Anderson Amendment Act* as part of the *Energy Policy Act of 2005* (P.L. 109-58 2005). The renewed Act extended coverage for commercial reactors until December 31, 2025, and increased the annual premium payments from $10 million to $15 million per reactor.

VII. Evidence of Role as Regulator and Safety Promoter

This section provides evidence of the role insurance as a private sector regulator and promoter of nuclear safety. It includes an overview of the two key insurance institutions, ANI and NEIL, their current processes for assessing risk and establishing premiums, their

mechanisms for managing client risk and controlling losses, and their collaboration with other institutions in regulating nuclear industry safety. It also discusses the current role of the US government in providing additional layers of insurance coverage to US nuclear operators, and the influence these additional mechanisms has on overall nuclear safety behavior. Evidence from the NRC library on nuclear insurance liability and property premium calculations is presented including the influence of INPO Indices, ANI ERFs, and NRC risk assessment factors.

A. American Nuclear Insurance (ANI) – Primary & Secondary Liability Insurance

As specified in Section 170 of the Atomic Energy Act of 1954 and under U.S. Code Title 42 Section 2210 (Indemnification and limitation of liability) all commercial power reactors having a rated capacity of 100 Mw or more, as a condition of licensure, are required to carry the maximum amount of financial protection available to cover public liability claims. Today this protection includes $450 million per reactor site in primary insurance and retrospective coverage of $137.61 million for each of the 94 reactors in operation in the US. All US NPPs get their primary liability insurance from American Nuclear Insurers (ANI). ANI also administers the retrospective insurance program established by the renewal of Price-Anderson in 1976.

ANI is not an insurance company but rather a joint underwriting association and managing agent for a syndicate of participating insurance member companies. The syndicate was formed to insure a broad array of nuclear facilities and suppliers of products and services to the nuclear industry. Member companies provide insurance by agreeing to pay a portion of insured losses up to a specified maximum per policy. In

return each insurer receives a portion of the premiums, after expenses. To be an ANI member, an insurer must have a Best Credit Rating of A or higher and at least $100 million in policyholder surplus. Each site policy is treated as a separate project with varying percentages of member participation. Insurance is state regulated, and to participate in a project a member must be admitted to sell insurance in the state where the reactor is located.

ANI issues policies, collects premiums, remits the premiums annually to participating insurers, handles claims, and otherwise administers the program. In 2015 when the organization was last examined by the State of Connecticut, the syndicate had twenty participating members, earned premiums of $53.1 million, incurred losses of only $286,813, and returned $34.9 million of net income (profit) to members. Seventy percent of annual premiums are put into a reserve fund for 10 years and, after accounting for losses, most is refunded to policyholders. ANI also has authority to cede or accept reinsurance to and from NEIL, as well as from foreign pools.

ANI currently provides primary insurance to 94 operating and 14 decommissioned commercial power reactors located on 76 sites in 34 states. In 2018, the average annual premium for a site with a single power reactor was approximately $1 million. The premium for a second or third reactor at the same site is discounted to reflect a sharing of the $450 million site limit. Once issued, the primary policy remains in effect continuously until cancelled or by exhaustion of its coverage limit. The limit is automatically reduced by payments for claims or claims expenses.

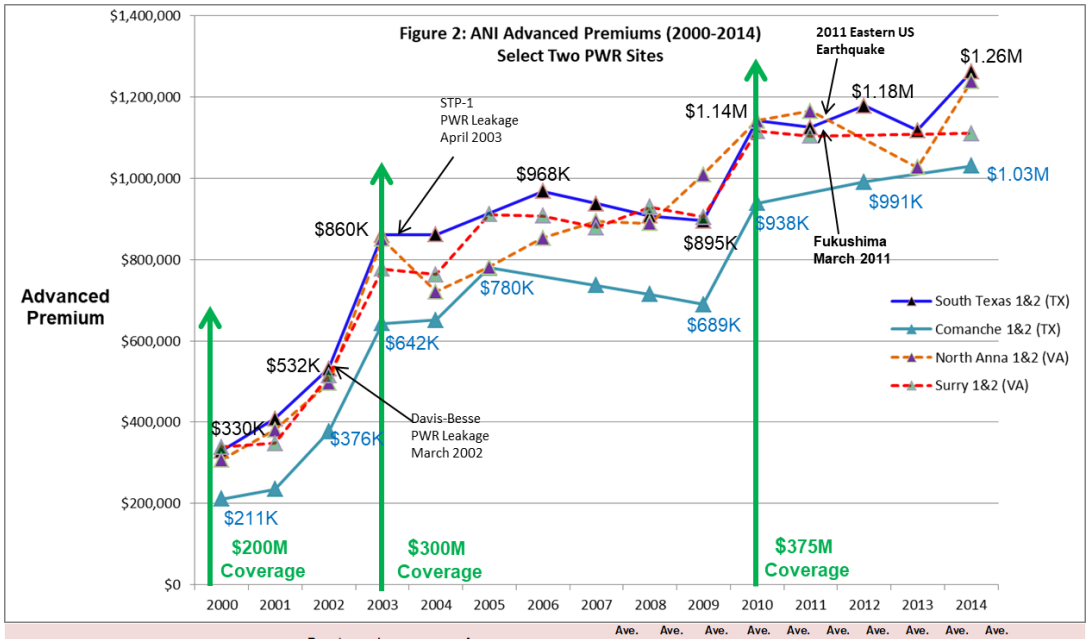
ANI issues primary insurance using a Facility Form Policy that is purchased by all U.S. commercial nuclear power plant operators and satisfies the Price-Anderson Act requirement for primary financial protection. This policy insures all interests (except the US government) with respect to their legal liability for covered damages including claims made for bodily injury or property damage caused during the policy period, if such claims are brought within ten years of policy termination. Onsite property damage and cleanup costs, as well as offsite environmental cleanup costs arising out of governmental directives are specifically excluded. Radiation-related workers' compensation liability claims are also excluded since they are covered under a separate Facility Workers Form Policy. While there is a $450 million policy limit, there are no deductibles, co-pays or sub-limits associated with the primary coverage.

Since Facility Form coverage is continuous, any changes to the policy including new Price-Anderson requirements (e.g. waiver of defense), additional coverage (e.g. TRIA), and annual premiums changes are done through policy endorsements. Policyholders must annually file with the NRC proof of financial protection certificates and any new endorsements. Thus there is a record of premiums paid for many reactor sites over many years of operation. Each premium endorsement includes the "advance" premium paid in January for the upcoming calendar year, and the "reserve" premium amount set aside by ANI in reserves. The annual premium can also include additional costs or returns of the previous years advanced premium, based on the plant's operational activity and changing risk profile as determined by annual ANI inspections.

1. ANI Premium Analysis –Sites with Two PWRs (2000-2014)

ANI premiums provide a lens into how ANI joint underwriters annually rate the risks associated with individual NPP sites. Plotting annual premiums over a period of time allows the comparison of one reactor site versus another, and also shows how the risk ratings for individual sites change over time. For example, Figure 4.2 below shows the premium plots for four reactors - two sets of "sister" NPPs that share many characteristics: 1) South Texas Project (STP) and Comanche Peak (CP) NPPs owned by a series of power companies in Texas (Texas Sisters), and 2) North Anna and Surry NPPs owned by Virginia Electric & Power Company (Virginia Sisters).

All four sites are equipped with Westinghouse PWRs. The Texas Sisters are about the same age (© 1990) and power (@3700 MWt), located in fairly sparsely populated part of Texas (<22,000 people), and have the same exact same reactor (4LP) and containment (DRYAMB) types. Likewise, the two Virginia Sisters also are roughly the same age (circa mid-1970s) and power (@2800 MWt), located in moderately populated portions of Virginia, and have the exact same reactor (3LP) and containment (DRYSUB) types. During the period covered, all NPP premiums are impacted by two increases in primary coverage levels from $200 to $300 million in 2003 (50% increase), and from $300 to $375 million in 2010 (25% increase).



Plant Name, Unit Number	City, State	# PWR	Reactor and Containment Type	Supplier	Ave Age 2000	Ave. MWt	# People w/in 10 miles	Ave. Plant Cap. 2005	Ave. Plant Cap. 2006	Ave. Plant Cap. 2007	Ave. Plant Cap. 2008	Ave. Plant Cap. 2009	Ave. Plant Cap. 2010	Ave. Plant Cap. 2011	Ave. Plant Cap. 2012	Ave. Plant Cap. 2013	Ave. Plant Cap. 2014	Ave. Plant Capacity 2005-2014
South Texas Project	Palacios TX	2	PWR-DRYAMB	WEST 4LP	11.5	3853.0	8,703	88.6%	94.8%	95.9%	95.2%	95.5%	94.5%	91.0%	82.5%	75.2%	92.0%	90.51%
Comanche Peak	Glen Rose TX	2	PWR-DRYAMB	WEST 4LP	8.5	3612.0	21,620	90.4%	96.7%	92.1%	95.2%	97.0%	97.5%	91.5%	94.5%	96.2%	89.0%	94.01%
North Ana Power Station	Mineral VA	2	PWR-DRYSUB	WEST 3LP	21.0	2940.0	34,081	95.3%	93.9%	87.0%	91.3%	96.0%	93.0%	77.0%	94.0%	87.4%	96.0%	91.09%
Surry Power Station	Gravel Neck VA	2	PWR-DRYSUB	WEST 3LP	27.5	2587.0	141,209	93.4%	88.3%	93.6%	93.3%	95.8%	93.8%	84.0%	88.3%	81.3%	94.0%	90.56%

Figure 4.2: ANI Advanced Premiums (2000-2014) – Two PWR Sites (Source: NRC)

Examination of the Texas Sisters shows that through the entire period, CP's ANI premiums were lower than STP's with a fairly consistent gap of about $200,000 each year. Based on this consistently lower premium, all other things being equal, CP represented a lower risk to insure than STP. STP is slightly older and higher powered, but CP is closer to populated areas. Both sites received high or highest grades from the NRC during their annual risk assessments for the period 2000 to 2014. CP did have three NRC Notifications of Violation (NOV) in 2002, 2004, and 2008, which seems to have had almost no impact on their premiums. The biggest increase in premiums for both sites occurred in 2002-2003, attributable not only to the ANI coverage increase, but also likely to the higher risk for all PWRs following the discovery of the reactor vessel leak at

Davis-Besse in 2002. The most notable difference between the two is that CP consistently had a much higher availability for the period 2005-2014.

The changing risk profile of the Virginia Sisters is more complex. Generally, the two sites had similar insurance risk profiles with annual premiums within $100,000 of each other. North Anna is slightly higher power, but is located in a less densely populated area. Both had similar availability, averaging 91%, for the ten year period 2005 to 2014. Surry tended to have slightly higher premiums during the period 2000 to 2008. During this time Surry received three NRC NOVs, and was only rated "high" during most NRC annual risk assessments. North Anna received NRC's highest ratings during this same period. However, beginning in 2009, the risk profiles flipped with North Anna having slightly higher premiums. In 2010, North Anna only received a high rating during its annual NRC assessment, while Surry had risen and stayed at the highest rating. In 2011, North Anna's location (Mineral VA) was the epicenter of the 5.8 magnitude earthquake that shook much of the east coast. Both reactors, which were at full power when the quake hit, were knocked off-line for 80 days – the first time in US nuclear history that an NPP had been shut down by a seismic event (Peltier 2012), and coming less than six months after Fukushima. Finally the following year, North Anna received its only NOV (2000-2014). Generally, examining premiums of the Virginia Sisters over the entire 15 year span, Surry was considered a higher insurance risk during the first nine years, and North Anna was higher during the final six years. Further their insurable risk generally fell between those of CP and STP.

2. Seabrook and Brunswick Nuclear Plants and ANI's Engineering Rating Factor

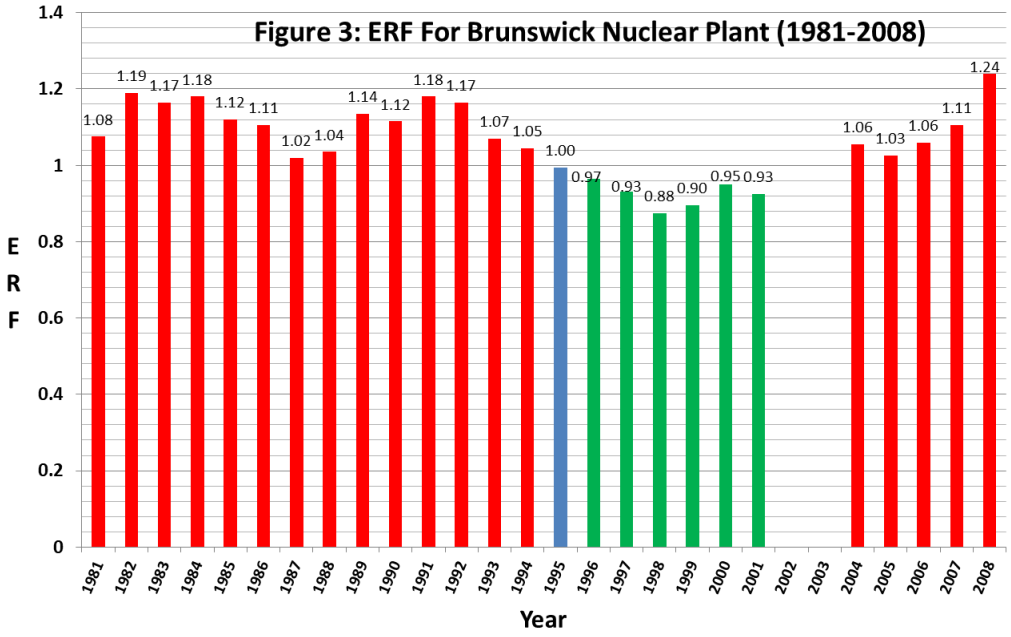
ANI's safety specialization is in managing risks and controlling losses associated with accidental radiological releases. ANI engineers audit safety activity and inspect every plant at least once a year in order to determine the facility's Power Reactor Liability Rating (PRLR). ANI uses the PRLR to determine a plant's annual advanced premium taking into account the plant design (type of plant, size, location and containment) and performance based on an Engineering Rating Factor (ERF). The ERF uses 10 factors to evaluate the reactor's performance including environmental release of radioactive materials, regulatory compliance, safety system failures, radwaste shipments, radiation exposure, safety system actuations, number of worker safety events, and unplanned automatic scrams. Based on the ERF, the performance of reactors of similar type are compared and used to establish annual premiums, rewarding the best performers and punishing those with the worst ratings. These adjustments are reflected in the following year's calculation of the plant's advanced premium. For example, the Seabrook Nuclear Station in 2002 started with an advanced minimum premium of $670,368 assuming a minimum ERF of 0.80 (ANI 2003). However Seabrook had ERF surcharges for:

• Environmental releases	$84,845
• Radwaste shipments	$2,891
• Safety system failures	$11,565
• Unplanned automatic scrams	$130,104
• Safety system actuations	$60, 715
	=======
Total surcharge of	**$289,120 (43%)**

This lead to a total revised advanced premium of $959,488 and based on an ERF of 1.23, which was well above the industry average for a single reactor site. Thus for being a less than average safety risk, Seabrook was surcharged 43% above the premium for ERF safest single site reactor.

Like INPO's index, ANI's ERF is highly confidential. Review of the NRC's public database reveals only one site – the Brunswick Nuclear Plant (BNP) - with an extended record of ERFs (Wendland 2008) covering the period 1981 through 2008 (Figure 4.3). The combined annual average ERF for the two BNP reactors ranges from a low of 0.875 in 1998 (less risky than average plant) to a high of 1.24 in 2008 (much more risky than average plant). While there are no ANI premium records for this plant during this period, one can speculate on the plant's premiums and risk profile. Over the 26 years of data (years 2002 and 2003 is missing), there were 19 years when the ERF was more than the industry average (1.0), and only 7 years when it was less than 1.0, with an average site ERF of 1.06. Thus BNP from ANI's perspective was less safe and likely paid higher premiums than comparable 2-reactor BWR sites operating at a similar power level. There is also some INPO index data (1996-2008) and complete NRC Licensee Event Report (LER) data (1981-2008) that can allow different perspectives on BNP safety. For the INPO Index, good safety is typically a rating of 90 or higher, with poorer safety having a rating of 80 or below. For NRC LERs, the smaller the number, the better. There appears to be relative consistency among the measurements with all three showing safer and generally improving results during the period 1996 to 2001, and declining safety results

in the period 2004 to 2008, with the INPO Index dropping below 80 in 2006, and the ERF peaking at 1.24 in 2008.



ND	ND	ND	ND	ND	ND	ND	ND	ND	ND	ND	ND	ND	ND	ND	89.30	90.40	95.00	96.60	97.50	99.30	ND	94.84	91.49	85.01	77.01	85.91	92.87	INPO INDEX
235	282	159	49	79	56	35	52	47	47	49	36	25	24	25	18	16	9	16	5	1	3	6	6	8	10	6	10	NRC LERs
1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009

Figure 4.3: ERF for Brunswick Nuclear Plant (1981-2008)(Source NRC)

In addition to establishing ERFs for underwriting and premium determination purposes, ANI engineers also make recommendations to policyholders on how to reduce the probability and consequences of possible losses. This includes making nuclear insurance risk assessments using traditional insurance industry methods. The focus of the ANI risk assessments is to reduce the probability of an accident and potential radiological health effects to plant workers and to the public. Specifically, the goal is to assure that plants comply with NRC guidelines and ALARA standards on radiological exposure and

protection. In this way, ANI independent radiological inspections supplement NRC inspections. The results are shared with operators and with groups that develop and modify safety performance standards for the nuclear industry (Olivera 1988).

ANI engineers and health physicists conduct industry training and plant workshops on ALARA criteria. They also produce manuals and bulletins on how to safely handle and dispose of radiological waste and assist plant staff in developing radiological emergency preparedness and evacuation plans. ANI also has an emergency response team which can quickly provide financial assistance to the public in the event a nuclear incident results in in an evacuation.

3. ANI's Secondary Financial Protection (SFP) Master Policy

Section 170(b) of the Price-Anderson Act requires all commercial power reactor licensees to participate in a retrospective premium program for loss in excess of primary financial protection. The program is written and administered by ANI. If needed, ANI, under the terms of its Secondary Financial Protection (SFP) Master Policy, would collect the retrospective premiums due, and administer the disposition of the funds including the settlement of claims. The SFP Master Policy is actually not an insurance policy, but rather a bond whereby the licensees contractually agree to pay ANI the retrospective premiums should circumstances warrant.

The SFP policy provides excess coverage for losses that exceed the maximum primary limit available under the Facility Form Policy. The current retrospective premium prescribed by the NRC is $131.056 million per rector (adjusted in 2018 for inflation), In addition, if the damages from a nuclear incident are expected to exceed the

financial protection amounts required under the Price-Anderson Act, the Act, each reactor must pay an additional 5% of its retrospective premium. This results in a maximum retrospective premium of $137.6088 million per reactor (times 94 reactors) bringing the total secondary protection to $12.94 billion. Annual installment payments of the retrospective premium are limited to $20.496 million per reactor, per incident.

Since the SFP is based on the number of reactors, there is ongoing concern about maintaining coverage levels as reactors shutdown and the number of reactors declines. Further, the financial risk is higher for those utilities that operate multiple reactors at multiple sites. For example, Exelon, that owns 16 reactors in operation at 9 sites, is potentially responsible for $2.2 billion in retrospective premiums per incident, and maximum annual premiums of nearly $328 million. Given this exposure, reactor owners closely monitor the safety of other pool operators and their abilities to meet their financial obligations. ANI as administrator of SFP currently receives an administrative fee of $19,175 per reactor per year. While they have no direct financial responsibility for secondary premiums, if an operator fails to pay its share of the retrospective premiums, ANI is obligated to pay up to $30 million and to collect the debt later.

B. Nuclear Energy Insurance Limited (NEIL) – Property & Power Outage Insurance

While the Price-Anderson Act does not require commercial nuclear power operators to have financial protection for their own property, NRC regulations (10 CFR Part 50) do mandate that licensees maintain a minimum of $1.06 billion in onsite property insurance at each reactor site. The purpose is to fulfill the licensee's obligation to stabilize the

reactor and decontaminate the site if an accident occurs. All US commercial nuclear power operators get their primary property insurance from Nuclear Electric Insurers Limited (NEIL). NEIL provides “all-risk” property insurance covering nuclear and other perils that could damage the facility. It also writes coverage for business interruption covering loss of use caused by an accident or other peril that disrupts electric power generation for an extended period of time.

NEIL is a nuclear mutual or "captive" insurance company that is owned and controlled by utility company members. As of March 2018, NEIL had 73 utility members, including Exelon, Duke Energy. Georgia Power, Consolidated Edison, Entergy, and Dominion Power. It is incorporated under the laws of Bermuda and based in Wilmington, Delaware. Since its inception in 1980 through the end of 2017 NEIL has collected $8 billion in premiums, earned nearly $9 billion from its investment portfolio, paid $3.7 billion in claims, and distributed $6.7 billion back to policyholders as annual and special dividends. Since NEIL property insurance covers “all-risks,” nearly all claims have been for non-nuclear events causing damage to plant generators and other equipment. As of the end of 2017, NEIL had $4.5 billion in reserves - a sufficient amount to cover claims from at least one catastrophic member event.

NEIL provides member companies with up to $1.5 billion per site of primary coverage, and $1.25 billion per site in excess coverage, for a maximum property coverage level of $2.75 billion per site per occurrence. NEIL’s 2018 Primary Property and Decontamination Liability Insurance Policy (NEIL 2019) has a term of one year and automatically renews. It covers damage to all of the insureds real and personal property,

including the land, and all buildings and structures. This includes the insured's legal obligations to protect the public health and safety by decontaminating the site. The policy is subject to numerous terms, conditions, deductibles, limits, sub-limits and exclusions that regulate the insured's risk behavior. The policy also contains several endorsements providing coverage from special hazards including acts of terrorism, windstorms, fire, floods, earthquakes, landslides and other movements of the earth. There are also exclusions including damage caused by gradual accumulation of radioactive contamination, fraudulent or criminal activities, normal wear and tear, and Acts of War.

Per NRC regulations, for accidents estimated to cost over $100 million, the primary coverage prioritizes reactor stabilization, decontamination, and site cleanup over other covered losses. Special extensions of coverage are given to removal of debris and contamination, and regulatory-required expedited repairs with policy sub-limits ranging from $2.5 to $20 million.

Primary coverage also has a mandatory deductible that typically is $2.5 million for the first $500 million of coverage. There are also higher deductibles of $10 million for non-nuclear events such as floods or windstorms, and lower deductibles for damage like expedited repair with sub-limits. Operators can also assume a quota share of the risk, for example 10% of the first $400 million, which is essentially up to a $40 million co-pay in return for a substantial premium discount. Operators tend to prefer coverage with higher deductibles and co-pays, to maximize deductible and quota share credits and reduce annual premium costs. Likewise, the insurer hopes that coverage limits and sub-limits,

along with high deductibles and co-pays will expose the insured to potentially high costs, thus encouraging them to minimize risks and maximize safety.

In addition to the $1.5 billion in primary coverage, all nuclear operators at their option can carry up to $1.25 billion in excess coverage under a separate "blanket" policy. Excess coverage is "follow form" meaning it only kicks in if the underlying primary coverage is exhausted. The terms and conditions are nearly identical to the primary policy except there is no deductible.

NEIL also provides accidental outage or "business interruption" coverage that reimburses the utility for loss of use of one or more reactors for electrical generating purposes following an accident. Under these policies, the insured can collect up to $4.5 million per reactor per week, with a coverage limit of $490 million per reactor for a nuclear outage event. The coverage kicks in following an initial deductible period ranging from 8 to 26 weeks. Other than the deductible period, the terms and conditions of this coverage are identical to the primary and excess policies.

All insured NEIL policyholders are required to be members of NEIL and be bound by the obligations and duties, of membership. As described in Section VI-C-2, all policyholders must be members of INPO and agree to INPO inspections and adhere to INPO standards of operation. NEIL membership also requires that the insured participate in a retrospective program whereby each member commits to providing a contribution to a pool if requested by NEIL. The annual contribution is listed in all policies as a multiple of the premium, often ten times the primary or excess premium, resulting in about $50 to

$60 million per site or approximately $2.9 to $3.5 billion for the current NPPs, and can be tapped if primary reserve funds are depleted.

Under the conditions of the primary, excess and power business interruption policies, NEIL is "permitted, but not obligated, to perform or to have performed on its behalf, evaluations of the Insured Property at any reasonable time." The evaluations are "solely for insurance purposes" to assure the insured's compliance with NEIL's loss control standards. NEIL's safety expertise is in preventing property losses and disruption to plant operations due to fire, natural hazards, and breakdown of non-nuclear components such as boilers and generators. NEIL's operating subsidiary Nuclear Service Organization (NSO) performs engineering and loss control functions focused on these areas. Likewise, NEIL's Engineering Advisory Committee reviews industry incidents to identify trends and ensure that the loss control standards are updated and relevant. Further, given NEIL's close relationship to INPO, they will be quickly notified of any discovered defect. If a "dangerous condition" is discovered through NEIL's or other parties evaluations, NEIL has the right to request that the property be taken out of service without delay, or that actions be taken to remedy the problem. If the insured fails to comply with the request (NEIL 2018), NEIL has the right to immediately suspend coverage. Likewise, NEIL can also immediately suspend coverage if the NRC suspends or revokes the operator's license.

In establishing the annual premiums for all of its policies, NEIL takes into account a number of risk factors that can impact the likelihood and severity of a claims event. For the nuclear component, some of the most important factors are the number, type, age,

energy output and operating status of reactor(s). After determining a weighted Nuclear Rate, quota share or other nuclear operations credits can be applied, followed by adjustment factors based on the relevance of other risks including from fire, floods, windstorms, and earthquakes. Also important is the size of the site, and the types of buildings and other site property that needs to be covered.

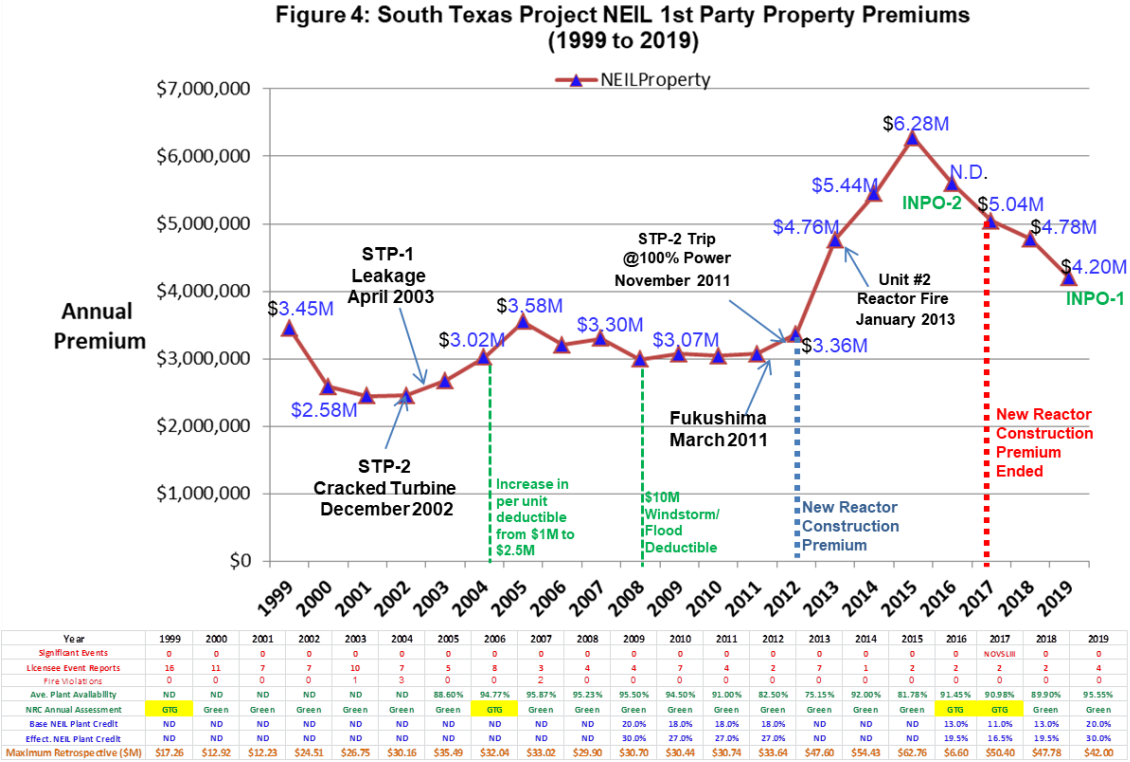
NEIL's primary interest is in determining the potential costs for long-term outages, site decontamination, and reimbursing the operator for equipment after depreciation. Additional credits can be given through the insured's assumption of more of the risk through higher deductibles and co-pays. Likewise, NEIL can apply substantial premium penalties based on the site's previous loss experiences. As a result, annual premiums for all coverages can vary among operator sites by millions of dollars based on all of the risk factors, credits, and penalties. Further, these higher premiums are magnified tenfold or more if a retrospective premium is demanded, potentially costing the operator tens of millions of dollars more for risky behavior.

As a mutual risk sharing organization, NEIL members have a vested interest in monitoring industry operations and eliminating any bad risks that might increase pool financial exposure and threaten the future existence of nuclear power generation. NEIL recently shifted its plant evaluation frequency from a time-based to a risk-based approach, concentrating its attention on those plants and issues that represent the greatest probability and consequences of loss. This includes focusing on issues that can improve plant operational safety such as compliance with applicable regulations; and overseeing

implementation of key safety procedures. NEIL also holds workshops and issues efficiency bulletins on their loss control standards.

1. South Texas Project NEIL Premium Analysis

A good example of NEIL property insurance coverage in the NRC library database is for the South Texas Project (STP) Units 1 and 2 covering the period 1999 to 2019 (NEIL 1999-2019). Throughout this period, STP had primary and excess coverage totaling $2.75 billion. The plotted results for NEIL premiums are shown in Figure 4.4. In interpreting this premium chart, there are a number of events and factors that need to be accounted for before one can speculate on both INPO ratings and NEIL's perceptions of the risk specifically for STP over time. These factors include NEIL adjustments to all member premiums based on their own business needs or events like Fukushima that alter the industry-wide risk profile. Operators like STP also request changes to their coverage such as adjusting the deductible or adding coverage for new construction.



Year	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Significant Events	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	NOVS LIII	0	0
Licensee Event Reports	16	11	7	7	10	7	5	8	3	4	4	7	4	2	7	1	2	2	2	2	4
Fire Violations	0	0	0	0	1	3	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0
Ave. Plant Availability	ND	ND	ND	ND	ND	ND	88.60%	94.77%	95.87%	95.23%	95.50%	94.50%	91.00%	82.50%	75.15%	92.00%	81.78%	91.45%	90.98%	89.90%	95.55%
NRC Annual Assessment	GTG	Green	Green	Green	Green	Green	Green	GTG	Green	Green	Green	Green	Green	Green	Green	Green	Green	GTG	GTG	Green	Green
Base NEIL Plant Credit	ND	ND	ND	ND	ND	ND	ND	ND	ND	ND	20.0%	18.0%	18.0%	18.0%	ND	ND	ND	13.0%	11.0%	13.0%	20.0%
Effect. NEIL Plant Credit	ND	ND	ND	ND	ND	ND	ND	ND	ND	ND	30.0%	27.0%	27.0%	27.0%	ND	ND	ND	19.5%	16.5%	19.5%	30.0%
Maximum Retrospective ($M)	$17.26	$12.92	$12.23	$24.51	$26.75	$30.16	$35.49	$32.04	$33.02	$29.90	$30.70	$30.44	$30.74	$33.64	$47.60	$54.43	$62.76	$6.60	$50.40	$47.78	$42.00

Figure 4.4: South Texas project NEIL First Party Property Premiums (1999 to 2019) (Source: NRC)

The data chart and table above includes two years of INPO report card grades (2016 and 2019), along with eight years of NEIL base and effective plant credit data (blue) which is based on the INPO index. In addition, NRC data related to INPO index calculations are given including significant events and LERs (red), as well as plant availability and annual plant assessment data (green) that takes into account the number of forced outages and unplanned scrams, and personnel radiation exposure. Generally, the NRC assessments over the past 20 years have been relatively uneventful, with only four years (1999, 2006, 2016-2017) highlighted in yellow being greater than green (GTG).

The table also includes the maximum retrospective premiums (orange) – a multiple of the premium - that NEIL could charge STP in case of a major industry event.

Analyzing the actual chart data, one is struck by an immediate 25% decrease in premiums between 1999 and 2000. While this may seem to represent a reduction in risk, the drop is actually attributed to an across the board 25% discount in rates for all NEIL insured plants. STP's premiums further decreased over the next two years (2001-2002) possibly indicating an improvement in STP's INPO rating during that time. However, beginning in 2003, STP's premiums began to increase significantly, rising 45 percent by 2005. Part of the change was due to the restructuring of all premiums by NEIL in 2003 to better reflect the assumed risks on a site-by-site basis. This resulted in an average premium increase of 10% per plant effective April 1, 2004 (NEIL 2003: 4). However, STP's increase was significantly more. Something seems to have occurred to alter the insurance risk profile for STP and possibly similar NPP sites.

In March 2002 at the Davis-Besse PWR plant near Toledo, Ohio onsite personnel discovered cracks and leakage at the top of the reactor pressure vessel (RPV). Later, the NRC described the discovery as the closest the nation has come to a nuclear accident since TMI-2, and the incident was subsequently rated INES Level 3 event (USNRC March 2002). Two rare NRC Bulletins were issued advising other PWR plants to inspect their upper head nozzles. The incident also triggered an even rarer INPO "Code Red" SOER in November 2002 (INPO 2002).

The Davis-Besse event affected the entire U.S. PWR fleet and may have resulted in the 2003 NEIL premium restructuring In December 2002, STP-2 experienced a manual

trip at 100% power caused by a crack in a turbine blade. The unit was out of commission for 37 days. A few months later during a scheduled refueling shutdown at STP-1, onsite personnel discovered a small leak at the bottom of its RPV – potentially a worse problem than at Davis-Besse. STP-1 was shut down for 4 months, the problem was fixed, the reactor was restarted, and the NRC released yet another rare bulletin alerting other operators of the problem. Subsequently, the STP plant had a 13% premium increase from 2003 to 2004, and a further 18% increase from 2004 to 2005. This increase would have been at least 5% higher except for STP agreeing to increase their deductible from $1 million to $2.5 million per reactor in the 2004 policy year. This evidence suggests that STP had a major downgrade of their INPO index in 2004-2005, with the subsequent reduction in their NEIL base and effective plant credit during this period.

From 2005 to 2006, premiums declined 10%, and then dropped another 6.5% by 2008 –essentially returning to 2004 levels – then holding steady between 2008 and 2011. This indicates that STP's risk profile was probably improving – evidence supported by its high availability (>95%), GREEN NRC assessments, no significant events, and few LERs or fire violations. This improvement is documented in maximum or near maximum base and effective plant credits for the period 2009 to 2011. Part of the reason for premiums to remain steady was the inclusion of a new $10 million wind and flood deductible by NEIL beginning in 2008.

Starting in 2012, there is a dramatic rise in STP premium rates, nearly doubling over the next three years to $6.28 million in 2015. There are a number of factors that could have contributed to this rise. First in March 2011, the Fukushima nuclear disaster

disrupted the risk models of both worldwide regulators and insurers, triggering a wave of costly safety evaluations and equipment retrofits. Ironically, less than a year before, Fukushima's parent company TEPCO had agreed to invest $125 million for two new reactors to be constructed at the South Texas site (TEPCO 2010). Not surprisingly, TEPCO's partner in the US withdrew from the project in April 2011. However, plans for the new reactors continued, preconstruction activities at the site commenced, and STP added $50 million in course of construction insurance beginning in 2012. In addition, the insured value of the STP plant site nearly doubled in 2012 from $2.2 billion to $4 billion. This combination of new insurance plus higher valuation certainly contributed much of the nearly 90% increase in premiums between 2012 and 2015. However, there were other risk factors that may have contributed to the increase. In November 2011, STP-2 once again had a trip at100% power when the main generator malfunctioned. The reactor was out of service for four months (Reuters 2012). Then in January 2013, a fire occurred at the main transformer feeding STP-2, once again taking the reactor out of service for another four months. For the November 2011 incident, NEIL paid STP $62.5 million in property repair and accidental outage costs (NEIL 2013: 26). There is no INPO or NEIL credit information for this period, but plant availability reductions in 2012 and 2013 may have negatively affected both measures, possibly leading to some of the premium increases.

In 2016, complete NEIL premium data is not available. However, partial data indicates that the NEIL base and effective plant operations credits were suboptimal, respectively at 13% and 19.5%. Reports to the NRC indicate that STP's INPO grade had

dropped from Category 1 to Category 2, with STP-1 experiencing three reactor trips in less than a year (STP 2016: 3). The performance got worse in 2017 with NEIL base and effective plant operations credits further declining to 11% and 16.5%, and the plant experiencing its first notification of violation for a significant event in over 20 years. In addition, STP annual assessments were Greater than Green for both 2016 and 2017. The premium for 2017 was actually 20% less than 2015; however most of this decline is related to the halt to construction plans and the removal of additional construction insurance in 2017. Premiums declined 5% in 2018, and another 12% in 2019 as STP returned to INPO Category 1 status with optimum NEIL base and effective plant operation credits respectively of 20% and 30%. The decline was also aided by a 15% credit given to STP for assuming a 10% quota share on the first $400 million of coverage (up to $40 million).

There are two other mechanisms embedded within the NEIL policies to internalize the risk with the operator and within the industry as a whole. The first is a 25% insured retention clause for the $2.25 billion of excess coverage above the initial $500 million in primary coverage. This clause is included in all NEIL policies through 2007, replaced by "to be determined" after that. The clause is meant to avoid disputes over aging plant valuations, but potentially leaves the insured liable for over $500 million in unrecoverable costs. The second internalization mechanism is the retrospective premium that could be demanded of all NEIL members in case of a major accident. The retrospective premium is ten times the primary and excess premiums, and is therefore directly affected by the INPO index and plant operational credits. Thus the maximum

retrospective premium for STP was nearly $9 million higher in 2017 when the plant was experiencing performance issues versus 2019 when it returned to INPO Category 1.

This example illustrates the many risk factors that influence nuclear property insurance premiums. Some of these factors are influenced by industry events such as Davis-Besse and Fukushima. Others are affected by the insured willingness to internalize more risk through higher deductibles, copays, and quota shares. However, insured safety behavior as measured by performance indicators such as NRC assessments, availability, claims history, plant operational credits, and INPO grades are significant factors in the variation of NEIL property premiums.

C. U.S. Government Backstop, Capital Markets & Nuclear Safety

Since the enactment of the Price-Anderson Act in 1957, the federal government through a number of economic mechanisms has been deeply involved in managing the financial risks associated with the operation of commercial nuclear power reactors. Initially, this included the requirement that all reactors as a condition of licensure have mandatory financial protection. Further, large commercial reactors were required to carry the maximum amount of private insurance available ($60 million) plus enter into a $500 million indemnity agreement with the AEC. In return, commercial nuclear power developed with the guarantee that operator exposure was capped by a $560 million liability limit.

Many in Congress and the public considered the indemnity and limit of liability to be a massive government subsidy to nuclear operators, enabling them to participate in activities that were potentially hazardous to the public. The Brookhaven and Rasmussen

studies clearly delineated this danger. From the government's perspective, Congress had to weigh the relatively low probability of a catastrophic accident against the national security and energy benefits of nuclear power development.

Over time the government gradually phased out the $500 million indemnity and imposed new legal constraints on the nuclear industry, including acceptance of strict "no fault" responsibility, channeling of liability to the nuclear operator, and waiver of defense in any nuclear accident lawsuits. Further, federal courts eventually were given jurisdiction over nuclear accident lawsuits and could then decide who, when and how much compensation was distributed to victims. In effect, the government granted the nuclear liability limit in exchange for the ability to rapidly compensate victims in the event of a major accident. Without a limit, it was believed that nuclear operators who experience an accident could go bankrupt, denying victims adequate compensation. .

When the Price-Anderson Act was enacted in 1957, it was implicitly understood that the government would have a role in compensating victims in the event that damages exceeded the limit of liability. This understanding was later explicitly recognized in the 1976 and 1988 Act renewals stating "that in the event of a nuclear incident involving damages in excess of the amount of aggregate liability, the Congress will thoroughly review the particular incident and will take whatever action is determined necessary and appropriate to protect the public from the consequences of a disaster of such magnitude" (P.L. 100-408 1988). This essentially created a fourth layer of unlimited financial protection. Price-Anderson does not specify how this potential public liability would be paid for. One clue is that in the event that liability costs exceed the secondary layer annual payment required of each commercial reactor owner, the

US Treasury would advance the money and pay for the obligation by the issuance of treasury bonds (P.L. 83-703). This is a similar solution to what the Japanese government used following the Fukushima accident in 2011.

The TMI accident also exposed a major flaw in in the secondary coverage system. It was assumed that coverage expansion would be funded by new reactor construction. Following TMI, all planned construction was cancelled and the number of operating reactors began to decline. While this decline has slowed, prospects exist that if the number reaches a low enough point, the NRC might once again have to provide an indemnity to maintain an adequate liability limit. Further, all parties know that another domestic accident would likely result in the end of nuclear power in the US.

Thus, maintaining nuclear safety at a sustainable cost is arguably an existential priority of all elements of the nuclear industry. This priority promotes an extremely high level of safety collaboration among nuclear operators, much higher than any other competitive industry. This collaboration extends to nuclear insurers and government regulators who possess specialized nuclear risk management knowledge and provide eyes and ears to monitor safety and reduce the probability of losses. The result is an unprecedented safety record unmatched by any other commercial industry which, by necessity, must continue in order for nuclear power industry in the US to survive.

VIII. Lessons That Can Be Applied to Other Emerging Technologies

How has insurance promoted better safety in the commercial nuclear power industry and what lessons learned can be applied to other emerging technological risk regimes?

Lesson #1: Mandatory Financial Protection as a Condition of Licensure

The Price-Anderson Act requirement of financial protection as a condition of licensure is a fundamental staring point tying nuclear insurance to nuclear safety. Power utilities could not get a license to build or operate a nuclear plant without having proof of financial protection equivalent to $560 million. Without a license, the issue of nuclear safety was moot. By signing an insurance policy, the utilities committed themselves to its terms and conditions including compliance with all regulations and adherence to the insurer's loss control standards.

Lesson #1: *Mandatory insurance as a condition of licensure provides public financial protection and also requires the insured to obey regulations and the insurer's risk control best practices.*

Lesson #2: Coverage Limits & Risk-Based Premiums

In the 1950s, commercial nuclear power was a new emerging technology that held great potential but also great uncertainty regarding accident probability and consequences. Through the use of stock and mutual pools, insurers were eventually able to provide an unprecedented amount of liability and property insurance protection - far more coverage than ever before. The pools' coverage limits signaled the maximum risk that they thought was acceptable. For this coverage, both the liability and property pools charged very high premiums, 30 to 40 times more than conventional power plants, and determined premiums based on individual plant risk factors.

In contrast, the $500 million government indemnity had very low premiums, 10 to 20 times less than the rates charged by private insurers for 8 times the coverage level, with no risk factors other than reactor power taken into account. These low premiums for high coverage failed to fully internalize the risk, and therefore did not maximize the incentives for safe operations.

Lesson #2: *Insurance can promote technological development. With risk-based premiums and coverage levels, insurance can also provide incentives for safe behavior.*

Lesson #3: Risk Pool Monitoring, Standards & Peer Collaboration

Early in the nuclear power era, human resources with knowledge in reactor technology and radiological safety were in short supply. During this period, the pools, composed of hundreds of insurance companies, provided many additional eyes to keep watch over the insured's behavior. They had staffs of health physicists and nuclear engineers who could report safety violations to the AEC, and could suspend insurance if violations were not corrected. The pools' engineering departments conducted risk assessments and developed ERFs to compare the relative safety of plants and determine fair premium. Over time, the composition of the pools changed with the establishment of mutual utility property pools such as NEIL providing a new level of peer review inspections and self-regulation. NEIL helped to establish INPO, and required their policyholders to be INPO members, agree to INPO inspections and adhere to INPO standards of operation. If a policyholder's membership in INPO lapsed, NEIL could suspend or cancel their insurance.

Lesson #3: *Insurance can provide regulators with additional surveillance, risk assessment, and enforcement capabilities and can encourage the development and adoption of safety standards.*

Lesson #4: Insurance Specialized Loss Management Services

As the commercial nuclear power industry matured, new industry safety institutions such as INPO came into being, and Congress created the NRC to focus on nuclear safety regulations.

Events such as the Browns Ferry fire and TMI-2 accident revealed that there was a need for specialized expertise in fire prevention and radiological release management, To fill this need, NEIL focused their inspections on fire prevention and ANI provided expertise on radiological waste disposal, ALARA training, and helping plants develop emergency plans. These specialized services complemented the inspection and risk assessment activities of the NRC and INPO.

Lesson #4: *As technology becomes more mature, specialized safety and risk management needs may evolve that can best be satisfied by insurance industry expertise and capabilities.*

Lesson #5: Role of Extraordinary Events in Shaping Insurance & Safety

For the first 20 years of US commercial nuclear power operation, no events having a significant impact on the public or resulting in third- party liability claims occurred. The TMI-2 accident in March 1979 caused a radical shift in the public's perception of nuclear power safety, development of new NRC safety goals, and the emergence of new

institutions such as INPO, and NEIL, to develop safety standards and performance metrics to better manage nuclear risk.

Lesson #5: *Extraordinary events with catastrophic financial consequences can have a profound effect on the evolution of public and private insurance mechanisms for new emerging technology.*

Lesson #6: Protection of Technological Investment & Risk Internalization

Utilities, when they decide to build a NPP, invest billions of dollars and well over a decade's time before the plant can become operational. Once operational, these plants can provide a substantial portion of their revenue by generating much of their electricity at a relatively low cost. As demonstrated by the TMI-2 and Fukushima accidents, the cleanup and loss of use costs can be devastating for the utilities involved. Further, public and regulatory reaction to any nuclear accident can have an adverse economic effect on the nuclear industry. Thus, much of the risk associated with a nuclear accident is already internalized by the utilities through their potential loss of a large capital investment, loss of business use, and loss of public reputation.

Lesson #6: *Having valuable assets, business revenue and reputations at risk can be a strong motivator for both firm and industry safety.*

Lesson #7: Retrospective Coverage & Internalization of Risk

In the early-1970s the AEC was looking at ways to phase out the indemnity and replace it with a solution that would better internalize the risk with the nuclear industry. In response, an industry-sponsored retrospective premium plan was implemented as part of the 1976 Price-Anderson extension. The advantages of the retrospective plan were that

it shifted more of the risk to operators allowing the indemnity to be phased out while not burdening operators with immediate high premiums. It also made the nuclear industry as a whole responsible for the behavior of each individual member. To manage this responsibility, the industry created INPO to conduct inspections and create peer pressure to improve safety performance.

Lesson #7: *Retrospective coverage can internalize risk with technology firms and their industry. It can improve safety by increasing surveillance and peer pressure to deter risky firm behavior.*

Lesson #8: Refocus on Operational Safety & Safety Goals

Following the TMI-2 accident, the Kemeny Commission found that there was too much reliance on technology and safety systems, and too little attention paid to the human aspects of safety including training, procedures, organizational structure and operator safety attitudes. In response, the NRC created new safety goals, the nuclear industry committed to more self- regulation, INPO established new safety performance metrics, and nuclear insurers focused their attention on specialized areas of operational and human safety.

Lesson #8: *As new risks emerge there may be an over reliance on safety technology, and too little focus on other aspects of safety. Insurers can play a role in refocusing firm safety mindset.*

Lesson #9: Insurance Adapting to Change & New Risks

For over 60 years since the first commercial nuclear power plant went into operation, the nuclear insurance regime has had to adapt to changes in the industry's risk profile. To

respond to these changes, the insurance pools created new policy types, amended policy language, added coverage, and modified their inspection, assessment and premium determination processes.

Lesson #9: *As emerging technologies evolve over time, new risks can arise. Insurance can respond to these changes through the creation of new risk management products and services.*

IX. Conclusion

This case study examined the role that insurance played in helping to regulate, promote safety and manage risks for firms operating commercial NPPs in the US. Early evidence showed that without the financial protection provided by the insurance pools, private sector investment in commercial nuclear power would likely not have occurred. Evidence also showed that during the AEC era, insurance played a moderating safety role balancing the AEC's nuclear power promotion agenda with sound insurance industry risk assessment and loss prevention services.

Following the TMI-2 accident in 1979, the role of insurance in nuclear safety changed. Through Price-Anderson renewal enactment of mandatory retrospective coverage and NRC requirements for property coverage, more of the nuclear risk was internalized by nuclear operators. To manage this increased accountability, nuclear operators with the support of insurers, created new institutions such as INPO to develop safety standards and performance benchmarks, and participated in more industry self-regulation through peer-review inspections and risk assessments. The insurance pools encouraged these activities by mandating INPO membership and compliance with NRC

regulations as a condition of coverage. The insurance pools also developed specialized risk management services such as fire prevention and performance metrics such as ERF that complemented NRC and INPO activities.

Finally, it is important to note, based on nuclear insurance industry claims history, the US commercial nuclear power industry has had an exceptional safety record. No deaths have ever been attributed in the US to a commercial nuclear power reactor accident. This case study has not argued that insurance is the primary reason for this outstanding safety record or that it is the principle institution involved in nuclear risk management or safety. Rather, it is a key variable in explaining the safety behavior of operators, regulators, other institutions and nations in managing nuclear risk, without which commercial nuclear power, as we know it, might not exist.

Chapter 5: Insurance as a Private Sector Risk Regulator & Promoter of Safety: Managing Environmental Risks at U.S. Chemical & Waste Disposal Facilities

I. Introduction

How has insurance promoted better safety in the chemical and hazardous waste treatment industries and what lessons learned can be applied to other emerging technological risk regimes? This case study examines the role that insurance plays in promoting safety and managing environmental risks for firms generating and disposing of hazardous waste in the United States.

Up until 1962 and the publication of Rachel Carson's *Silent Spring* (Carson 1962), government officials, insurers, and the public were generally unaware of the hazards caused by the release of harmful substances into the environment. Prior to the book's release there were no federal agencies specifically responsible for environmental regulations and few federal laws regarding hazardous waste disposal. Most pollution problems were settled by litigation among the parties involved using state or local ordinances. Insurers usually provided coverage for environmental risks under their Commercial General Liability (CGL) policies.

This case study will trace the process of environmental insurance development and the evolution of environmental safety before and after a seminal event - the Love Canal health emergency. For insurers of emerging technologies it is a cautionary tale. Unlike the nuclear insurance regime, there has never been any limit of liability and no federal

backstop to cover catastrophic losses. As a result, many insurers initially underestimated the risk and became entangled in the environmental liability crisis of the 1980s that caused some to become insolvent. The environmental insurance regime that emerged from this crisis required insurers to become much more proactive in managing their clients' environmental risks.

The case study provides evidence that insurance can be a powerful public policy tool in incentivizing private sector companies to proactively manage environmental and other emerging technological risks. It can motivate firms to invest ex ante in loss prevention measures. Insurers also have resources and business motivation to verify and facilitate safe client behavior through specialized information gathering, targeted risk assessment, and loss control capabilities.

A key finding of this case study is that there is a synergistic relationship among insurance, regulation, and litigation that when properly aligned can optimize firm risk management behavior and consequently the safety of the public. Each element provides both incentives and penalties that influence firm safety behavior. All three elements also gather information on firm safety either before or after an accident occurs. However, the evidence in this case study suggests that insurance can be a better ex ante public policy mechanism for collecting information, assessing risk, and motivating private sector firms to invest in safety before an accident occurs.

The organization of the remainder of this case study is as follows. Section II describes the early history of the US chemical production and hazardous waste disposal industries prior to the founding of the EPA in 1970, and the insurance regime that developed to

support their activities. Section III provides an overview of the political economy, risks and uncertainties related to the production, use of chemicals, and the treatment, storage, and disposal of chemicals and hazardous waste. Section IV next discusses environmental laws that were enacted in the early-1970s, the rising level of litigation, and the development of Environmental Impairment Liability (EIL) insurance. Section V then describes the Love Canal health emergency and the pivotal role it played in the development of US environmental policy and the liability crisis that enveloped the hazardous waste and insurance industries during the 1980s. Section VI reviews and analyzes the post-Love Canal environmental legal and political conditions and how industry and insurers attempted to cope with the growing environmental liability crisis. Section VII outlines the roles that regulation, litigation and specialty insurance play in managing firm environmental risk behavior. Section VIII presents evidence of the roles of regulation and insurance in managing environmental safety using data from the EPA's RCRA database with evaluation and violation data for 1808 U.S. TSDFs over the period 1980 to 2020, including historic safety and financial protection performance. Section IX then gives lessons that can be applied to new emerging technologies, with Section X providing conclusions.

II. Early Historical Background – Laws, Litigation, Insurance & Events

This section describes the period from the early-1880s when no environmental laws existed and firms were free to pollute with little legal or liability ramifications, through the end of the 1960s when the environmental movement, triggered in part by notable

environmental disasters and the publication of ***Silent Spring***, began to exert influence in legislation and in the courts.

A. Early Regulatory and Litigation History

During most of US history, environmental risks were largely dismissed with the ignorant belief that pollution posed little threat to people or property. Air and water pollution were considered a public or private nuisance that, if necessary, could be litigated between the plaintiff and the alleged polluter in court. Pollution was also considered a local issue that had little impact outside of the immediate vicinity of the discharge. All industries and nearly all cities dumped their wastes and sewerage raw and untreated into the nearby waterways (Hines 1966, 202). Eventually, states and municipalities, recognizing the risks to public health, implemented measures to protect the quality of domestic water supplies. Laws were enacted in many states making the dumping of sewage and refuse into waterways a criminal offense; cities were granted powers to abate pollution contaminating their water supplies; and local boards of health were created to monitor the quality of water consumed for domestic uses (Hines 1966, 202). By 1930, most states responded to expanding water pollution problems by vesting regulatory authority in one or more state agencies – most often, the state's Department of Health (Hines 1966, 203).

Likewise, to deal with air pollution, local and state governments took the lead. In 1881, two cities, Chicago and Cincinnati, enacted smoke abatement ordinances. By 1940, 200 cities had implemented such ordinances with about a quarter also establishing smoke abatement agencies (Stern 1982, 44). By the early 1940s, smog was recognized as a

major problem in the Los Angeles basin, and in 1947 California authorized the creation of Air Pollution Control Districts in every county of the state, with the first established in Los Angeles County (Stern 1982, 48).

The first federal regulation involved in protecting the nation's water was the *Refuse Act of 1899* (EPA 2020). The act outlawed the "dumping of refuse that would obstruct navigation of navigable waters, except under a federal permit." (P.L. 55–425, S. 407). Thus, Congress did not consider the Act to be anti-pollution legislation, but rather a law to protect navigation. However, over time, the courts broadened the definition of "refuse" to include "anything which has become waste including foreign substances and pollutants" (*U.S. v. Standard Oil* 1966). In 1936, the 9th Circuit Court determined that oil and other chemicals spills could be consider refuse under the Act since they presented a fire hazard that could impede navigation (*U.S. v. Alaska Southern Packing Co.* 1936). The Act was enforced by the US Army Corps of Engineers who could issue legal dumping permits, or ask the Department of Justice (DOJ) to prosecute offenders. Violations were considered a criminal misdemeanor punishable by a fine of not more than $2500 or less than $500 or by imprisonment not to exceed one year (P.L. 55–425, S. 411).

B. Early Environmental Disasters

In the late-1940s and early-1950s, several manmade environmental disasters occurred that highlighted the threat to public health and property damage from pollution, and ultimately changed the face of environmental protection in the United States.

In 1948, one of the worst air pollution disasters in US history occurred in Donoro, a small steel mill town with a population of about 14,000 located in southwestern Pennsylvania. From October 27 to 31, thick smog covered the town, eventually resulting in 20 immediate deaths and causing severe respiratory problems for nearly half the population. This event led to the first large-scale epidemiological investigation of an environmental health disaster by the newly formed United States Public Health Service (USPHS). Later studies found the rate of death from cancer and cardiovascular disease in Donora from 1948 to 1957 was also significantly elevated versus expected rates (Ciocco and Thompson 1961). Over 130 lawsuits totaling $4.6 million were filed against U.S. Steel, with the company eventually settling with all claimants in 1951 for $235,000 without accepting blame (Boissoneault 2018).

A similar but much more deadly air pollution disaster occurred in the United Kingdom in December 1952. Known as the Great Smog of London, the event killed at least 4,000 people, with later studies estimating that as many as 12,000 excess deaths occurred between December 1952 and February 1953 because of the pollution's acute respiratory effects (Bell and Davis 2001). However, this was mostly a stealth event. Londoners were so use to thick "peasouper" fogs that they gave little notice. Ambulance service stopped and many victims died in their homes. Hospitals did not immediately recognize the disaster, and did not attribute increased admissions and death rates to the smog. The government did not react to the disaster until the increased death rates were reported to parliament on December 18th. An investigation eventually led to the passage of Europe's first national pollution legislation - *The Clean Air Act* – in 1956.

There were also severe water pollution disasters as well. Most notably in November 1952, the heavily polluted Cuyahoga River near Cleveland caught fire causing over $1 million damage. The blaze was caused by the ignition of oil leaking from the Standard Oil facility which formed a two-inch thick slick that spanned the river. The fire was not the first on the river or the last. Also many other industrial cities including Detroit and Philadelphia had dealt with similar water pollution infernos (Adler 2014).What made the 5-alarm 1952 fire unique was the symbolism it provided to a much less severe fire on the Cuyahoga on June 22, 1969. An alleged photograph of the 1969 fire published in *Time Magazine* made it a "seminal" event in the history of water pollution, helping to spur the growth of the environmental movement and the passage of national legislation, including the *Clean Water Act* in 1972 (Adler 2002). The *Time* photo was actually of the much more severe 1952 fire that destroyed a shipyard and a nearby bridge.

C. Early Environmental Insurance – CGL Pollution Occurrences & Exclusions

As originally conceived in the 1940s, CGL coverage was meant to be "comprehensive" covering "all-risks." A few risks such as "acts of war" were excluded; however since environmental risks was not specifically mentioned, coverage was available so long as the policies standard conditions were met. Prior to 1966, one key condition was that coverage was limited to third-party claims resulting from "an accident." Thus, only sudden and accidental discharges of a pollutant were covered – pollution liabilities arising from intentional acts or omissions were not. Most CGL policies also contained an "owned property" exclusion that precluded coverage for

damages to their own property. However, companies could get first party coverage for environmental risks via a comprehensive property and casualty (P&C) policy.

In 1966, the insurance industry began revising the broad language found in CGL and P&C policies to reduce the likelihood that such policies would be interpreted to provide coverage for all environmental claims. Both standardized forms were modified substituting the word "occurrence" for "accident," and then defining an occurrence as "an accident, including injurious exposure to conditions, which results, during the policy period, in bodily injury or property damage *neither expected nor intended* from the standpoint of the insured" (Landow-Esser & Spears 1992, 68). In one sense, this change broadened coverage by allowing the insured to be covered for gradual pollution occurrences. However, the change also placed more emphasis on the intent of the insured and whether the event was foreseeable, better allowing denial of coverage for the failure to disclose information about the nature of the environmental risk.

Two major oil spills in the late-1960s drove insurers to reconsider their coverage for both accidental and gradual pollution events. In March 1967, the supertanker *SS Torrey Canyon* ran aground on a reef off the coast of the United Kingdom, breaking apart and spilling over a half million barrels of crude oil. The spill fouled beaches along the coastlines of Britain, France and Spain, and, at the time was the world's worst oil spill.

Two years later in early-1969, a blowout on an oil rig off the coast of Santa Barbara, California dumped an estimated 100,000 barrels of oil into the sea. At that time it was the largest oil spill in US waters, and remains the third largest offshore spill in US history. These and other pollution disasters led Lloyds of London to impose restrictive

endorsements upon its policies for pollution coverage (Hourihan 1980, 555). Soon after the US insurance industry implemented a pollution exclusion in June 1970. This exclusion was meant to eliminate coverage for gradual pollution. A second exclusion applied to oil and natural gas operations, and specifically eliminated coverage for bodily injury or property damage arising out of the discharge of oil or other petroleum derivatives into or upon any water course or body of water, whether or not the discharge was sudden or accidental (Hourihan 1980, 555). Thus coverage for accidents like *Torrey Canyon* or Santa Barbara would be excluded.

While these exclusions were a protective action on the part of the insurance industry, they also served a very specific safety purpose. They signaled to affected industries and to the world that the risks associated with gradual pollution and oil spills were no longer insurable under standard CGL and P&C policies. This would lead to the development of specialty lines of insurance with more stringent safety requirements for coverage. These requirements would include compliance with new federal environmental laws passed by Congress in the 1970s, and environmental regulations administered by newly created federal institutions including the EPA.

D. "Silent Spring" and the Environmental Movement of the 1960s

Despite these and many other less publicized environmental disasters during the 1950s, medical professionals, government officials, and the general public remained mostly unaware of the dangers of chemical pollution to wildlife and human health. This lack of perception changed radically in 1962 with the publication of Rachel Carson's landmark book *Silent Spring.*

Prior to its publication, a condensed version of *Silent Spring* was released in a series of three articles in *The New Yorker* beginning with the June 16, 1962 issue. This immediately gave it a wide and influential readership, including President John F. Kennedy, who on August 29, 1962 announced that he had set up a special panel to investigate the environmental issues cited in articles. The book was subsequently released on September 27, 1962 becoming an immediate best seller, with over 600,000 copies sold by the end of 1962 (Lear 1993, 38). Late in 1962, CBS television announced that it would produce a special on the book the following spring. "The Silent Spring of Rachel Carson" aired on April 3, 1963, dramatically escalating its influence. The following day Senator Abraham Ribicoff (D-CT) announced that he would conduct a congressional review of environmental pollution, including the roles that federal agencies play in regulating the use of hazardous chemicals (Lear 1993, 39).

In *Silent Spring*, Carson wrote that "For the first time in the history of the world, every human being is now subjected to contact with dangerous chemicals, from the moment of conception until death" (Carson 1962, 15). The first senate hearings began on May 16, 1963 with the expressed goal “to examine the role of the Federal Government as it deals with one of the great problems of our time: man's contamination of his environment” (US Senate 1963, 1). Rachel Carson testified on June 4th, noting that “We have acquired technical skills on a scale undreamed of even a generation ago. We can do dramatic things and we can do them quickly; by the time damaging side effects are apparent it is often too late, or impossible, to reverse our actions” (US Senate 1963, 207).

With the publication of *Silent Spring*, the word "ecology" became part of everyday vocabulary. Further, it is frequently cited as a primary catalyst inspiring the environmental movement of the 1960s. Carson believed that pesticide regulation should not reside with the Department of Agriculture that had the conflicting role of promoting pesticide use and safety. Rather she believed that a separate agency should be created focused on keeping the public safe from environmental hazards. Such a body, the EPA, was ultimately established in 1970.

III. Political Economy, Risks and Uncertainties of Chemical Production & Disposal

This section discusses the political economy of chemical production and hazardous waste disposal. It includes a brief overview of the benefits of pesticides and other chemicals, and the costs associated with their production, use, and disposal.

Rachel Carson during her Senate testimony recognized the benefits of some pesticide use, but noted that: "if we are ever to solve the basic problem of environmental contamination, we shall have to begin to count the many hidden costs of what we are doing, and weigh them against the gains" (US Senate 1963, 209).

A day before the Senate hearings began, the President's Science Advisory Council (PSAC) released its report entitled "The Uses of Pesticides" (White House 1963).While the PSAC's report specifically focused on the environmental benefits and hazards of pesticides such as DDT, the analysis and recommendations were applicable to other types of chemical compounds as well. In its report, the PSAC outlined the merits of pesticides while cautioning "advances have always entailed a degree of risk which society must weigh and either accept, or reject, as the price of material progress" (White House 1963,

1). Advances included improved food production through the cost-efficient control of harmful insects and plants; and enhanced human health by reducing the spread of diseases like malaria and yellow fever via mosquitos and other pests.

However, in the early-1960s, the costs and risks associated with pesticide and other chemical dispersion and use were less clear. It was known that specific chemicals in specific concentrations could cause acute toxicity resulting in fish and bird kills, and poisoning deaths in humans. Less clear at the time were the long term health effects of persistent exposure to low-levels of toxic chemicals, though it was suspected these substances could cause cancer, birth defects, and genetic mutations in either animals or humans. Further, it soon became clear that pesticides sometimes killed beneficial insects and plants that protected crops, and some targeted insects developed resistance to specific pesticides, rendering their use increasingly ineffective.

The PSAC report noted that traces of toxic chemicals had been detected in many food items, in man and in animals, oftentimes at great distances from the suspected source, and sometimes persisted in the environment for long periods of time (White House 1963, 4). Dispersion can be sudden such as from catastrophic oil spill; or gradual from a buried source that might occur slowly, undetected over decades. Contaminates can be carried from one locality to another by air currents, water runoff, and via living organisms, inhaled from the air, ingested from food and water, and absorbed through the skin. Thus, by the early-1960s, pesticides and other types of pollution were quickly becoming a ubiquitous and surreptitious threat to public health and safety.

This emerging threat was a concern to both chemical and waste disposal companies, as well as to their insurers. Up until this time, there had been zero or near zero cost for polluting the environment and any liability costs arising from the discharge of hazardous chemicals was covered by insurance under their CGL policies. The new public and government awareness of environmental hazards introduced a plethora of uncertainty and risk unforeseen by any of these parties. Foremost among their concerns was the prospect of complex and costly litigation (Liability Risk) complicated by many little understood pollution risk factors such as delays in detection, latency periods, multiple sources and pathways of contamination, and unclear causal links between toxic chemicals and public harm. With increased government involvement, there was also the fear of new costly laws and regulations, and the possibility of huge regulatory fines for violations or non-compliance (Regulatory Risk). The pollution problem was also evolving with new chemicals and environmental hazards being introduced by companies every day. Thus there was no clear understanding of the frequency or magnitude of potential losses.

IV. Environmental Regulation, Litigation & Insurance in the 1970s

This section describes the period in the 1970s when the environmental movement was in full swing, the EPA was created, Congress enacted many federal air and water pollution laws, and firms were required to have proof of financial responsibility for environmental liabilities. During this period, environmental liability insurance coverage evolved from being a standard part of most firms' CGL policies, to being excluded from such policies, forcing firms to buy specialty environmental impairment liability (EIL)

insurance as their federally required proof of financial responsibility for pollution hazards.

A. Environmental Laws and New Environmental Institutions of the Early 1970s

The modern federal regulatory infrastructure to protect the environment was created through Congressional legislation and by presidential executive order during the early-1970s. The first of these actions took place on January 1, 1970 when President Richard Nixon signed into law the *National Environmental Protection Act* (NEPA) (P.L. 91-190). Specifically NEPA Section 102 established a national policy to protect the environment and required all federal agencies to detail the environmental impact of "major Federal actions significantly affecting the quality of the human environment." NEPA's most important requirement was that all federal agencies had to conduct an Environmental Assessment (EA) and produce an Environmental Impact Statement (EIS) for every proposed federal activity. The EA and EIS provide public officials with relevant information and the potential environmental consequences of each proposed project.

In July 1970, President Nixon issued Reorganization Plan No. 3 that transferred 15 programs from existing executive branch departments into a strong new independent agency – the Environmental Protection Agency (EPA) (White House 1970). The mission of the EPA would be to establish and enforce environmental protection standards, conduct environmental research, provide assistance to states and other groups combatting environmental pollution, and develop recommendations on new policies for environmental protection. EPA's first administrator, William Ruckelshaus, was

confirmed by the US Senate on December 1, and the EPA officially came into existence on December 2, 1970.

Over the next few years more than twenty major federal environmental laws were enacted or substantially amended, giving EPA enormous regulatory and enforcement powers. Thus, through NEPA, the establishment of the EPA, and new environmental laws, US environmental policy was transformed in a few short years from limited federal government involvement into a comprehensive national regulatory program to manage air, water and other pollution risks. This new federal environmental regime also empowered citizens to file lawsuits against federal agencies and polluters who violated the new pollution laws to help ensure they would be implemented and enforced (Percival 1995, 1161).

B. Environmental Lawsuits and Challenges to CGL Insurance Exclusions

During the 1970s, citizens and local governments increasingly turned to the courts and litigation seeking compensation for damage to the environment and injuries arising from environmental contamination. In turn, companies accused of pollution violations and the target of pollution lawsuits looked to their insurers for support in litigation defense and paying for settlements, fines, and cleanup costs when judgments did not go in their favor. As a result, the language in CGL policies, especially related to exclusions, came under intense scrutiny.

Through its 1966 CGL policy modification the insurance industry aimed to exclude coverage for intentional polluters including pollution losses resulting from normal business activities. Their justification for denying coverage was to incentivize companies

that knowingly polluted to improve their manufacturing and waste disposal processes (Rosenkranz 1986, 1253). However in 1972 an Ohio appellant court decided that a long time intentional polluter could be covered for damage to adjacent property. In *Grand River Lime Company v. Ohio Casualty Insurance* (Grand River Lime 1972*)* the court ruled that even though Grand River had intentionally emitted pollutants for seven years as part of its normal business, the damage to surrounding properties was completely unexpected and unintended. Further, the court added that Ohio Casualty had full knowledge of the nature of that company's business, and could have excluded coverage when the policy was initially issued (Soderstrom 1976, 765-766). Thus, Ohio Casualty was responsible for paying for Grand River's settlement as well as legal defense costs. Following the Grand River Lime decision, the insurance industry acted swiftly to standardize the pollution exclusion in all CGL policies, reemphasizing the industry's intent to limit pollution coverage to occurrences that were "sudden" and "accidental" causing "damage" specifically to "offsite third-party" property. Over the next 20 years, the meaning of these words would be debated in many environmental lawsuits involving billions of dollars in claims.

The seminal case challenging the wording of the CGL pollution exclusion occurred in *Lansco, Inc. v. Department of Environmental Protection (NJ) and Royal Globe Insurance Companies et al. (Lansco* 1975) decided December 4, 1975. The essential facts of the case were as follows. Lansco leased property bordering the Hackensack River where it maintained tanks for the storage of asphaltic oil. Sometime during the night of December 29, 1974 vandals opened the valves on two storage tanks, causing some 14,000

gallons of oil to leak from the tanks, making its way into the Hackensack River. Under New Jersey environmental statutes, Lansco was obligated to pay for the cleanup. Lansco notified its insurance carrier, Royal Globe, but the insurer denied coverage based on the grounds that the occurrence was neither sudden nor accidental within the meaning of the exclusion clause. Further, Royal contended that the CGL policy did not cover statutory liability for cleanup costs. Royal and most other insurance carriers gave “sudden and accidental” a temporal meaning, instantaneously taking place at a distinct time and place, like an explosion. However the court determined the terms “sudden and accidental” were not defined in the policy, and therefore must be interpreted from the standpoint of the insured. The court then found that a common definition of these terms is “unexpected and unintended,” and consequently determined that "since the oil spill was neither expected nor intended by Lansco, it follows that the spill was sudden and accidental.” Thus the court ruled in favor of Lansco and required Royal to pay for all statutory cleanup costs, interest on past due cleanup debt, and all legal fees (*Lansco* 1975).

The Lansco definition of "sudden and accidental" became the foundation for a number of subsequent decisions, literally opening the flood gates to new “gradual” pollution lawsuits in the 1980s. The Lansco decision created a great deal of uncertainty within the insurance industry regarding judicial interpretation of policy language and the possible impact on future environmental claim exposures. This came at a time when Congress was considering new federal laws requiring owners and operators of hazardous waste facilities to provide proof of financial responsibility for third-party environmental liabilities.

C. Resource Conservation and Recovery Act and Required Financial Protection

In 1975, the EPA conducted studies of 13 industries that were key generators of hazardous waste (Hickman 1975). They found that approximately 90% of the hazardous waste generated by those industries was managed by practices which were not adequate for protection of human health and the environment (Federal Register 1978, 58948). In response, Congress on October 21, 1976 passed the *Resource Conservation and Recovery Act* (P.L. 94-580).

RCRA Subtitle C established a comprehensive program to protect the public health and environment from improper disposal of hazardous waste. Under these provisions, EPA was required to establish minimum federal standards applicable to all who generate, transport, treat, store or dispose of such wastes. Within eighteen months of RCRA's passage, the EPA was required to create a list of hazardous wastes that would be subject to regulation, and establish standards applicable to generators regarding recordkeeping, labeling, and use of appropriate containers for transport and storage. The RCRA also established a rigorous cradle-to-grave manifest control system to track and assign responsibility for hazardous waste throughout its lifecycle. The manifest is a control and transport document that accompanies the hazardous waste at all times from its point of generation to its point of disposal.

Under RCRA Section 3004, owners and operators of treatment, storage, and disposal facilities (TSDFs), including any generators retaining over 1,000 kilograms of hazardous wastes for more than 90 days had to also comply with additional requirements regarding monitoring, inspections, facility design, operating practices, and contingency plans in

case of an accident. Each owner or operator of a TSDF was required to apply for and obtain a permit to operate the facility from either the state or federal EPA. If the requirements above were not met, the permit could be revoked. One additional requirement for permitting was that TSDF owners and operators provide "assurances of financial responsibility" for environmental liabilities demonstrating their ability to pay for third-party claims resulting from a release of contaminants and for closure/post-closure care costs. Over time the EPA proposed (Federal Register 1980) and eventually implemented rules requiring TSDFs to have coverage for $1 million per occurrence and $2 million yearly aggregate for sudden events, and $3 million per occurrence and $6 million yearly aggregate for non-sudden (gradual) pollution events (Federal Register 1982). In its initial proposed rules, the EPA admitted that it had difficulty establishing indemnification levels due to the lack of actuarial data on the regulated waste management industries (Federal Register 1978).

Initially, insurance, self-insurance or a combination of the two was accepted by the EPA as proof of financial responsibility. To demonstrate the existence of insurance coverage, TSDF owners and operators had to submit a Hazardous Waste Facility Liability Endorsement or a Certificate of Liability Insurance to the appropriate federal or state government official (Hale & Bailey 1988). To respond to this need for environmental insurance as a condition of permitting, the insurance industry began to develop a new type of policy that would meet EPA liability guidelines, while not exposing themselves to unacceptable claims losses.

D. Environmental Impairment Liability (EIL) Insurance and Safety

In 1972, around the time the standard pollution exclusion was being finalized in the US, a group of European reinsurance companies began joint meetings in Paris to discuss the gradual pollution liability insurance problem. They were particularly concerned about the uncertainties surrounding new regulations and standards of care, and the unknown harmful qualities of past, current and future pollutants. Under the leadership of London insurance broker H. Clarkson, Limited., the group devised a plan to conduct technical surveys of prospective client plants, management and processes to assess the risk, develop premiums, and underwrite a new form of specialty insurance. The coverage which emerged from these discussions was subsequently embodied in an Environmental Impairment Liability (EIL) policy.

Prior to the launch of EIL, Clarkson organized an international network of cooperating research organizations with representatives from each country where coverage would be offered. Each participating organization of what became known as the Environmental Risk Analysis System (ERAS) was asked to assist in the development of a risk categorization system based on the special industrial, social, legal, and regulatory conditions in their country. The system developed assigned a numerical value to each industry based on key environmental hazards.

The ERAS insurance industry risk classification system and risk assessment process (Table 5.1) predated US government efforts, including those of the Nuclear Regulatory Commission (October 1975), EPA (December 1975) and the National Academy of Science "Red Book" (1983). The system and process consisted of a number steps leading

to the calculation of “environmental impairment units” for a particular polluting industry, and the evaluation of a number of individual factors resulting in the calculation of insured’s specific risk rating.

For the risk classification system ERAS examined the inherent environmental claims potential of more than one hundred different industries and quantified key hazards as "environmental impairment units" or “ELUs” (Soderstrom 1976, 762-777). The total number of ELUs designated for each industry was the sum of two separate calculations. The first was based on the likelihood of a specific industry releasing one or more of 18 different kinds of contaminants. The second was to determine the extent of damage which might be caused by the release of one or more of those pollutants. Then, the total number of ELUs for each industry was listed under key impact areas that could be polluted such as waterways, surrounding property and nearby populations. This gave insurers the claims potential of an individual industry, the contaminants that would likely discharge, and the locations that would likely be affected. The indices of hazards were then incorporated into a formula to derive preliminary premium estimates. For individual company premium estimates, elements such as volume of sales, proximity to population centers, type, volume and toxicity of hazardous waste produced, site characteristics, and past record of claims, violations and public complaints were included in the calculations. These initial premium quotes could then be used by insurance buyers to compare cost with anticipated benefits of the coverage sought before authorizing a required technical risk assessment survey. In the US, the International Research and Technology Corporation (IR&TC) was selected as the ERAS organization designated to formulate the

insurance industries national risk classification system and authorized to conduct client technical assessment surveys.

Table 5.1: ERAS Risk Classification System & Risk Assessment Process

ERAS Industry/Country Risk Factors*	ERAS Company Risk Factors*	ERAS Risk Assessment Survey Process**
Evaluation of 100+ Industries	Size of Insured's Business	**Detailed Application Form**
Likelihood of industry releasing up to 18	Extent of pollution already present in the	**Evalutation of chemical hazards/treatment**
Extent of possible damage (geography/population)	Type of hazardous waste operation	**Headquarters Meeting with Company Management**
National Political Risk	Type, volume and toxicity of hazardous waste produced	Company history of pollution problems
National Regulatory Enforcement Risk	The methods used for waste disposal	Review of Company Pollution Control Program
National Judicial Risk	Size and nearness of population in plant vicinity	Review of Procedures for Regulatory Compliance
Calculation of ELUs for Industry/Country	Land use patterns and wildlife population	Financials on past & future pollution control investment
Preliminary Premium Estimate	Site weather, soil, and grundwater characteristics	**Site Visit/Survey by Engineers/Health Physicists**
	Past record of claims, fines, and public complaints	Review plant operating procedures
	Degree of risk-awareness among comoany management	Collect data on emissions
	The present quality of housekeeping	Records on regulatory compliance
	Local standards for the industry in area concerned	**Contact/Interview Regulatory Officials**
	The effectiveness of local enforcement agencies	Is site complying with applicable regulations?
	The type of local statutory liability	Satisfisfaction with company's pollution control plans?
	The practice of the local courts	Are there any plans to change regulations or standards?
		Final Hazards/Risks Evaluation
		Library review of hazards/risks found during survey
		Preliminary Report
		Review by Company for for corrections
***Source: Soderstrom (1976)**		**Final Report**
****Source: Humpstone (1977)**		**Underwriting & Premium Quote**

The technical survey process (Humpstone 1977) was then as follows. Prior to initiating the technical survey, the client completed an intricate application form providing details on the company, past insurance coverage and claims, description of site and current operations, site history including past land use, past storage and disposal activities, environmental testing and permitting information, known hazardous waste

producing undertakings, and established regulatory violations. Based on the application data and library research IR&TC then evaluated the chemical hazards, and treatment processes, and identified potential pollution problems.

IR&TC next conducted a headquarters visit to gather details on the company's pollution history, and reviewed the firm's pollution control program, procedures for regulatory compliance, and plans for pollution control investment. IR&TC then conducted one or more site visits to review plant operating procedures, collect data on emissions, and examine regulatory compliance records. They also contacted and interviewed local, state, and federal regulators to confirm that the site was complying with applicable regulations, and to determine if any changes might impact the company's pollution control plans. IR&TC then provided a preliminary report to the client to review for errors and omissions, and then a final report to the underwriters to assess the risk for final premium determination purposes. The client paid IR&TC directly for the survey cost, but was given up to a 10% credit on the premium if coverage was accepted.

In 1974, the Howden-Snow Group became the managing agent for the program in the US, and sold the first EIL policy the following year. The EIL policy covered third-party liability and offsite cleanup costs resulting from gradual and unintended releases of contaminants from TSDFs and other industrial operations. In addition to covering gradual pollution events, EIL coverage differed from CGL coverage in other significant ways (see Table 5.2). First, EIL policies were issued on a "claims-made" basis while CGL policies were issued on an occurrence basis. Under a claims-made policy, the insurer provides coverage only if the claim is first made during the policy period – typically one

year. This differed from an occurrence policy which provides coverage for bodily injury and property damage that occurs during the policy period even if a claim is filed years later. Another difference was that EIL policies are generally underwritten and issued on a site-specific basis while CGL policies usually cover general liability across all of the insured's properties. Some EIL policies covered multiple sites; however each site was subject to a separate environmental assessment survey before coverage was extended.

Table 5.2: CGL vs. EIL Coverage – Impact on Safety

Feature	CGL	EIL	Safety Improvement
Term	Mutiple Years	One Year	Annual assessments for renewal
Claims Basis	Occurrence-Based	Claims Made- Based	Claims must be made during premium year (Immediate/Short Term Notification of Event)
Scope	Comprehensive - All properties	Site Specific	Site specific technical surveys and assessments
Coverage	Third Party Liability (Sudden and Accidental Pollution Event)	Third-Party Liability (Gradual & Unintended Pollution Events)	Focus on gradual pollution event prevention and safety
Exclusions	Gradual Pollution Events & Owned-Property (Onsite Cleanup)	Sudden & Accidental Pollution Events	Some EIL Policies provide coveragge for onsite cleanup based on insured's risk profile and practices
Deductibles/Co-Pays	All-Risks (not pollution specific)	Gradual Pollution Specific	Client has stake in preventing gradual pollution events
Preferred Pollution Premiums	Not available	New sites using latest technologies	Encourages development of new sites and adoption of new technology and best practices

The Howden-Snow EIL policy contained limits on payments of $4 million for any one claim and on $8 million total claims during a given period of coverage, usually one year. The policy also contained absolute exclusions including nuclear contamination, known preexisting conditions, deliberate noncompliance with environmental laws, fines, penalties, punitive damages, and areas covered by other policies (IR&TC 1979, 33). Because of such exclusions and its high underwriting and premium costs, EIL did not initially appeal to potential clients. However, following the passage of RCRA , demand for EIL in the US increased significantly.

By September 1980, four other carriers including American International Group (AIG) offered EIL policies with limits up to $50 million per year. Higher coverage levels and lower premiums were given to new operators and facilities that used the latest in pollution control technology. Contrastingly, firms with older facilities were subjected to high premiums, or even denied necessary coverage. Of particular concern to the EPA were sites that had been abandoned. This issue came to a head in August 1978 with the announcement of a public health emergency at an abandoned chemical waste landfill site in Niagara Falls, NY.

V. Love Canal (1978)

The Love Canal environmental disaster was a "creeping" economic and social catastrophe that evolved over a period of more than a hundred years. During that period a project site originally envisioned as the center of a "Model City" became a dumping ground for tons of hazardous waste. Despite warnings, schools and homes were built in the area surrounding the landfill. Over a long period of time, the site's population, including children and pregnant women, were exposed to high levels of nearly 300 different toxic chemicals. Exposed people experienced a variety of negative health effects. Hundreds of families were forced to evacuate the area and compelled to sell their homes to the state. Many studies were conducted by numerous state and federal agencies, oftentimes producing troubling and conflicting results.

Soon after its discovery, thousands of additional "Love Canals" were discovered across the US, and litigation with settlements in the billions of dollars transpired. In the middle,

were insurers who mostly though "occurrence-based" CGL policies were exposed to huge catastrophic claims.

A. Historical Background

In 1892, entrepreneur William Love proposed a plan to build "Model City," a community of parks and residences on the banks of Lake Ontario. At the heart of Model City was a navigable power canal connecting the upper and lower levels of the Niagara River and producing electricity for factories to be built along its banks. At the time, electricity could not be economically transmitted over long distances, making it necessary for industry to be located close to generation sources. Canal construction began in 1894, but was soon halted with the development of alternating current allowing the economic transmission of electricity over long distances. When the project was abandoned, only a mile had been dug, 50 feet wide and 10 to 40 feet deep.

Beginning in the 1920s, the abandoned canal became a popular disposal site by the City of Niagara Falls, the US Army, as well as for many of the chemical companies located in the area (Zuesse 1981). In 1942, the Hooker Chemicals and Plastics Corporation (later a subsidiary of Occidental Petroleum) obtained permission from Niagara Power and Development (then owner of the canal) to dispose of byproducts from the manufacturing of dyes, perfumes, and solvents. The abandoned canal site was ideal for disposal of Hooker's chemical waste because it was close to their production facilities and lined with clay – specifically built to retain water and other fluids. Eventually, in 1947, Hooker bought a 3000-foot section of the canal and 70 foot-wide banks on either side and converted it into a 16-acre landfill. Between 1942 and 1953 Hooker, under

license from the City of Niagara Falls (Simon 1994, 435) deposited nearly forty-four million pounds of hazardous waste from its nearby plant. Independent engineering analysis of the Love Canal landfill in 1979 indicated that the site was a "state-of-the-art" facility at the time it was used, and that Hooker's disposal techniques all followed the standard industry practices of the period (*U.S. v. Hooker Chemical Corporation* 1988).

In 1952, the Niagara Falls School Board approached Hooker about purchasing the Love Canal property for the purpose of constructing a new school. Hooker specifically told them that they did not want to sell the property and that the landfill was not a suitable site for a school. Under threat of eminent domain seizure, Hooker in 1953 agreed to sell the landfill for $1.00 with the deed stating that the property had been used for the disposal of hazardous waste and relieving Hooker of all future risks and liabilities. As part of the transfer, Hooker provided the Board with a map showing the location of buried chemicals and stipulated that the information on the site's use be conveyed to any future property owners (Deed 1953). Despite Hooker's warnings, the Board proceeded with the construction of the 99th Street School on the central portion of the acquired land. While excavating the site, the contractor breached the landfill exposing 55-gallon drums and allowing toxic chemicals to seep out. The Board was alerted and the decision was made to move the school about 80 feet north. Upon completion in 1955, about 400 children attended the school. Later that year, another school a few blocks away was also completed.

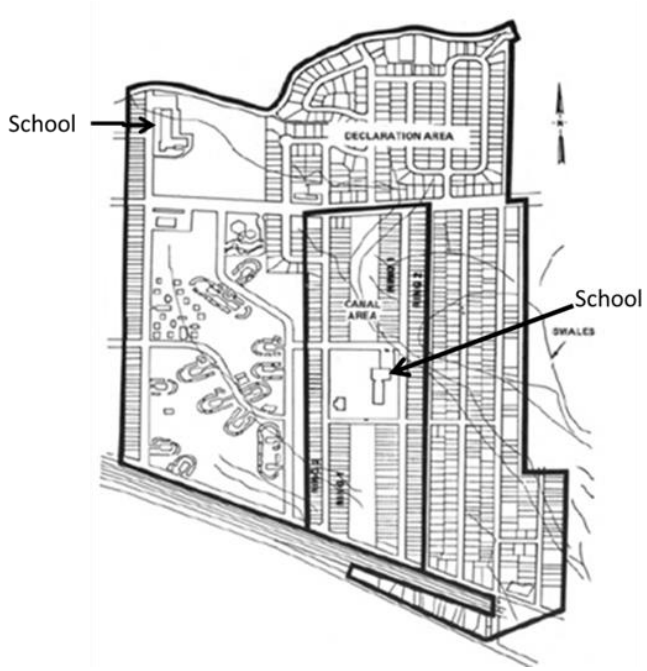


Figure 5.1: Map of Love Canal Evacuation Zones Showing Landfill, Schools & Homes (EPA 1982A)

The new schools attracted real estate investors interested in building houses. Against the advice of Hooker (Ives 1999, 44), the School Board sold the remaining land to private developers who eventually built around 800 houses and 240 apartments in the area. Around 100 homes had their backyards adjacent to the former canal (EPA 1982A). By the mid-1960s, physical evidence of the landfill disappeared and the restrictive covenants included by Hooker in the original deed dissolved. Thus the residents were unaware that their community was a toxic time bomb.

B. Love Canal Disaster & Emergency Declarations

It was not until 1976 that the problem literally came to the surface. Unusually heavy precipitation during the previous winter raised the groundwater level, and oozing chemicals leached upwards to ground level. Homes began to reek of chemicals, ponded

surface water contaminated with chemicals was found in backyards, vegetation died, and ultimately a portion of the landfill subsided exposing drums of hazardous waste (EPA1982A). Residents complained to the city but health officials were slow to respond. Eventually, the local newspaper, the *Niagara Falls Gazette*, published a series of articles in late-1976 outlining the complaints and, also, test results of samples taken around the landfill showing high levels of toxic organic chemicals (SUNY 2020). The publicity helped to spur the city and the State Departments of Health (DOH) to conduct intensive air, soil, and groundwater sampling and analyses. Based on the results, State Health Commissioner Robert Whalen in April 1978 declared the Love Canal area to be "an extremely serious threat to health and welfare." He ordered that the area nearest the landfill be fenced and that the Niagara County Health Commission and DOH initiate a house-to-house health survey and collected air samples in houses directly abutting the canal.

Armed with new epidemiology information Commissioner Whalen on August 2, 1978 declared a state of emergency, closed the 99th Street School, and recommended evacuation of pregnant women and children under two years of age living in an area two streets wide and three blocks long surrounding the canal (Rings 1 & 2). Subsequently, on August 7, President Jimmy Carter announced a federal health emergency, enabling the use of federal funds and ordering the Federal Disaster Assistance Agency to help the City of Niagara Falls in remediation efforts. During the first week of the emergency, New York Governor Hugh Carey ordered the evacuation of 236 families from Rings 1 and 2, and authorized the purchase of all Ring 1 houses. Over the course of the next 20 months,

additional evacuations would be ordered and the second school would be closed. This culminated on May 21, 1980 when President Carter declared a second state of emergency leading to the relocation of an additional 800 families who lived within a mile long and half a mile wide emergency declaration area or "EDA" (Figure 5.1). It also authorized the purchase of an additional 564 homes at a cost of nearly $30 million (Ives 1999. 46).

C. Love Canal Contamination & Health Studies

The results of chemical migration and health studies conducted by the EPA, state and local investigators over the next few years were confusing, alarming and controversial. The initial DOH study ordered by Commissioner Whalen and released in September 1978 identified 82 different chemical compounds at the landfill, of which one was a known human carcinogen and 11 were presumed animal carcinogens. However, there was no conclusive evidence that Love Canal residents were experiencing higher rates of cancer, though results did show a slight excess frequency of miscarriages in women living in homes immediately adjacent to the landfill. Further, the study showed no increased health risk for people living in homes outside Rings 1 and 2 (NYSDH 1978). Subsequently, a follow up independent study released in January 1979 did reveal a higher than expected rate of birth defects and miscarriages among families that lived outside of the rings, specifically along migration paths for contaminated water (Paignen 1979).

As part of the second emergency declaration, Carter also ordered the EPA to conduct a comprehensive monitoring study of Love Canal. This monitoring program involved the collection and analysis of approximately 6,000 field samples, making the Love Canal study the most comprehensive monitoring effort ever conducted by EPA at a hazardous

site (EPA 1982A). The study's purpose was to determine the extent of chemical contamination of the evacuated area, and assess the relative human living quality or "habitability" of the EDA (EPA 1982A).

The results of the EPA monitoring study at Love Canal were released to the public on July14, 1982. The conclusions were surprising and highly controversial. The environmental monitoring study did not produce any evidence that Love Canal contributed to contamination in the area encompassed by the second emergency declaration order with the exception of certain storm sewer lines and creek sediment areas. Further, the study produced no evidence that, outside of Ring 1, swales served as preferential chemical transport routes (U.S. House 1982). These results were reviewed by the Department of Health & Human Services (DHHS) which concluded that the Love Canal EDA, outside Rings 1 and 2, was habitable (US DHHS 1982).

However, these conclusions were contested by the National Bureau of Standards (NBS), and the Environmental Defense Fund (EDF). The NBS challenged the quality control and assurance of the EPA study and the validity of the results (Kammer 1982). The EDF contended that the EPA study did not include an assessment of the actual and potential health hazards needed to determine absolute habitability or safety (US DHHS 1982, 69). Ultimately, the Office of Technology Assessment (OTA) was asked to examine the validity of, the habitability decision. Their 1983 findings were that there was insufficient information in the EPA study to: 1) conclude either that unsafe levels of toxic contamination exist or that they do not exist in the EDA or, 2) support DHHS's conclusion that the EDA was habitable. Thus, five years after the 1978 emergency

declaration, there remained a great deal of uncertainty about the extent of contamination and magnitude of health effects

D. Love Canal Litigation

Under this cloud of uncertainty, the first lawsuit was filed on September 26, 1979 against Hooker Chemical, the City of Niagara Falls, the Niagara Falls Board of Education and the County of Niagara. By October 31, 1979 over 800 individual lawsuits and 6 class action lawsuits were filed with claims totaling over $11 billion (Collin 2006). By April 1981, the claims in these lawsuits had grown to between $12 and $14 billion in damages (NYSDH 1981).

In addition to these personal lawsuits, the DOJ and state filed civil lawsuits against Hooker Chemical and its parent company Occidental Petroleum Corporation (OPC). On December 20, 1979, the DOJ on behalf of the EPA filed a $124.5 million civil suit against these parties for environmental damage caused by improper hazardous waste disposal, site cleanup, and the cost of the federal emergency response (*U.S. v. Hooker Chemical* 1979). The federal lawsuit cited violations of the RCRA and the Refuse Act of 1899 (NYSDH 1981). A few months later on April 28, 1980, the State of New York filed a $635 million civil suit against OCP and Hooker seeking to recover nearly $100 million spent by the state in taking emergency action, as well as over $500 million in penalties and punitive damages for harming the state's resources (*State of New York v. Occidental Petroleum* Corporation 1980).

Hooker never denied that it disposed of hazardous waste at Love Canal. However, in its defense, they claimed that they were being unfairly singled out since others, including

the City of Niagara Falls, had also used the site for hazardous waste disposal. They had followed the waste disposal practices that were then almost universal throughout the chemical industry, and were considered an industry leader in safety. Further, they had warned the School Board about the hazard, and tried to prevent both public and private development of the site (Beauchamp 2013).

The litigation dragged out for decades. Despite their defense, Hooker and OCP over time began to settle various cases. On December 20, 1983, the New York Supreme Court approved a $20 million settlement agreement between OCP and 1328 Love Canal families (Urban et al. v. Occidental Chemical Corp. 1983). The average settlement was $14,250 (Dabkowski 2018). Over ten years later in June 1994, OCP settled with New York State, agreeing to pay $98 million for damages and state cleanup expenditures. OCP also agreed to take over maintenance of the site (Wald 1994). A year later, OCP settled the December 1979 lawsuit with the DOJ, agreeing to pay $129 million dollars to reimburse the federal government for Love Canal clean-up costs (USDOJ 1995). Finally, in March 1998 the last of the remaining individual lawsuits were settled, with 900 families receiving cash settlements that range from as high as $100,000 to as little as $83 (Brokaw 1998). In 1988, before these settlements, the New York State Department of Health determined that half of the homes in the evacuated Love Canal area were fit for habitation, with the remaining area deemed fit for industrial use. Beginning in August 1990, 236 formerly boarded up homes renovated by the Love Canal Area Revitalization Agency were put up for sale, at 20 percent below market value, and were quickly bought up. Today, the area formerly known as Love Canal is the revitalized community known

as Black Creek Village (Ives 1999, 47). In 2004, the EPA announced the completion of the federal cleanup of Love Canal, at a total estimated cost of $400 million (Depalma 2004).

E. Love Canal and Insurance

During the 12-year period that Hooker actively disposed of hazardous waste in the Love Canal landfill (1942-1953), they purchased CGL policies from nearly 50 insurance companies, many of them underwritten by Lloyds of London (Herbeck 1996). Further, during the years when residents were primarily exposed to the leaching chemicals (1963-1979), Hooker's parent company OPC had $320 million in CGL coverage (Vuono and Hobbs 1997, 86). In addition, other parties to Love Canal lawsuits also had millions of dollars in CGL coverage.

The response of insurers to client requests for lawsuit defense and claims settlement assistance was decidedly mixed. Because of the "long-tail" of environmental damage and injury spread out over decades of time, it was difficult to determine when the terms of the CGL policies were triggered, which parties were liable, and how to apportion the costs. In addition, insurers, in some cases, invoked the 1973 pollution exclusion to limit their exposure. For example, one of the defendants, Niagara County, was initially denied defense assistance by its insurer, citing pollution exclusion clause. A subsequent court decision ruled that the pollution exclusion did not apply because while the County technically owned the landfill, unlike other named defendants, it was not an "active polluter" responsible for the actual damage (Niagara County v. Utica Mutual Insurance 1980). Subsequently, when settlement was reached with the majority of Love Canal

families in 1983 for $20 million, the defendants collectively paid $6 million in deductibles, and the insurers paid the rest (Gruson 1985, Mazur 1998).

Where the insurers universally denied coverage was in regard to the state and federal lawsuits seeking reimbursement for over $500 million in cleanup costs. Citing the "owned-property" exclusion in the CGL policies, insurers maintained that they were not responsible for damages caused to the Love Canal landfill site. Complicating matters, it was soon found that Hooker had disposed of significant quantities of hazardous chemicals at several other sites in Niagara County including at Bloody Run found to contain four times as much toxic waste as at Love Canal (Tyson 1980, 107). Ultimately, thousands of abandoned toxic waste sites would be discovered around the US, leading to the enactment of the "Superfund Act" by Congress in 1980.

VI. Post-Love Canal Regulation, Litigation & Insurance

This section examines the evolution of environmental regulation, litigation and insurance in the 1980s following the discovery of the Love Canal disaster. It includes RCRA financial protection going into force, the passage of the Superfund Act, the rise of mass toxic torts, the near collapse of the environmental insurance market, and its ultimate recovery in part through the adoption of more stringent underwriting practices.

A. Superfund Historical Background

In December 1978, several drums were discovered floating in a creek near Louisville, Kentucky. When environmental officials traced the drums 25-miles upstream, they discovered 17,000 drums filled with unlabeled wastes disposed across a 23-acre abandoned site in what became known as the "Valley of the Drums." Six thousand of the

drums exposed to the elements were oozing toxic chemicals onto the ground (Reisch 1983, 684). This discovery "visualized" the hazardous waste problem and, coupled with the publicity surrounding Love Canal, drove public opinion to demand federal action to identify and clean up abandoned hazardous waste sites.

During 1979, Congress conducted a series of hearings to investigate the hazardous waste problem and to determine what should be done about the cleanup of abandoned sites. During these hearings, the EPA estimated that over 77 billion pounds per year of hazardous waste was being generated in the US, and that only 10% was disposed of in an environmentally sound manner (US House 1979). Further, EPA had identified as many as 2,000 abandoned sites estimated to cost up to $22.1 billion to completely clean up.

On June 14, 1979, President Carter proposed legislation to Congress to create a multi-billion dollar "super" fund, comprised of federal money and fees collected from hazardous waste producers, to help clean up abandoned toxic waste dump sites. After lengthy debate mainly focused on the size of the fund and the chemical industry's legal and financial responsibilities, the lame-duck Democratic Congress enacted the *Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA)* (P.L.95-510), signed into law by President Carter on December 11, 1980, only weeks before Republicans took control of the Senate and Presidency.

B. RCRA and CERCLA (Superfund Act)

By 1981, two laws existed regulating the liability and safety at US hazardous waste disposal sites: 1) RCRA that primarily regulated hazardous waste activities at existing disposal sites, and 2) CERCLA, commonly referred to as the "Superfund Act," that

primarily addressed cleanup at inactive or abandoned waste sites. Under RCRA the EPA was required to establish minimum national standards governing management of hazardous waste, and a permit program for TSDFs. It also required that owners of TSDFs demonstrate financial responsibility for third-party liabilities resulting from their operations, for facility closure, and for post-closure care. However, in 1981, the EPA still had not established minimum national standards or financial requirements for permitting, nor did they have a clear understanding of the location of closed or abandoned facilities, or the costs and risks associated with post-closure maintenance and cleanup.

CERCLA focused on the latter issue, requiring the EPA to conduct an inventory of hazardous waste sites and authorizing the use of Superfund to take immediate action to clean up hazardous conditions. CERCLA required that the EPA initially identify 400 sites and develop a method for their prioritization. The first interim list of 115 priority sites was released on October 24, 1981. The list included 29 sites around the country more dangerous than Love Canal (Omang 1981). In 1982, EPA formally published the first National Priorities List (NPL) of 400 targets that were eligible for Superfund reimbursement cleanup. Sites were placed on the NPL primarily on the basis on their score under EPA's Hazard Ranking System (HRS). The HRS evaluated the relative threat a site posed to human health or the environment via five pathways; groundwater, surface water, air, direct contact, and fire. HRS scores ranged from 0 to 100, with sites scoring 28.5 or higher being eligible for the NPL (EPA Factbook 1993). By the end of the decade, EPA had 1300 sites listed on the NPL with an average cleanup cost of about $30 million per site.

To initially pay for NPL site cleanups, Congress created the $1.6 billion Hazardous Substance Response Trust Fund (Superfund) financed by taxes on the petroleum and chemical manufacturing industries collected over four years. States had to contribute at least 10 percent of the actual long-term costs of cleanup, unless the site was publicly owned, in which case the state was required to pay at least 50 percent of the costs (EPA 1981). However, if it was a privately owned site, both the federal government and the states could seek reimbursement from Potentially Responsible Parties (PRPs); or require PRPs to undertake the cleanup themselves. Under CERCLA Section 107, a party is a PRP if it (1) currently owns and/or operates a hazardous waste facility; (2) previously owned and/or operated a hazardous waste facility; (3) arranged for disposal of hazardous substances at the facility; or (4) transported hazardous substances to the facility. Thus liability under CERCLA was retroactive, related to both past and present owners/operators of a property. Under CERCLA Section 302, liability was also "strict" meaning that negligence by PRPs did not need to be proven by the EPA or other plaintiffs. Thus, under CERCLA, a PRP could be held strictly liable for cleanup costs as a past or present owner, operator or waste transporter even if it followed then-current regulations, employed state-of-the-art technology and modern practices, or did not cause or contribute to the pollution at all.

Further, CERCLA permitted but did not specifically require the imposition of "joint and several" liability. Because waste at a disposal site was often comingled, courts attempted to apportion liability among the various PRPs. However, in many cases, apportionment of responsibility could not be determined, in which case each PRP could

be held liable for the entire harm. This created huge settlements that were far in excess to the actual cleanup costs. Likewise, if only one PRP was identified, it could be held liable for the entire cost of cleanup even though it may have contributed only a small percentage of hazardous waste or none at all. This was particularly devastating to small operators who oftentimes were forced into bankruptcy.

Faced with this enormous financial burden, many PRPs turned to their insurers requesting coverage to pay for legal defense and cleanup costs under their CGL policies. Because the pollution damage was 'long-tail" occurring over an extended period of time, PRPs often claimed coverage under multiple insurance policies issued over the period of many years. Many times insurers refused coverage citing the pollution and owned-property exclusions, and PRPs responded with coverage suits. The resulting litigation was typically complex, involving scores of policies covering decades of time. The suits often dragged on for years, were very expensive, and delayed the cleanup of many NPL sites. Insurers felt ensnared in a web of litigation and potential liability that limited their ability to underwrite environmental insurance and threatened their financial viability. As a result, many considered withdrawing from the market.

C. Mass Toxic Torts and Judge-Made Insurance

Love Canal and subsequent passage of the Superfund Act with its retroactive and strict liability provisions unleashed an unprecedented barrage of litigation that included federal and state cleanup enforcement actions against PRPs, PRP contested coverage suits against insurers, and a range of "toxic tort" class action and personal lawsuits for damage to adjacent property and injury to nearby populations. Complicating the litigation

landscape was the involvement of state and local environmental laws and regulations, the variance between state and federal court decisions, and the inherent conflict of interest that states had in regulating the insurance industry.

Insurance companies continued to try to limit their exposure by using exclusion clauses in CGL policies and by arguing that CERCLA cleanup costs did not constitute "damages" under the policy coverage clause. Increasingly in early-1980s cases, these arguments were rejected by the courts. They found the exclusion clauses to be ambiguous and ruled in favor of the insured. Insurance companies were also seen as the “deep pockets” that could afford huge settlements.

Between 1982 and 1984, a series of judicial decisions reinterpreted insurance policy language, undermining insurer arguments in favor of the insured. First, in *Jackson Township Municipal Utilities Authority v. Hartford Accident and Indemnity Company* (1982) a New Jersey court ruled that under the CGL policy the insurer had a duty to defend an active polluter, the municipality, whose landfill had seeped and contaminated 97 nearby wells. The court ruled that the pollution exclusion did not apply because the seepage was neither expected or intended, and awarded Jackson Township $16 million. Second, in *United States Aviex Co. v. Travelers Insurance Co*. (1983), the Michigan Court of Appeals became the first court to hold that coverage for "damages" under Aviex’s CGL policy encompassed the cost of state-ordered environmental cleanup. Finally, in *Riehl v. Travelers Insurance Company* (1984) the judge rejected the Owned Property Exclusion, ruling that the insurer was responsible for the cleanup of the insured’s property. As part of this decision, the court ruled that the pollution had

contaminated the property's ground and surface water that legally was owned by the state.

In addition to these legal setbacks, insurers were increasingly involved in environmental bodily injury and property damage (BI/PD) litigation claims. These BI/PI claims were generated not only from third-parties living in close proximity to hazardous waste facilities, but also from people exposed to a variety of environmental hazards such as asbestos and dioxin in their homes, communities and workplaces. For example, in 1983, the EPA ordered the evacuation of 2,239 residents of the City of Times Beach, Missouri, at a cost of $30 million. The town had been contaminated through the spraying roads for dust control in the 1970s with dioxin-contaminated oil. In addition to the buy-out, the cost to clean up the town and incinerate the soil was approximately $170 million (EPA 1988). Likewise, a class action settlement in 1985 netted 800 asbestos workers in East Texas $137 million (Jenkins v. Raymark Industries 1985). Following these decisions, the number of asbestos-related claims increased drastically, reaching 340,000 in 1989 (American Bar Association 1989) – a huge mass tort whose litigation was tying up the state and federal courts (US House 1992). From 1982 through 1990, more than 20 asbestos manufacturers including Johns-Manville filed for bankruptcy, with many forming trust funds partially capitalized using insurance compensation, to pay billions of dollars of asbestos claims.

All told, estimates by RAND indicated that by the end of 1989 insurers had paid out $470 million in CGL claims for inactive hazardous waste sites (Acton, and Dixon 1992, x), and over $2.6 billion for asbestos-related claims (Carroll et al. 2005, 92-93).

However, this was only the tip of the iceberg. Only a small fraction of toxic torts had been settled in the 1980s, with the Office of Technology Assessment estimating hazardous waste and asbestos cleanup costs ranging from $500 to $700 billion, with an insurance industry exposure between 15 and 40 percent (OTA 1989) This far exceeded US industry reserves, threatening the solvency of many of the largest carriers. Given this evolving financial mess, the industry had to act. It did so by implementing an "absolute" pollution exclusion, and by most carriers exiting the pollution insurance market.

D. Absolute Pollution Exclusion & the Collapse of the Pollution Insurance Market

Following the passage of CERCLA in December 1980 and the October 15, 1982 effective date for TSDFs to have proof of financial responsibility under RCRA (EPA 1982B), insurers initially believed they had an extraordinary market opportunity to sell pollution liability insurance (PLI). With the goal of increasing capacity, ISO in 1981 developed a claims-made pollution liability policy, broader than EIL, covering both sudden and gradual accidents, as well as defense costs and "reasonable and necessary" clean-up costs. By 1984, over 50 insurers in both the US and London markets offered EIL and ISO pollution insurance with coverage levels of $5 to $10 million annual per site and $10 to $20 million annual aggregate per company – well in excess of RCRA requirements. Between 1982 and 1984, approximately two thirds of TSDFs used insurance to fulfill RCRA financial responsibility requirements (GAO 1988, 4). This included CGL policies to cover "sudden and unintentional" pollution events, EIL to cover gradual pollution incidents, and ISO policies to cover both sudden and gradual pollution claims.

However, by 1984, insurers were finding these policies to be far from perfect. The flaws in CGL policies were increasingly becoming apparent. Despite the 1973 pollution exclusion clause and the insurer's contention that policies only covered sudden "instantaneous" events, the courts were interpreting sudden to mean "unexpected" from the insured's point of view, and requiring insurers to provide coverage. Despite the fact that EIL and ISO pollution coverage required that prospective clients undergo a rigorous risk assessment, insures still experienced significant and unexpected losses. For example, in 1983, insures collected $35 million for EIL and ISO premiums, but paid out approximately $90 million in claims (Journal of American Insurance 1986). The reasons for these losses relate to: 1) CERCLA's strict and retroactive liability that made insurers pay for damages that may not have been caused by the insured party, 2) state and federal mandated cleanup costs that exceeded what insurers thought was "reasonable and necessary," and 3) the realization that even when operators followed the strictest safety standards, some leakage at virtually all hazardous waste sites was bound to occur. Thus, insurers had drastically underestimated the judicial, regulatory, and technical risks associated with the operation of hazardous waste disposal sites.

In order to rectify this situation, insurers took several actions. First, ISO in October 1984 introduced the "absolute" pollution exclusion (APE) to the standard CGL policy. The APE was an extraordinarily broad exclusion that eliminated CGL pollution coverage for bodily injury and property damage for both sudden/accidental and gradual events, including any government mandated cleanup costs. Second, EIL and ISO pollution policy insurers dramatically increased premiums and decreased coverage levels. Between 1984

and 1986, premiums for pollution insurance increased six-fold and total US coverage dropped from$7.4 billion to $2.6 billion (GAO 1988, 15). In addition, insurers began to withdraw en masse from the pollution liability insurance market. The exodus began in 1984 when a leading London reinsurance pool ceased accepting pollution liability reinsurance and other reinsurers followed. As a result, primary insurers began to withdraw from the US market. By 1987, the GAO reported that only one insurer, AIG was actively marketing pollution insurance policies (GAO 1988, 20).

Thus during the second half of the 1980s, the market for pollution insurance had virtually collapsed. All pollution coverage had been eliminated from CGL policies and the little EIL coverage still available was prohibitively expensive and very limited in scope. In 1984, Congress amended the RCRA requiring all hazardous waste facilities to comply with the financial responsibility requirements by November 8, 1985 or close down their businesses.

Thus, the collapse of the market could not have come at a worse time. According to the EPA, only 492 of 1,600 facilities were able to meet the deadline (US House 1985, 332). Some facilities were able to satisfy the financial requirements through self-insurance. Others formed risk pools, risk retention groups, or Protection & Indemnity (P&I) clubs with owners and operators in similar lines of business.

Roughly a third of facilities that were in business in 1982 ceased operations by 1987, with the inability to obtain insurance being the primary factor. The burden of insurance unavailability fell disproportionately on smaller operators. Safety was affected because contractors hired to cleanup dangerous Superfund sites could not secure insurance. The

absence of insurance also disrupted business across many US sectors. Any company that used chemicals (e.g. dry cleaners) or disposed of hazardous waste materials (e.g. hospitals) had to be concerned about environmental liability. Land transfers were hindered because potential buyers were concerned about inheriting toxic skeletons in the closet.

Given the enormous backlog of open claims, many insurance companies were concerned about their solvency. In the early 1990s, several prominent insurers including Lloyd's of London, Zurich Insurance and CIGNA went through bankruptcy reorganizations in large part to relieve the financial pressures caused by environmental and asbestos liabilities. Consequently, what the insurance industry lobbied vigorously for were state and federal tort reform to limit the amount of damage awards; and a loosening of CERCLA's joint, strict and retrospective liability provisions that obliged them to pay claims for environmental damage (including cleanup) that their policies did not cover and for which they collected no premiums.

E. Reemergence of the Pollution Insurance Market

During the period 1987 to 2000, the market for pollution insurance gradually recovered. This recovery was facilitated by new court interpretations of CGL policy language, state tort reforms, changes in TSDF pollution business philosophy, insurer adoption of more comprehensive risk assessment and underwriting practices, development of new insurance products, and ongoing RCRA requirements that all TSDFs have proof of financial protection.

Since Superfund's inception in 1980, and its reauthorization in 1986, the perception was that these programs were inefficient and that there was extremely slow progress in getting NPL sites cleaned up. By 1989, the number of hazardous waste sites identified had grown to over 30,000 with an additional 800 sites added to the NPL while only 26 were removed. While Superfund reauthorization in 1986 increased the cleanup trust fund to $8.5 billion, this amount was insufficient to remediate the vast majority of NPL sites. As specified in CERCLA, EPA expected PRPs and their insurers to pay for cleanup costs. However, extensive litigation and PRP bankruptcies slowed the collection of reparations. In fact, most of the money spent by PRPs and insurers during the 1980s was on legal fees rather than cleaning up sites. Further, the lack of insurance was preventing engineers and contractors from engaging in remediation projects. Thus, liability and the absence of pollution insurance were directly impacting environmental safety.

The states were the first to act in trying to resolve the liability and insurance crises. While CERCLA was a federal law that mandated joint and several liabilities, most environmental lawsuits were adjudicated in state courts under state common law. Beginning in 1986, many states began to reform their tort laws, limiting joint and several liability and putting caps on punitive damage awards. Studies conducted in the 1990s showed that these reforms significantly decreased the number of lawsuits and the size of awards. This led to decreases in liability insurance premiums and reestablished profitability in the US insurance market (CBO 2004).

A second factor that bolstered the environmental insurance market was a series of judicial decisions that recognized the intended meaning of CGL and EIL policy language.

Beginning in 1984, some courts had already begun to interpret the pollution exclusion in CGL policies to bar coverage for "sudden and accidental" pollution unless the occurrence was instantaneous (*Techalloy Company v. Reliance Insurance* 1984). This interpretation was solidified in 1986 in *Waste Management of Carolinas v. Peerless Insurance Co.* when the North Carolina Supreme Court ruled that the pollution exclusion clause exempted insurance coverage for damages caused by landfill seepages, thus rejecting the court's decision in the Jackson Township case. Likewise, in one of the few cases involving EIL insurance, a California court in 1990 interpreted the language in the policy in favor of the insurance company limiting coverage to the specific policy terms and conditions (*Masonite Corp.. v. Great American Insurance Company* 1990).

As the environmental liability and judicial risks became more manageable, insurers and reinsurers reentered the market. Throughout the 1980s, AIG continually wrote pollution insurance, issuing approximately 400 EIL policies in 1986. The majority of these policies, with coverage limits up to $12.5 million per year, were written for TSDFs subject to RCRA regulations (GAO 1987, 20-21). AIG attributed their EIL success to their history of adhering to very careful underwriting standards, including requiring detailed risk assessments for each facility considered for coverage. They believed that their EIL competitors, during the early-1980s pollution insurance "gold rush" failed because they were less careful with their pollution underwriting, and placed insufficient emphasis on the actual risks (GAO 1987). By 1995, 14 companies were selling environmental insurance products, with three companies - AIG, ECS, and Zurich - accounting for 75% of the $800 million market (Vuono and Hobbs 1997, 94-95).

During the insurance void of the mid-1980s, only about a third of hazardous waste facilities could secure insurance to meet RCRA requirements. In lieu of insurance, many firms established “captives” - a form of self-insurance funded through tax-deductible reserves. Under captive scenarios, these firms were internalizing all of the environmental risk, motivating them to adopt safety measures to try and minimize losses. When the insurance market recovered, firms were able to use this knowledge to secure coverage with premiums and terms at a preferred rate. These companies also learned that environmental responsibility was good business practice, differentiating environmentally safe firms from competitors who were perceived to be polluters.

New environmental business opportunities also created demand for insurance. First, there were the contractors and engineers hired to clean up abandoned hazardous waste sites. During the late-1990s, there was increased interest by the federal and state governments, as well as the business community, in the redevelopment of contaminated properties or "brownfields" to allow these sites to be reused for industrial or other revenue-generating purposes. Governments offered financial incentives to motivate revitalization. To protect themselves against future environmental liabilities, developers, banks that invested in revitalization activities, and the buyers and sellers of brownfield properties all needed financial protection. Since developers planned to repurpose many of these sites for industrial activities, this activity sparked debate on “how clean was clean enough” and an understanding that environmental safety, in part, depended on how the property was going to be used in the future. Realizing that not all property had to be returned to its original pristine condition, some states scaled back their clean up

requirements. This helped cap cleanup costs, allowing insurers to reestablish coverage for remediation activity.

What emerged was the segmentation of the environmental insurance market into highly specialized niche areas. By the year 2000, over 35 insurers offered highly specialized environmental risk coverage targeted at specific properties, operations, hazards and professional services. Thus, there were specialty environmental insurance products for asbestos cleanup contractors, bankers and borrowers for brownfield remediation, and indemnification of gas station owners for underground storage tank leakages. These specialty insurers in turn developed expert knowledge on the specific risks they were insuring, oftentimes spending more on underwriting, risk assessments, inspections and accident prevention than they paid out in claims. This strong emphasis on prevention kept their loss expenses low. Thus, one key metric on how insurance promotes safety is when expense ratios exceed loss ratios (Anderson 1998, 15).

VII. How Insurance Promotes Safety & Risk Management at Hazardous Waste Sites

This section describes how insurance helps promote safety and environmental risk management at hazardous waste sites. Recognizing that there are many public policy mechanisms that influence firm environmental safety behavior including regulation and litigation, this section analyzes how insurance and other private-sector policy instruments complement and substitute for government policy measures. The section examine environmental underwriting and risk assessment processes and how specialty insurance policy capabilities can enhance information gathering, site monitoring, and loss control

for hazardous waste operations in different industries throughout the production, transport, treatment, and disposal lifecycle.

A. Instruments of Environmental Safety Policy

Today, there are both public (government-oriented) and private (marketplace-oriented) policy instruments for managing environmental safety. The most common public instruments include federal, state, and local environmental regulations; as well as court ordered safety actions. The primary private instrument is specialty environmental insurance, though there are other marketplace tools including captives, risk retention groups, mutual pools, tradable permits, and environmental risk internalization though capital markets (ERICAM) (Anderson Kill 2019).

The primary goal of all of these instruments is to internalize the cost of a firm's environment-damaging activities by making the "polluter pay" for harm to people, property, and natural resources. This can be done "ex ante" by imposing some form of Pigouvian tax - a tax assessed against private businesses for engaging in activities that create adverse side effects for society. An example in the environmental realm would be an effluent charge that assesses the environmental damage caused by a polluter's activities. Alternatively, firms could also be offered tax incentives such as discounts or rebates, to invest in pollution abatement technology.

Internalization can also be accomplished "ex post" by imposing penalties on polluters through regulatory fines or court liability rulings. Ideally, such internalization is accomplished both equitably and efficiently – assuring that any environmental harm is remediated expeditiously, that victims are fairly and quickly compensated, and risks are

managed efficiently so that costs of risk reduction do not exceed the expected benefits of the industrial activity.

The successful ex ante and ex post management of environmental risk behavior requires three key things. First, it requires accurate information for assessing the risk, encouraging loss prevention, licensing conduct, verifying outcomes, and determining remedies. Second, there needs to be well-specified and accepted standards of behavior that make risks measurable. Third, there need to be incentives for investing in safety measures and penalties to punish environmentally unsafe activities that causes harm to others or violate norms of due care.

1. Government Regulation and Environmental Safety

Government regulation is a primary pillar supporting environmental risk management. Global, national, state and local environmental regulations are a principle source of well-defined and accepted standards of behavior used to measure waste generation, hazard exposure and safety performance. In the US there are thousands of standards for air and water quality, hazardous waste disposal, and cleanup activities. Most of these national standards are administered by the EPA codified through laws enacted by Congress and via EPA's rulemaking authority. Other federal institutions administer environmental regulatory standards including OSHA, CEQ, and DOD. State EPAs and other state institutions also administer environmental regulatory standards, many of which are stricter and more comprehensive than the federal code.

Regulators gather ex ante information primarily through permit applications, audits conducted for licensure or land transfer, required reporting, and periodic inspections to

monitor compliance. They also receive ex ante information via proof of financial responsibility forms such as certificates of insurance required under RCRA. They get ex post information through public complaints, accident investigations, court proceedings, and during cleanup operations. Nearly all regulatory actions managing safety are punitive in nature, and ex post, after the discovery of violations. Fines are the most common action, some of which can be extremely stiff. For example, current EPA fines for each RCRA violation is up to $75,867 per day (Smith and Fanning 2020). Regulators can also revoke permits for accidents or repeated violations.

There are several recognized problems with managing environmental safety through regulation. First, as already mentioned, most regulatory actions are punitive and ex post in nature. Except for some state programs subsidizing safety investment there are few regulatory incentives encouraging firms to implement ex ante preventative safety measures. There are also too few government inspectors needed to monitor safety, and some firms are willing to risk fines in order to avoid compliance costs. The regulatory process is also highly political, with safety oversight and enforcement impacted by industry lobbying and the environmental preferences of the governing parties. Often, regulatory standards are suboptimal, compromising safety for political expediency. Regulation is also slow to react to new environmental risks, often requiring years for the enactment of new laws and the vetting of new standards via the regulatory process.

2. Court Litigation, Tort Liability and Environmental Safety

A second pillar of environmental risk management is the influence that court decisions and the threat of huge liability settlements have on firm safety behavior. The

courts are a common arena for addressing environmental issues and exposing unsafe behavior by polluting firms.

Generally, the courts do not create new environmental standards. However, court decisions can play a role in interpreting standards by determining the extent that polluters demonstrated due care in complying with government regulations and industry safety norms. The courts only gather information ex post, often long after both the pollution and harm occurs, and usually only for the specific legal case. This information is gathered via public complaints, investigations, subpoenaed records, oral and written testimony, and other evidence collected by the plaintiffs and their legal teams. However, much of the safety impact of litigation is ex ante as a deterrent, encouraging potential polluters to enact safety precautions to avoid huge lawsuit costs and harm to their business reputations. In fact, scholars have argued that liability may induce more environmental prevention than public regulation (Shavell 1984). Liability also buttresses safety ex post by providing a mechanism for victim compensation and site cleanup that optimizes cost internalization by potentially making polluters pay the full amount for harm.

Still, tort litigation like regulation has environmental safety policy issues related to fairness and efficiency. First, the court process is lengthy, expensive, and unpredictable. The latency period associated with identifying environmental harm and the lag between cause and effect makes identification of injurers and proof of causal relationships difficult. After long legal battles victims have no guarantees of fair compensation. Guilty polluters may declare bankruptcy and be unable to pay compensation or for court ordered cleanup costs. Even if the polluting firm has insurance, legal defense can consume much

of the indemnity coverage, leaving little for victim compensation. For example, a 1992 study by RAND Corporation found that in 1989, 88% of insurance outlays were transaction costs ($410 million) covering legal defense and court costs, with only $56 million spent on liability payments and cleanup costs (Acton and Dixon 1992, xi). Court rulings, particularly in the 1980s, were inconsistent, creating a great deal of uncertainty and risk that interfered with normal litigation, business and insurance processes.

3. Insurance, Marketplace Mechanisms and Environmental Safety

A third pillar of environmental risk management is marketplace policy instruments that primarily use private sector financial incentives and disincentives to influence firm environmental safety behavior. Specialty environmental insurance is the primary marketplace instrument that transfers a portion of the risk to an insurer, under agreed terms and conditions, in exchange for the payment of a risk-based premium. Insurance companies are experts on gathering and processing information on risk. They invest in the technology and the expertise to analyze risk in order to avoid adverse selection of unsafe prospects and to monitor clients for moral hazard issues that may arise after insurance is in place.

Specialty environmental insurers help to drive the adoption of new regulatory risk management and safety standards. For example, in 1990, Congress passed the Clean Air Act Amendments (CAAA) that included two new federal regulatory programs aimed at preventing releases of hazardous chemicals: OSHA's Process Safety Management (PSM) standard and EPA's Risk Management Program (RMP) modeled in part on insurer risk management programs. Under these new rules, regulators could make unannounced

inspections to verify compliance. Insurers participated in PSM/RMP trial audits and third party inspections (Barrish et al. 2000), and later mandated that applicable firms comply with these regulations as a condition of insurance. Insurers are also arbitrators of the many government regulations and private standards, helping clients to understand requirements and expecting them to adhere to ones most optimal in assuring environmental safety at an affordable cost. Insurers also create industry-specific underwriting standards that often exceed the safety levels required by regulators.

Much of the information that specialty insurers gather is ex ante, meant to verify safe operations and prevent claimable losses. Specialty environmental insurers have technical underwriters and engineers on staff to conduct site-specific audits and inspections. They required the insured to submit detailed applications outlining the operational history of the site, records of hazardous materials, past accidents or regulatory violations, etc. Some insurers may hire third parties to conduct more extensive inspections and to make recommendations on safety improvements. They may also require the insured to implement technologies to assure the continuous monitoring of site conditions. If a sudden accident occurs or gradual pollution is detected, insurers have teams of investigators to collect ex post information, provide recommendations on loss mitigation, assist with remediation, conduct claims adjustments, and pay settlements when appropriate.

Unlike regulation and litigation, insurance has extensive positive ex ante incentives to motivate safer client behavior. Most of these incentives involve reductions in premium rates reflecting implementation of new safety technology or improved risk management

practices. Thus, environmental insurance acts like a Pigouvian tax, with firms presented with a menu of premium discounts that they can receive in exchange for investing in safety. Likewise, insurers can impose ex ante or ex post penalties for accidents or failure to make required safety changes. These can include steep premium increases, reductions in coverage levels or, in the extreme, denial of coverage or policy cancellation. Since most policies are for a term of one year, this process is repeated annually with the assessment costs included in the renewal premium.

Similar to regulation and litigation, insurance also has environmental safety policy issues. Most notably, despite rigorous efforts to assess the risk and monitor client behavior, insurance can fall prey to adverse selection and can actually encourage moral hazard. Studies in the 1990s showed that within statistically defined limits, site assessments failed to detect contamination 40 percent of the time. Consequently, at that time, insurers likely covered many risky sites inappropriately. From a moral hazards standpoint, TSDFs may have less financial incentive to comply with costly safety regulations and to spend capital on expensive safety technology if they have insurance against pollution losses. Thus, insurance can dampen the deterrent and financial internalization effects of liability and regulation. Insurers manage this type of moral hazard through risk-internalization mechanisms such as co-pays, deductibles, and coverage limits.

There are also external moral hazard issues caused by insurance, such as encouraging victims to file unjustified claims and courts to make exorbitant judgments because insurers have deep pockets. Faced with potentially huge judgments, insurers contest

coverage and subsequently decrease safety by delaying victim compensation and site cleanups. Thus, as a standalone instrument of environmental safety policy, insurance has its limitations.

4. Safety through Synergy of Regulation, Litigation & Insurance

As described above and as outlined in Table 5.3 below, there is a synergistic relationship among regulation, litigation, and insurance that, if properly tuned and aligned, can enhance the safety of firms dealing with a variety of different emerging risk, including environmental risk. They play complementary roles in gathering information, establishing and enforcing standards, incentivizing or penalizing firm safety behavior, and internalizing these risks. In theory, an ideal combination of these three instruments could optimally interact to maximize safety (Faure 2014).

Table 5.3: Strengths, Weaknesses, and Synergistic Relationship Among Regulation, Litigation and Insurance in Managing Emerging Risk

Attribute	Type	Regulation	Litigation	Insurance
Ex Ante Information Gathering (e.g. Audits & Inspections)	Information Gathering	Both Strength & Weakness	Weakness	Both Strength & Weakness
Ex Post Information Gathering (e.g. Audits & Inspections)	Information Gathering	Both Strength & Weakness	Both Strength & Weakness	Both Strength & Weakness
Proof of Financial Responsibilty for Permitting	Information Gathering	Strength	Weakness	Strength
Ex Ante Standards Setting	Standards	Both Strength & Weakness	Weakness	Strength
Ex Post Standards Evaluation	Standards	Strength	Both Strength & Weakness	Strength
Flexibility Adapts Quickly to Changes	Standards	Weakness	Weakness	Strength
Fair Compensation for Victims	Risk Internalization	Both Strength & Weakness	Both Strength & Weakness	Both Strength & Weakness
Fast Compensation for Victims	Risk Internalization	Weakness	Both Strength & Weakness	Both Strength & Weakness
Ex Ante Incentives for Safety Investiment	Risk Internalization	Both Strength & Weakness	Weakness	Strength
Ex Ante "Deterrent" for Safety Violations/Accidents	Risk Internalization	Both Strength & Weakness	Strength	Strength
Ex Post Penalties for Safety Violations/Accidents	Risk Internalization	Both Strength & Weakness	Strength	Strength

This template can be used to analyze the any of the three regimes, and will be used in the Conclusion to compare one case study to another.

Using environmental risk as an example, from an information gathering perspective all three instruments have strengths and weaknesses. Both regulation and insurance have resources to audit and inspect hazardous waste operations however these resources are limited with different motivations for data collection. The EPA and other federal agencies work in collaboration with state programs to assure compliance with regulations, but political interests and funding modulates activity. EPA and most state inspections are highly targeted, focusing primarily on very large operators and allowing smaller operators to avoid inspections for many years. In contrast, insurers have a financial motive to conduct annual audits and inspections for firms of all sizes. They also have economic incentives for clients to share information that they might be unwilling to give to regulators. Insurers provide a certificate of insurance to regulators verifying proof of financial responsibility, while regulators audit TSDFs to assure financial protection is in place. Thus, regulatory and insurance information gathering complements each other providing a much broader view of firm environmental safety behavior than either collects on its own. Evidence gathered by investigators after accidents and in support of liability trials then adds further data to create an even more complete picture of each firm's overall safety behavior.

All three instruments also influence environmental standards development and enforcement. Both federal and state regulators produce volumes of environmental standards that complement and sometimes conflict with one another. Lobbying and

political activities often dilute these standards, making them suboptimal in assuring public safety. Sometimes states establish a stricter safety standard than the federal government. The courts use both federal and state regulations as a baseline for liability decisions, with violations validating safety negligence and regulatory compliance affirming safe behavior. However, through strict liability, courts can also establish a higher standard of care, finding firms responsible for environmental damage despite regulatory compliance. In addition, neither regulation nor litigation reacts quickly in responding to new environmental risk, while insurance can adjust to emerging threats by creating new underwriting standards, implementing new assessment procedures, and making changes to policy terms. Through policy language, insurers translate complex regulations into concrete rules, consolidate standards, and compel compliance in establishing an optimal level of due care.

Both regulation and litigation primarily use the threat of fines and penalties to encourage firm safety behavior. Both state and federal regulators have substantial fines for discovered violations which accumulate daily until the violation is corrected. Both federal and state environmental agencies also have grants, subsidies and tax incentives for specific programs such as brownfield cleanups (EPA 2020C), and removal and replacement of underground storage tanks (EPA 2020D). Litigation is purely punitive with the threat of huge liability decisions acting as a deterrent to bad behavior. Insurance provides more positive incentives encouraging safe behavior, using premium discounts to reward safety improvements. Insurance can also take punitive actions including

terminating coverage that, in turn can lead to regulatory action including revoking a firm's operating permit due to no proof of financial responsibility.

Finally, all three instruments compel TSDFs to internalize the cost of their hazardous waste operations by making them pay ex ante for environmental safety or ex post for environmental harm. Each has its advantages and disadvantages as an internalization agent. Litigation potentially maximizes the compensation of victims. However, it takes time and has very high transaction costs that can dilute the pool of funds. Further, victims are not guaranteed full compensation because of the time lag between exposure and the manifestation of harm, challenges in proving causality, inability to identify responsible parties, or insolvency of those legally responsible. In these ways, litigation is neither efficient nor totally equitable in internalizing environmental risk. Likewise, regulation compels firms to internalize environmental risk primarily through fines and penalties imposed ex post after a violation is discovered or an accident occurs. However, like litigation, the polluter's bad behavior might not be discovered until long after they've gone out of business. In addition, despite having proof of financial responsibility, firms still may have insufficient assets or insurance to cover these costs.

Insurance attempts to make firms internalize environmental risk by making them pay upfront through risk-based premiums and by leaving the insured clearly exposed to a portion of the risk through policy mechanisms. The strength of insurance is that it can motivate firms to invest in safety. Further, with well-defined standards, insurance can provide faster victim compensation and site cleanup than litigation or regulation, with lower overall transaction costs. Thus, insurance can be more efficient and equitable than

other policy instruments in internalizing environmental risk. The weakness of insurance is if insurers fail to adequately assess the risk, and improperly extend coverage or charge risk-inappropriate premiums. The challenge then is to determine insurability and provide coverage at a profitable and affordable price.

B. Specialty Insurance Policy Mechanisms & Environmental Safety

Thus, the overall goal of specialty environmental insurers is to profitably and affordably provide coverage by assuring that insured firms behave safely by adopting appropriate standards, adhering to regulations, minimizing liability losses, and acting responsibly when accidents occur.

Today, there are about 50 US specialty environmental insurance providers collecting over $2 billion in annual premiums (USI 2018) by offering over 150 types of environmental insurance products (IRMI 2020). Often specialty insurance covers non-actuarial risks where there is a lack of historical loss data to determine premiums. Instead specialty insurers rely on more subjective expert opinion, using scorecards to assess risk factors. They may assemble their own team of experts or partner with third parties to support their underwriting efforts.

Insurance products are differentiated based on a number of factors. First, products vary depending on the age and the lifecycle phase of the facility. Different products exist for new facilities, existing operations, sites that are undergoing closure, post-closure "brownfield" locations, and even abandoned land with suspected past industrial activity. New facilities are typically the easiest to assess with the insurer sometimes involved in the site and safety technology selection process. As facilities age, the degree of

uncertainty expands, increasing the likelihood of accidental releases resulting in claimable losses.

The second factor is the specific hazards that might be present. This includes not only chemical toxic waste, but also biological, nuclear, and manufacturing–related hazardous waste. Mixtures of various toxic materials, such as might be found at a public landfill or private hazardous waste storage facility, complicates the insurance process, requiring additional assessment and possibly different types of coverage for the same site.

The third factor relates to the economic or industrial activity that is being insured. Owners and operators of TSDFs are one activity category, as well as waste transporters such as ships, trucks and railroads which are particularly prone to sudden accidental releases. Other activities include environmental consultants, engineers and contractors hired to oversee or remediate hazardous sites, land developers and lenders looking to protect investments in brownfield projects, and product manufacturers who produce, use and dispose of toxic materials.

Combinations of these three factors result in a multitude of various policy types such as remediation lender pollution liability (LPL), contractor cleanup cost cap (CCC) and owner post-closure liability (PCL) coverage. All are modern variants of EIL with enhanced information gathering, advanced technical risk assessment and underwriting capabilities, updated premium safety incentives, and strengthened loss prevention and mitigation capacity. Many of the risk assessment and underwriting techniques utilized by specialty insurers today are similar to those developed by H. Clarkston Limited for EIL as described in Section IV-D. A brief review of how new techniques are utilized by

specialty insurers to minimize adverse selection and moral hazard, categorize good and bad risks, and ultimately improve client safety follows.

1. Specialty Environmental Insurance and Information Gathering

Environmental risk is highly complex, and specialty insurers need to gather extensive information on client past and present behavior to properly evaluate and classify the risk. Information gathering begins with the initial client application, and continues on with audits, inspections, technical risk assessment, underwriting, premium determination, policy issuance, loss control actions, and measures to mitigate losses when an accidental pollution release occurs.

Especially for complex environmental risks such as TSDFs, the application[5] can be extensive, with detailed questions on the applicant's operations. A single application may encompass multiple types of environmental coverage, and the applicant's representative needs to select and complete the questions for each desired policy. For TSDFs, questions are focused on the site to be insured and company's operations.

The application also includes questions about the firm's hazardous waste activities. This includes whether they are doing hazardous waste storage, disposal or treatment onsite and, if yes, details on the types of waste, quantities, and the methods used. There are also questions on the number and qualification of staff involved, their training, and whether there is any ongoing monitoring of tanks and testing of groundwater. They also want to know if the applicant is doing any offsite disposal with details on the type and annual quantities of materials, location and owner of external site, and how often and by

[5] This analysis involved the review of applications from several specialty environmental insurers including AIG, Zurich, and Chubb, for a variety of different coverage types such as PLL and LPL policies.

what type of carrier it is transported. The application also asks for information on how the site is regulated. The insurer will require information on regulatory compliance and if the applicant has in the past five years had any accidental discharges or been prosecuted for any violations.

In addition to the application, firms requesting new or renewed coverage will usually need to submit additional documentation that is audited by the underwriting team. US-based insurers audit site documentation following the International Organization of Standards (IOS) 14000 series of environmental management guidelines (IOS 2020) and strict insurance industry underwriting standards. Documents typically required include financial, business, insurance, regulatory and operational records. A primary purpose of the audit is to assure the firm's compliance with all applicable government regulations. The company will be asked to provide copies of all required permits, regulator inspection reports, and records of required reporting such as hazardous waste inventories and transport manifests under RCRA. Insurers will also check public records to confirm that the firm does not have any outstanding civil suits.

For new policies, and high risk renewals, the insurer will likely want to conduct an inspection. Insurance inspectors often use existing EPA RCRA /RPM and OSHA PSM guidelines.[6] However, unlike these government inspections, insurer inspections serve to identify risks and to assess possible loss scenarios that might result in claims. Also, while government inspections may result in citations, the insurance inspections proactively identify issues and suggest corrective actions to avoid violations and improve safety. The

[6] Information on inspections was collected from EPA, OSHA and insurance industry guidelines.

primary goal of the inspection is to confirm the information gathered in the application and reviewed in the audit. The insurance inspection also seeks to visually confirm that the facility is being operated in a safe manner following recognized and generally accepted good engineering practices.

In a typical onsite inspection insurer representatives visit the site for between 3 and 8 hours. Interviews are held with key management personnel including facility managers; environmental managers, engineers, health and safety directors, operations managers or foremen; and corporate risk management personnel. The key purpose of the interviews is to prepare an accurate description of the facility and its operations, assess key personnel understanding of safety protocols, and get firsthand knowledge of any potential issues that might have to be addressed. During an initial plant walk around they look for any obvious safety issues. They assess the level of housekeeping; examine the grounds for distressed vegetation; verify that personnel are using required protective equipment; and view locations where air and waste water discharge.

The remainder of the inspection will depend on the type of operations and nature of the hazards present. They often select one or more processes to undergo more intensive evaluation. For example, if the TSDF is a landfill, the inspector may wish to check the condition of the liner and water levels in the leak detection sumps. If it is a storage facility, the inspectors will check the status of any tanks to see if there are any signs of corrosion. In some cases, the inspectors may test groundwater, soil, air emissions to confirm compliance with regulations.

All the information collected through the application, audit, site inspection, and monitoring is used by the specialty insurer's engineers or third party consultants to write a technical risk assessment for insurance underwriting, risk segmentation, and premium determination purposes.

2. *Specialty Environmental Insurance and Environmental Site Assessment (ESA)*

For specialty insurers, the environmental site assessment (ESA) is the interdisciplinary process for identifying and analyzing all of the hazards and risk factors that could result in claimable losses and help determine if those risks are insurable. Usually, the ESA is performed by a trained environmental professional knowledgeable in the appropriate standards, and supported by a multidisciplinary team of scientists. The team tailors the ESA to the exposures presented by the operations (e.g. asbestos) and the type of specialty coverage sought (i.e. CCC).

The ESA team gathers and analyzes the site information specified in the previous section typically following standards established by the American Society for Testing and Materials (ASTM). The ASTM created and updated these standards to satisfy CERCLA's All-Appropriate-Inquiry" requirements for evaluating a property's environmental conditions and assessing potential liability for any contamination (40 CFR 312.20). Most of the information is gathered using a Phase I ESA following ASTM's E-1527 standard (Johnson 2014).

The ESA's primary purpose is to evaluate the frequency and magnitude of health risks to humans and ecological exposures that may occur as a consequence of contact with hazardous materials on the site. However, in addition, the ESA looks to assess the

risks to and the threats from the surrounding community. The assessment team looks at current geological maps and aerial photographs to understand local drainage patterns and topography. They identify nearby surface water, protected environments, and the proximity of residential populations, and other industrial activities. They examine local insurance maps to see if any nearby properties have been used for high-risk purposes. They search available federal, state, county, and municipal records to identify possible sources of contamination. They will also interview neighbors to see if there were any past unreported pollution events or transport activity in and out of the site. They may also be concerned about security risks such as vandalism or terrorism and, if the site is in a dangerous area, require additional security measures such as more fencing, alarms, or guards.

If evidence of contamination is discovered during the Phase I ESA, or if the hazard warrants additional attention, the insurer may request a Phase II ESA following ASTM E1903-11 standard assessment procedures (ASTM International 2011). The Phase II ESA is a more intrusive investigation than Phase I involving the collection and laboratory analysis of soil, groundwater or building materials. The team will typically focus the testing specific site locations such as wells, underground tanks, or for the presence of specific hazardous materials like petroleum, PCBs, heavy metals, pesticides, asbestos and mold. If further evidence of contamination is uncovered, the insurer may require broader site testing to characterize the extent of contamination (Phase III ESA) and likely will expect the applicant to remediate the site prior to extending coverage.

Throughout the ESA process, the team works closely with the underwriters to address coverage issues and particular areas of concern. For example, the underwriter may have concerns about the qualifications of operating personnel, regulatory compliance, emergency preparedness, or specific operational processes. In addition to the ESA process, the assessment team and underwriters will consider other less tangible risk factors that can affect insurability. For example, political and regulatory risks can increase or decrease with changing federal or state regimes. New regulations may emerge and firms may find that they are no longer in compliance. Technological risk can also increase with the development of more sensitive hazard detection equipment, finding contamination which no previous technology had found before. New chemical substances may be developed creating new liability exposures.

Once the risk assessment is completed, the team will meet with the underwriters to discuss the findings, and write a detailed report that includes their loss control recommendations.

3. *Technical Underwriting, Premium Determination and Policy Terms & Conditions*

Like the assessment team, specialty insurance underwriters typically come from a technical background, able to synthesize the complex information provided by the team with scientific underwriting guidelines and methods. Environmental insurance underwriters are employed by an insurer to evaluate, select and price risks to be accepted by that insurer. They decide whether coverage should be extended and, if yes, the amount of coverage and the premium to be charged. Underwriters also segregate risks, discriminating among different classes of potential policyholders using identifying firm

characteristics as industry, size, revenue and geographic location. In this way they are able to compare one firm against another, differentiate good risk from bad risk, and make insurability and pricing decisions accordingly.

Most specialty environmental insurers are “surplus” or “non-admitted” carriers, not approved by individual state’s insurance departments or not necessarily subject to state insurance regulations. Many states allow non-admitted carriers to transact business in their state if there is a special need that cannot or will not be met by admitted carriers. As such, these insurers are able to charge unregulated “market-based” premiums, for customized coverage, following their own set of proprietary underwriting guidelines. Coverage, premiums, and underwriting standards can vary considerably from carrier to carrier. Acceptance or rejection of coverage can fluctuate based on current market conditions, and the carriers “risk appetite” which can vary considerably from one insurance company to another. Disproportionate focus on profitability may result in some insurers taking on excessive risk. Thus, the ability of specialty insurers to help clients manage risk also depends on their competence to regulate their own risk behavior.

Once the underwriter reviews all of the information gathered from the client application, audit, onsite inspection and risk assessment, they will coordinate the insurer’s decision to accept or reject the submission. In making this decision, the underwriter will consider the limits, deductible, copays, and coverage terms sought by the applicant. If the submission is accepted, the underwriter will select appropriate policy forms in the jurisdiction where it operates, and determine the appropriate policy period, limits, aggregates, and deductibles. The underwriter will then calculate the premium

amount including the costs associated with the assessment, deductibles, other coverage terms, and reinsurance. The underwriter will also consider the market conditions and the price the applicant might secure for similar coverage from competitors. Finally, a profit margin on top of estimated costs is included in the price. Once the proposed premium price is established, the underwriter presents a quotation and, if accepted, negotiates the terms and policy execution.

As previously noted, specialty environmental insurers use risk-based premiums and policy mechanisms to encourage policyholders to invest in cost-effective loss reduction measures. Each specialty insurer has its own proprietary method for rating environmental risks and establishing premium pricing. However, evidence from the literature suggests that "similar methodologies are employed by the major U.S. markets and variations are found principally in the weighting of factors and the degree of subjective evaluation permitted to or exercised by individual underwriters" (Kronenberg 1995, 338). The discussion below describes a generalized ratemaking process[7] for establishing PLI premium pricing. Other types of PLI (e.g. CCC) would involve the inclusion of additional risk factors specific to the industry, hazard or activity.

When PLI first appeared during the 1970s, there was very little historical loss data to allow for actuarial determination of premiums. However, over time, some actuarial data has been accumulated allowing specialty insurers to segregate environmental risks by class of industry, size, age, location, and other known rated factors. They start with an initial base rate (e.g. $5000) from a rate schedule for an industry class, for a level of

[7] The ratemaking process comes from a number of insurance sources including Werner, et al. "Basic Ratemaking: Fifth Edition," Casualty Actuary Society, May 2016, and Kronenberg (1995).

annual coverage (e.g. $1 million per incident/$3 million aggregate). They then apply established relative risk factors for size, age, location, and other applicable schedule factors to determine a modified base rate (MBR).

MBR = Initial Base x Size Factor x Age Factor x Location Factor x Other Factors

After the MBR is determine using known factual data, underwriters then apply more subjective exposure criteria for both gradual and sudden pollution risks. Depending on the type of facility, these exposure factors (EF) can be numerous and highly complex. Each EF reflects a variable that can cause increased likelihood and consequence of loss above the MBR risk. One key EF is the type and quantity of hazardous substances present. Substances can be rated individually, and also based on their possible interactions with other chemicals. Regulatory compliance is also a key EF, with the number and type of past violations highly considered in premium determination. There can also be specific EFs for gradual pollution like the existence and number of underground tanks, and for sudden pollution such as the presence of explosive or highly flammable substances. Each exposure factor is scored (e.g. scale of 1 to 5) based on degree of severity, and then assigned a weighting to reflect the relevant impact of an EF to other factors. The results are then tabulated to compute an exposure modified rate (EMR).

$$\mathbf{EMR = MBR \times EF_1 \times EF_2 \times \ldots EF_n}$$

Either the MBR or EMR can be significantly adjusted by credits or debits that are often chosen by the applicant and that can reflect and influence their future safety behavior. The first adjuster is the deductible (D_a) where the applicant chooses the initial

amount that they will pay on an insurance claim before the insurance coverage kicks in. Large deductibles, where the insured assumes a large portion of the risk can result in large premium discounts of 30% or more. Specialty environmental policies with sufficient coverage to satisfy RCRA minimums can have very large deductibles of $100,000 or more. Insurers usually prefer large deductibles because they eliminate small nuisance claims, provide incentives for loss control, reduce an insurer's exposure, and characterize low risk applicants that are unlikely to file a claim.

Specialty environmental policies can also include coinsurance adjusters (C_a) whereby the insured agrees to a pay a percentage (e.g. 20%) of the total losses up to the coverage maximum. Thus for $6 million in coverage with a 20% copay, the insured could pay as much as $1.2 million, as well as all of the losses that exceed the coverage maximum. This internalizes much of the risk with the insured encouraging safer behavior. Likewise, insurers also offer client "schedule rate" adjustments (S_a) for environmental safety enhancements "that are expected to have a material effect on the insured's future loss experience" (Werner et al 2016, 297). This includes correcting a previously identified hazard, installing monitoring technology, organizing a safety program, or updating the site's emergency response plan. Implementing loss management capabilities or contrarily failing to implement recommended safety changes can result in scheduled rating credits or debits of 5% to 15% for each safety action (Werner et al. 2016, 298).

Finally, the underwriter adjusts the rating based on a number of subjective and objective factors. As noted above, despite an exhaustive risk assessment, there can still be

a great deal of uncertainty regarding actual site conditions, as well as future regulatory and technological risk. To account for this uncertainty, underwriters can modify the rate based on a subjective uncertainty factor (UW_{uf}) using their expert knowledge and experience. After any uncertainty is accounted for, the underwriter adds the any underwriting expenses (UW_e) such as costs for the inspection, risk assessment, and commissions; and also the desired underwriting profit (UW_p) varying based on competition and market conditions. The premium is then calculated as follows:

$$\textbf{Premium} = (\textbf{EMR} \times D_a \times C_a \times S_a \times UW_{uf}) + UW_e + UW_p$$

Another way that insurers manage firm risks is through the terms under which coverage is extended. The policy[8] is a contract which defines who and what is covered, the responsibilities and rights of both parties, and the circumstances when coverage is granted or denied.

Some of the policy language is negotiable, with the understanding that either party can decline coverage. As already noted, most pollution policies are written on a claims-made basis for a period of one year. This generally means that any claims for loss compensation must be submitted during the policy year plus an extended reporting period of 60 days following the policy's normal expiration. However, the insured can negotiate up front and optionally purchase a longer reporting period or claims-made term of up to 5 years, provided the entire premium is paid up front, and subject to additional technical assessment and underwriting scrutiny.

[8] Information on policy terms, conditions, and exclusions was collected from sample broad form environmental liability policies from AIG, Chubb , Zurich, QBE, and other insurers downloaded from the National Association of Insurance Commissioners (NAIC) System for Electronic Rates and Forms Filing (SERFF) database at: https://www.serff.com/serff_filing_access.htm

The policy defines the entities covered (Named Insured), type of pollution activity insured (e.g. CCC), the type of pollution indemnified (e.g. sudden, gradual or both), specific hazards covered (e.g. asbestos), and the harm for which victims can be reimbursed.

The contract also specifies the rights of the insurer to collect and the responsibilities of the insured to provide information on changes to operations or conditions that alter the risk profile of the insured property. Most important among the insurer's rights is the guarantee that the insurer is allowed with reasonable notification, to "conduct inspections, surveys, audits or reviews" of the insured's location and operations including "the taking of samples, interviewing of employees," and accessing "materials or information" concerning the operations, structure or financials of the insured's company (Philadelphia Indemnity Policy, 14). Likewise, in the event of an accident that might result in a claimable loss, the insured is required to take all responsible steps to prevent or minimize losses and immediately notify the insurer of any event that might give rise to a claim (Chubb Insurance, 18). The insured is also obligated to provide all information relevant to the event and to cooperate in any claims investigation. The insurer can cancel or refuse to renew the policy if the insured fails to comply with any term or condition.

Specialty insurers also use exclusions to promote responsible behavior by precluding coverage for certain types of risky activities. One common exclusion aims at preventing the insured from fraudulently misrepresenting or willfully failing to disclose any pollution condition in existence prior to the policy start date (Known Condition Exclusion). Coverage can also be excluded if the insured intentionally causes harm

(Intentional Harm Exclusion), fails to comply with environmental statutes or regulations (Intentional Non-Compliance Exclusion) or otherwise violates the law through criminal activities (Criminal Activity Exclusion). Likewise, compensation for fines and penalties associated with a violation are also typically excluded. As already noted, insurers can also specifically exclude coverage for a specific toxic substance (e.g. asbestos) or condition (e.g. UST) not specified as part of policy. Often, specialty insurance provides coverage in excess of other types of insurance that a firm may have. Thus, employee liability arising from a pollution event would first be covered by a firm's workers compensation plan as the primary insurance before pollution coverage is tapped.

4. *Specialty Environmental Insurance Loss Control and Mitigation*

A final way that specialty insurance can improve client environmental safety is through the offering of policy period loss control and mitigation services - risk management techniques that seek to reduce the probability and consequences of losses. An effective loss control and mitigation program will help policyholders minimize claims and insurance companies reduce losses. Insureds benefit from lower premiums while insurers can reduce their costs and increase profits by having to pay fewer and less costly claims. Virtually all specialty environmental insurance carriers, either directly or via third-party proxies, offer expert loss control services to advise their policyholders on how to avoid exposures and excessively dangerous hazardous waste activities.[9] The cost of these services is typically included within the premium dollars paid. Standard services

[9] Information on environmental loss control and mitigation services was collected from specialty environmental insurers including AIG, Chubb, Zurich, AXA XL et. al. as well as third party associates such as VERTEX and AFIRM.

include loss control education, tool kits, and guidance that firms can use in making decisions affecting their exposure to environmental loss.

More enhanced services include 24-hour phone consulting and the deployment of onsite experts who conduct inspections and make recommendations on safety improvements. These experts also conduct training, coach safer conduct, and help the insured develop written safety plans. Because specialty environmental insurers have access to multiple client experiences, they can analyze loss trends and make recommendations on new best practices, standards, and safety technology. They also stay abreast of changes to state and federal regulations that could affect policyholder safety and operations. They then use this knowledge to incentivize clients to adopt new safety procedures and technology, rewarding cooperation with premium discounts, lower deductibles, or longer and more extensive coverage. Throughout this process they monitor client implementation and in some cases assist in safety system performance testing and certification.

Insurers also have a vested interest in encouraging and helping clients to quickly mitigate environmental damage when accidents occur. This encouragement begins with policy conditions requiring policyholders to “take all responsible steps” to minimize damage and “immediately notify” the insurer when a potentially claimable event occurs. Following an accident, insurers can provide policyholders access to around the clock emergency response services. They can assemble and dispatch teams of emergency response contractors, disaster recovery and restoration professionals, and environmental consultants to control remediation costs and minimize environmental liabilities. They can

also organize a forensic investigation to determine the cause of an accident, the extent of damages, and the best way to manage claims. If litigation transpires, insurers will finance the insured's legal defense, manage litigation expenses, and if necessary be involved in the negotiation of settlements with victims. In this way, specialty insurers provide a mechanism to efficiently deal with environmental harm, assure victims are compensated, and better allow environmental safety to be restored.

VIII. Evidence of Role Regulation & Insurance Play in Managing Safety

This section provides evidence of the interaction of regulation and insurance in managing environmental safety. This evidence is based on data from the EPA's Enforcement and Compliance History Online (ECHO) Database - more specifically from the Resource Conservation and Recovery Act Information System (RCRAInfo) data subset. RCRAInfo contains data on evaluations, violations, and enforcement activities for over 1.1 million hazardous waste facilities subject to RCRA regulations, including requirements for financial assurance under 40 CFR 264 and 265, Subpart H. Of these RCRA facilities, there are currently 1808 TSDFs operating in 49 states, Puerto Rico, and the District of Columbia. Of these, 1608 are privately owned and subject to RCRA financial protection requirements, while 200 are owned by public entities including 162 by the federal government and 38 by states and municipalities. Texas has the most TSDFs (171) while Washington DC only has one federally- owned TSDF, and New Hampshire has none. The medium number of TSDFs per state is 22.

During the 40-year period 1980 to 2020, regulators conducted 141,503 "evaluations" of TSDFs including onsite inspections, groundwater monitoring, and offsite financial and

non-financial records review – an average of roughly two evaluations per TSDF per year. Over 90% of evaluations are conducted by state regulators, with only 9.1% conducted by the EPA or EPA hired contractors. Thus, state regulators are the primary overseers and enforcers of both state and federal environmental regulations. This includes confirming adherence to financial protection regulations. Over the same 40-year period, states and the EPA conducted nearly 23,000 Financial Records Reviews (FRRs) to verify that TSDFs have adequate financial protection through insurance or other financial mechanisms to internalize the costs to clean up, close and maintain their facilities throughout its life cycle.

However, not all states evaluate TSDFs equally. States such as New Jersey (283), North Carolina (240), Colorado (176) and Montana (174) evaluate private TSDFs at three to four times the medium state rate of 68 evaluations per TSDF over the period 1980 to 2020. In some cases these and other states conduct nearly annual FRRs to verify financial protection. Conversely, other states, most notably Texas (21), Connecticut (21), and Vermont (21) conduct evaluations on average only every other year, and rely on the EPA to conduct FRRs. Nearly a third of states conduct few if any FRRs (5 or less over 40 years). Thus there is a notable dichotomy between states that rigorously evaluate TSDFs safety and financial protection, and those that do not.

While one might expect that states with more evaluations might have more opportunity to find violations, this is not always the case. As shown in Figure 5.2, states such as North Carolina (16) and Colorado (21) with higher levels of financial and non-financial evaulations had far fewer violations than the medium TSDF state average (33).

Possibly this is due to the additional scrunity and pressure for facilities in those states to implement safety measures to avoid violations. Likewise states that had little oversight including Texas (26) and Connecticut (28), while below the medium, still had more average violations per TSDF than high oversight states.

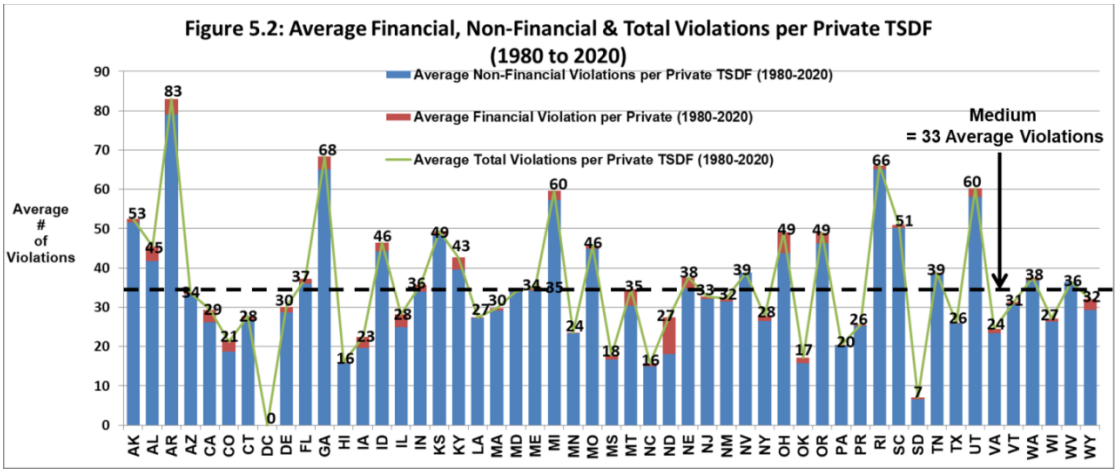


Figure 5.2: Average Financial, Non-Financial & Total Violations per Private TSDF (1980-2020) (Source EPA)

One way to visualize the interrelated roles that regulation and financial protection (e.g. insurance) play in managing environmental safety and internalizing environmental risk is through analysis of historical trends. In this analogy evaluations represent safety verification and violations symbolize unsafe behavior.

Figure 5.3 shows both annual evaluations and violations for all TSDFs over the period 1979 to 2020. Between 1983 and 1988 there was a rapid rise in the number of annual evaluations and violations. By the early-1990s, evaluations steadied out at between 3800 and 4500 per year, but violations began to gradually decrease, declining by over 50 percent by 2010 – TSDFs were getting safer.

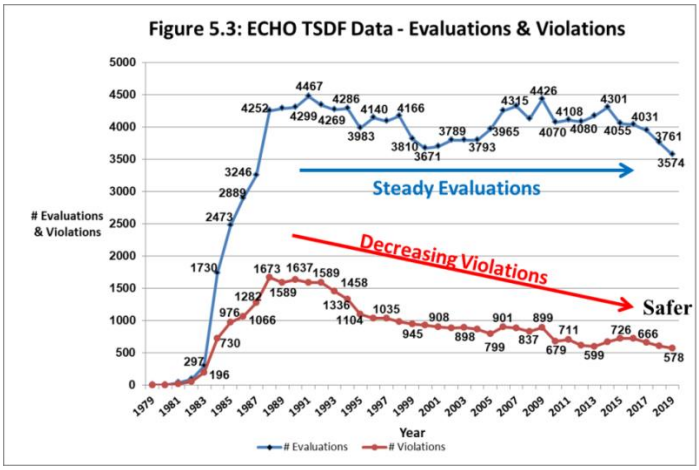


Figure 5.3: ECHO TSDF Data – Evaluations & Violations (Source: EPA)

Figure 5.4 shows the trends in financial evaluations and violations over the same period. Once again you see a rapid rise in financial evaluation and violations. The rise in financial violations corresponds closely to the crash of the environmental insurance market between 1985 and 1992. TSDFs could not secure financial protection from insurers and were often found in violation of RCRA regulations. Financial evaluations actually increased by nearly 50 percent between 2005 and 2007, reaching a peak in 2014 (926). However financial protection violations gradually decreased during this same period. Despite more examinations, regulators were finding fewer financial protection violations. TSDF operators were better internalizing their risk through insurance or other financial mechanisms.

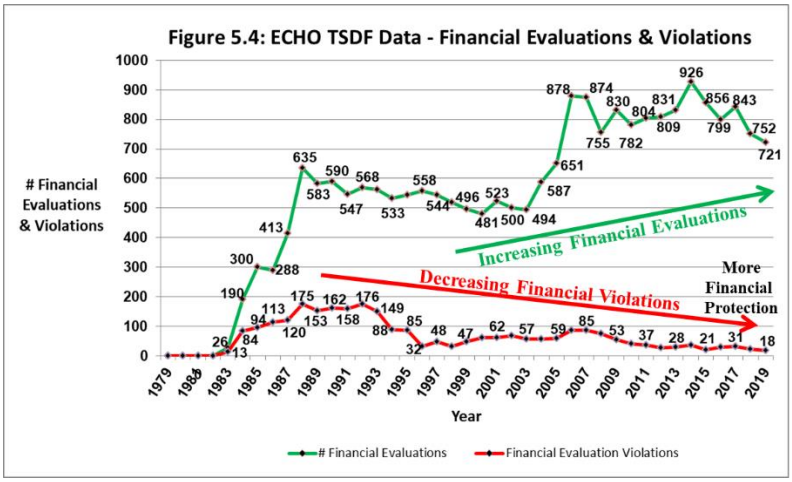


Figure 5.4: ECHO TSDF Data – Financial Evaluations & Violations (Source: EPA)

Another way to visualize the roles of regulation and financial protection in managing environmental safety is through the creation of indices to allow comparison between individual TSDFs. The first index is the ratio of non-financial evaluations (NFEs) to non-financial violations (NFVs) = NFE/NFV. NFEs and NFVs specifically deal respectively with safety evaluations and safety violations. The logic of this index is that TSDFs with high indices that have many evaluations and few violations are safer than TSDFs with low indices that have few evaluations and many violations.

Likewise, a second index looks at the ratio of financial evaluations (FEs) to financial violations (FVs) = FE/FV. This index can only be applied to private TSDFs, since government TSDFs are not subject to RCRA financial protection regulations. The logic of this index is that private TSDFs with high indices that have many financial evaluations and few financial violations are more likely to have insurance (or other forms of financial protection) than private TSDFs with low indices. The NFE/NFV index can be calculated

for each state or individually for all 1808 TSDFs, while the FE/FV index can be calculated by state or individual TSDF, but only using data for the 1608 private TSDFs.

Figure 5.5 below maps all 1784 TSDFs in the continental United States including 1592 private TSDFs (flags), 154 federal government owned TSDFs (stars) and 38 state owned TSDFs (diamonds).The size and color of the marker for each type of TSDF indicates the magnitude of the NFE/NFV index for the site, with larger black markers depicting the safest facilities with the highest NFE/NFV indices. The FE/FV index is shown using a heat map with deep red and intense yellow indicating areas where the index is high, and light blue and white showing areas where the index is low. Several observations can be made from this data. First, black high NFE/NFV index TSDFs often cluster together in the Carolinas, New Jersey, upper mid-west, lower Mississippi Valley, Florida, and Colorado. Second, these high NFE/NFV index clusters are often located in intense yellow and red areas of the heat map where the FE/FV indices are high. This provides evidence that environmental safety as indicated by high NFE/NFV index could be influenced by financial protection as indicated by high FE/FV index. Further, white and light blue areas with low FE/FV indices seldom contain black flag TSDFs.

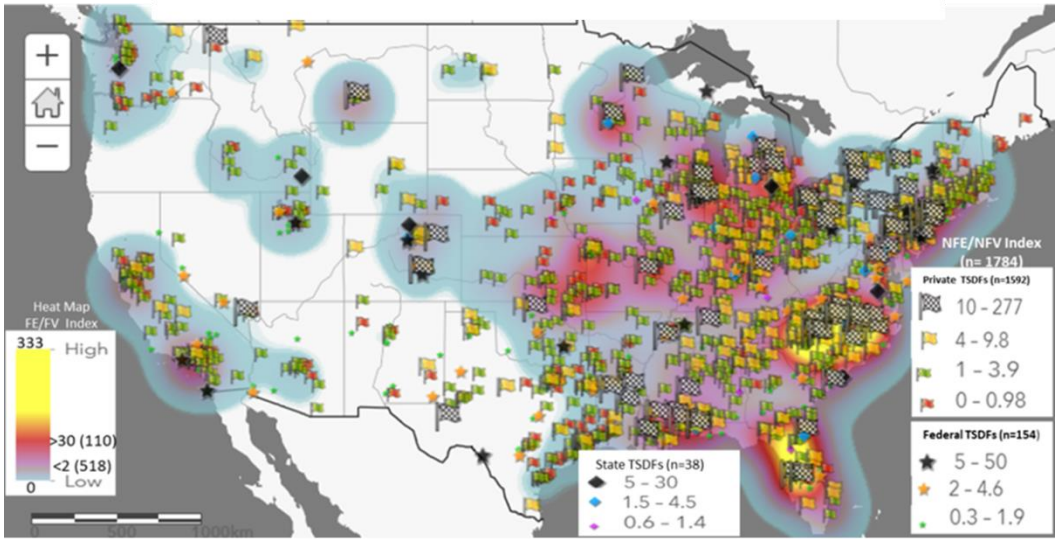


Figure 5.5: Continental US TSDFs with NFE/NFV Index Markers & FE/FV Heat Map

Figure 5.5: Continental US TSDFs with NFE/NFV Index Markers & FE/FV Heat Map (Source: EPA)

This section used EPA ECHO RCRAinfo data on TSDF evaluations and violations to provide evidence of the interaction of regulation and financial protection (including insurance) in managing environmental safety. The evidence also supports the primary hypothesis that insurance can improve the safety posture of firms engaged in emerging technologies.

IX. Lessons Applicable to Managing Other Emerging Technological Risks

So what do these experiences teach us about the role insurance plays in helping to manage environmental safety, and how can these lessons learned be applied to managing the risks associated with other emerging technologies?

Lesson #1: Synergistic Relationship among Regulation, Litigation and Insurance

One of the key findings of this case study is that there is a synergistic relationship among regulation, court litigation and insurance that, if properly tuned and aligned, can

enhance the environmental safety of companies involved with hazardous wastes, and consequently the safety of the public. Each element complements the other in gathering information, establishing and enforcing standards, incentivizing or penalizing firm safety behavior, and internalizing risk. When these elements are not aligned, such as occurred in the 1980s, safety can be compromised.

Lesson #1: *It is important that all three safety elements be available and aligned to optimize the safety and management of future emerging technological risks.*

Lesson #2: **Insurers Can Underestimate Risk Exposing Them to Excessive Losses**

Insurance is a competitive business and the lure of new coverage opportunities with potentially high profit margins may cause some insurers to underestimate the risk and extend ill-considered coverage that is not appropriately priced. During the 1980s, many insurance companies rushed to provide EIL policies, but all but AIG failed to adequately assess the risk, with several high profile insurers ending up in bankruptcy.

Lesson #2: *Insurance covering emerging risks needs to be priced with risk-based premiums built on data gathered and analyzed by a competent team of technical assessors and underwriters.*

Lesson #3: **Required Financial Protection – Unintended Consequences**

RCRA mandates that all operators of TSDFs have proof of financial responsibility as a condition of permitting. This mandate, fulfilled through the purchase of insurance or operator-funded self-insurance internalizes the risk of an environmental accident by making the polluter pay for harm caused by their hazardous waste activities. However, when environmental insurance virtually disappeared in the 1980s, many small operators were forced out of business. Further, contractors hired to cleanup polluted sites were

unable to secure coverage, hampering cleanup efforts, and ultimately decreasing environmental safety.

Lesson #3: *Mandating financial protection can have unintended consequences that must be considered when trying to maximize both technological benefit and safety.*

Lesson #4: Role of Key Events in Shaping Emerging Technology Insurance & Safety

Like nuclear insurance, major pollution events shaped the evolution of environmental insurance. These events included sudden accidents such as the Santa Barbara oil spill resulting in major revisions to CGL coverage; and gradual pollution catastrophes like Love Canal, and subsequently found at thousands of toxic waste sites around the US. The disaster at Love Canal led to the passage of CERCLA, massive litigation, the creation of the "absolute" CGL pollution exclusion, the collapse of the pollution insurance market, and the eventual creation of new types of specialty pollution coverage customized to insure specific industries and environmental risks.

Lesson #4: *The likelihood of similar seminal events needs to be considered as the insurance regimes for new emerging technologies evolve.*

Lesson #5: Site-Specific Claims-Made Coverage and Customized Policies

One of the hallmarks of early pollution coverage was that, unlike CGL insurance, it was usually issued for a specific site, on a "claims-made" basis, typically for a period of only one year. By making these policies site specific, insurers could focus their attention on assessing a specific set of hazards in a relatively contained space. Further, claims-made policies required that insured undergo an initial screening, report any claims during the policy period, and have annual examinations as a condition of renewal. Thus, site-specific claims-made coverage, limited the insurer's exposure to a specific time and

place, and increased the likelihood that any issues would be quickly identified and mitigated, minimizing possible claimable losses.

Lesson #5: *Future emerging technology insurance may require similar underwriting scrutiny and policies customized to handle the unique hazards and uncertainty*.

Lesson #6: Importance of Well-Defined Standards to Measure and Optimize Safety

In order for insurance and other mechanisms to manage emerging technological risks there needs to be well-specified and accepted standards of behavior that make these risks measurable. Standards definition and acceptance, including those created through government regulations, are influenced by both political and economic forces. Suboptimal standards decrease safety or create unaffordable cost burdens on some firms. One role of insurance is to arbitrate standards, help clients understand sometimes competing safety requirements, and incentivize them to adopt those that measurably improve safety at an affordable cost.

Lesson #6*: Insurers can help emerging technology firms analyze the cost and benefits of risk reduction measures and optimize safety*.

Lesson #7: Need for Incentives for Safety Investment & Fines for Unsafe Behavior

Given the profit motive of private TSDFs, most want to invest in activities that maximize revenues and minimize costs. Safety as a standalone activity rarely produces revenue, but can in tandem with other activities reduce the probability and consequences of losses. Environmental regulation and litigation can result in stiff penalties for a firm's failure to comply with safety standards or by causing environmental harm. Both can also incentivize ex ante prevention mainly through the fear of massive fines or liability settlements. Insurance also uses both incentives and penalties to influence firm safety

behavior. Unlike regulation and litigation, insurance has more ex ante positive incentives for firms to invest in safety including premium discounts, smaller copays and deductibles, and higher coverage levels that reduce firm costs and help their bottom lines. Insurance premiums and safety investments are also tax deductible, often in the year that they are made. Penalties and liability settlements may or may not be deductible and can be applied to taxes in later years.

Lesson #7: *Insurance for future technologies should also provide similar ex ante investment and tax relief to spur client positive safety behavior.*

X. Conclusions

This case study examined the role that insurance plays promoting safety and managing risks for firms operating chemical production and hazardous waste disposal facilities in the U.S.

As shown in this case study, insurance can be a powerful public policy tool in incentivizing private sector companies to proactively manage environmental risks. Insurers through premium discounts and other measures, motivate firms to invest ex ante in loss prevention measures. They also have resources and business motivation to verify client safety behavior through specialized information gathering and risk assessment capabilities. Further, they offer their clients loss control and mitigation services to reduce loss probability and consequences if an accident occurs.

However, insurance is not a panacea. If they are not careful, it can fall prey to adverse selection and moral hazard, underestimate the risk, and improperly insure clients with non-risk-based premiums. When this happens, as it did for environmental insurers in

the 1980s, the market can fail, some insurers can become insolvent, and insurance can become unavailable.

The key lesson that can be learned from the environmental insurance story is that there is a synergistic relationship among insurance, regulation, and litigation that when properly aligned can optimize firm risk management behavior and consequently the safety of the public. Each element provides both incentives and penalties that influence firm safety behavior. All three elements also gather information on firm safety either before or after an accident occurs. This case study provided evidence that insurance can be a better ex ante public policy mechanism for collecting information, assessing risk, and motivating private sector firms to invest in safety measures before an accident occurs. It also provided evidence supporting the primary hypothesis that insurance can improve the safety posture of firms engaged in emerging technologies.

Chapter 6: Insurance as a Private Sector Risk Regulator & Promoter of Safety: Managing Cyber Risk at U.S. Healthcare Firms (Case Study)

I. Introduction

How has insurance promoted better cybersecurity and safety at private U.S. healthcare firms, and what lessons can be learned from and applied to other emerging technological risk regimes? This case study examines the role that insurance plays in promoting safety and managing cyber risks for firms involved in delivering healthcare services in the United States.

This case study will examine the development of cybersecurity and cyber insurance for the healthcare industry beginning in the late-1980s and continuing to the present day. It will also provide evidence that cyber insurance can be a powerful public policy tool in incentivizing private-sector healthcare firms to manage privacy breaches and other cybersecurity risks.

The healthcare sector was chosen as the focus of this cyber insurance case study for several reasons. First, like the other case study regimes, U.S. healthcare cybersecurity activities are federally regulated by the Department of Health and Human Services (DHHS) - Office of Civil Rights (OCR) under the ***Health Insurance Portability and Accountability Act*** **(HIPAA) of 1996**, and ***Health Information Technology for Economic and Clinical Health (HITECH)*** **Act of 2009**. Under HIPAA and HITECH, healthcare "covered entities" are required to comply with HIPAA Privacy and Security

Rules, and notify OCR of any data breach involving 500 or more records. Then, OCR posts these breaches to a publicly accessible breach portal. Through August 13, 2021, a total of 4,171 breaches were reported, exposing over 305 million records (OCR 2021). This data, along with over 1400 additional healthcare breaches identified from other sources are used to create a new database – the ***Healthcare Cyber Attack Database (HCAD)***.

A second reason for choosing the healthcare sector is that it is large and diverse, allowing the analyses of wide variety of different sizes and types of public and private entities. Today there are over 20 million healthcare workers in the US, employed by an estimated 784,626 U.S. healthcare firms supporting $3.4 trillion in healthcare spending (PolicyAdvice 2021). The data in HCAD has been divided into 27 sub-sectors (e.g. doctors, hospitals, insurers), each with unique characteristics including size, specialty, operations/ownership and technological sophistication that provide different vulnerabilities for cyber-attackers to exploit.

Finally, a third reason to study this sector is because healthcare sector firms historically have been the target of more cyber-attacks than other sectors. This is due, in part, to the high value and sensitivity of healthcare data that makes sector entities susceptible to both internal and external hacks, and especially ransomware attacks that can immobilize entity operations or hold hostage critical patient data, unless an extortion payment is made. To deal with these issues, many healthcare sector firms have turned to cyber insurance to help manage the risk. Subsequently, the take-up rate for cyber insurance is higher than any other sector.

An econometric analysis of the HCAD data over the period 2015 to 2020 reveals several key findings. First, cyber insurance can have a small but significant positive? impact on healthcare-sector cyber safety as measured in both frequency and magnitude of cyber-attacks. This correlation is more pronounced in smaller, for-profit private healthcare firms such as individual and group practices than in larger, not-for-profit public entities such as government-operated facilities and health plans. HCAD quantitative evidence also indicates that cyber insurance may be more effective in helping firms manage non-ransomware, internal attacks than external hacks.

The organization of the remainder of this case study is as follows. Section II describes the early history of healthcare industry cybersecurity and cyber insurance including initial breaches, the promulgation of HIPAA, and other federal and state privacy and breach reporting regulations, and the concurrent development of early forms of healthcare cyber insurance. Section III discusses the political economy of healthcare cybersecurity and cyber insurance including an overview of the healthcare industry ecosystem and both the benefits of healthcare technology adoption and costs associated with healthcare cybersecurity and cyber breaches. Section IV reviews and analyzes healthcare cybersecurity vulnerabilities, threats and risk, followed by Section V that provides information on healthcare cybersecurity safety actions including technical, regulatory, legal and private sector insurance mechanisms. Section VI then discusses the healthcare cyber insurance market, coverages and specific healthcare cyber safety practices. Section VII then uses the HCAD data to conduct a regression analysis to examine how insurance safety practices interact and complement regulatory and liability

safety controls in managing firm cyber risk behavior. Section VIII then gives lessons applicable to future emerging technologies, with Section IX providing conclusions.

II. Early Healthcare Cyber History

This section describes the early history of healthcare industry cybersecurity and cyber insurance including initial breaches, the promulgation of HIPAA, and other federal and state privacy and breach reporting regulations, and the concurrent development of early forms of healthcare cyber insurance.

Recognition of cyber-attacks against healthcare-sector targets began in the late-1980s with the widening use of personal computers and the Internet by medical researchers and other healthcare professionals. Many of the early attacks were untargeted, affecting a broad range of organizations that had early connections to the Internet. Possibly the most famous of these was the "Morris Worm" - a self-replicating and self-propagating malware that in 1989 infected 6,000 computers, roughly 10% of all Internet connections at that time. Its victims included hospitals, and medical research facilities, causing an estimated $10 million in damage (Sack 2018).

The following year, the first documented ransomware attack targeted the healthcare industry. In 1989, Dr. Joseph Popp, a biologist actively involved in AIDS research, distributed 20,000 floppy disks to fellow researchers in 90 countries saying the disks contained a computer-based application that gauges a person's risk of contracting AIDS. When researchers ran the installation program, a hidden file was installed onto their PC which, after a specific number of reboots, encrypted the hard disk, and displayed a message demanding that the user pay the license fee of $189 in exchange for the

decryption key (Lee 2018). While the ransomware was rudimentary, it created the basis for more sophisticated attacks targeting healthcare in the future.

A. HIPAA & Other Early Cybersecurity Regulations

This section provides details on the origins of HIPAA and other state regulations, and the role they play in mandatory breach reporting. This case study later uses data from these breach reports to analyze patterns of cyber-attacks against various healthcare sector entities.

During the 1990s, the public use of computers and the Internet grew rapidly. Among many industries, the healthcare-sector wanted to modernize and use information technology to improve efficiencies and reduce costs. This included the use of large databases and electronic records to collect, store and disseminate patient information for a variety of uses including filing claims, billing patients, and coordinating care. These capabilities benefited both patients and providers by improving the management of care and reducing costs. However, this technology also enabled the theft of personal health information (PHI) such as name, address, Social Security number, diagnosis, and date of birth—often used to commit identity theft and Medicare fraud.

While federal statutes such as the ***Privacy Act of 1974*** protected the disclosure of confidential medical records under federally funded programs—such as Medicare and Veterans Affairs – no federal privacy laws covering private sector activities existed. The absence of federal privacy protections allowed private healthcare firms to sell, transfer or use PHI for commercial advantage or financial gain and also potentially enabled employers, schools and other entities to gain access to this confidential information. To

rectify this situation, Congress in 1996 enacted the ***Health Insurance Portability and Accountability Act*** (Pub.L. 104–191). Under Section 263, Congress directed the DHHS Secretary to drive the adoption of healthcare information security standards including administrative, physical and technical safeguards. This was to "ensure the integrity and confidentiality of the information," and "protect against any reasonably anticipated – (i) threats or hazards to the security or integrity of the information; and (ii) unauthorized uses or disclosures of the information" (HIPAA Sec. 263(2)(A&B)). Eventually, DHHS released the final Privacy and Security Rules respectively in 2002 and 2003.

The U.S. Congress was not the only domestic legislative body interested in privacy breaches. In April 2002, hackers broke into a California state database and accessed the names, Social Security numbers, and payroll information for 265,000 state employees. Within a few months, the California legislature passed the ***Database Breach Notification Security Act*** (CA Senate Bill 1386) requiring state government agencies and any firms that do business in California to promptly notify California residents when they have a reasonable belief that a system breach has occurred exposing their personal information to third parties. The Act went into effect on July 1, 2003, and was the first state data breach law in the country. Today, all 50 states, the District of Columbia, Puerto Rico and other US territories have enacted data breach legislation, with many posting results to public websites (NCSL 2021).

In March 2006, OCR began to enforce HIPAA privacy regulations with fines ranging up to $25,000 (VanderLaan 2010). However, under HIPAA, firms accused of non-compliance could easily avoid sanction. Recognizing this problem, Congress in 2009

enacted the ***HITECH Act*** that amended HIPAA, widening the scope of privacy and security protections available; increasing the potential legal liability for non-compliance; and providing for more enforcement.

B. Early Healthcare Cyber Insurance

A previously discussed in the literature review (p.24), cyber insurance first appeared in the late-1990s soon after the enactment of HIPAA. However, the growth in demand from healthcare and other sector entities was likely driven more by events than fear of regulatory reprisal.

On May 4, 2000, a new computer virus called the Love Bug began to disabled computer networks around the world, ultimately infecting an estimated 10% of global Internet-connected computers. At the time it was the fastest spreading and the most expensive computer attack in history, aptly described as "the first global computer pandemic" (Winder 2020). Lloyds of London estimated its cost at over $15 billion in damages and lost productivity (US House May 2000). Like other industries, the healthcare-sector was not immune from the Love Bug's effects. The virus infected the email system of the Mayo Clinic, taking the system down for 30,000 employees nationwide for about six hours (Tieman 2000). It also affected email systems at all 150 medical centers operated by Veterans Affairs. Most of the systems recovered in less than 24 hours and, generally, little data was lost and patient care was unaffected (Tieman 2000).

Following the Love Bug cyber-attack, demand for cyber insurance exploded, and it became the hottest product in the insurance industry (Banham 2000). By the end of 2000,

at least ten major carriers were offering first- and third-party cyber coverage including AIG, Chubb, Hiscox, Lloyds of London, Marsh, and Zurich, with coverage limits up to $25 million (Rossi 2000). The Insurance Information Institute (III) estimated that the market for cyber insurance would grow from about $75 million in 2001 to $2.5 billion by 2005 (Baer 2003, 194). Some cyber insurers, wanting to differentiate their offering from competitors, began to tailor their coverage to specific sectors. For example, AIG in 2003 began targeting its NetAdvantage products to the healthcare-sector. It included providing free security scans for healthcare-specific vulnerabilities, and assistance in demonstrating HIPAA compliance (AIG 2003).

Initially, premiums were extremely high with costs in the early-2000s ranging from $45,000 to $60,000 per million dollars in coverage. Later that year, as more insurers entered the market, costs decreased to about $15,000 to $25,000 per million dollars in coverage, still a very steep price for small to medium sized companies. Often, as a precondition of coverage, early cyber insurers made applicants undergo a rigorous security assessment by a third-party technology security firm. The assessment was time consuming, invasive, and very expensive, with the entire cost borne by the applicant (Banham 2000). Over time, most insurers phased out the onsite risk assessment, simplifying their underwriting process for all but their largest clients (Majuca et al. 2006). While this decreased the cost of coverage, it also arguably increased the insurer's loss exposure and lowered the overall cyber safety benefit to clients. Further, cyber insurance premiums remained too expensive for most small companies.

Thus, despite high expectations, the cyber insurance market stagnated throughout most of the period between 2000 and 2010. In 2008, the estimated cyber insurance market was only $450 to $500 million (Betterley 2009) – less than a fifth of the market projection for 2005. Only 34% of companies had some form of cyber insurance, with growth the previous three years being flat or actually decreasing (CSI/FBI 2008). There were many reasons given for the failure of the market to grow as expected. The most commonly cited reason was that insurers' lack of experience and actuarial data led them to overprice the product (DHS 2014). However, some scholars have speculated that the problem was on the demand side and client fears of disclosing cyber breaches to a third party (Bandyopadhyay et al. 2009). While insurance would cover primary losses, it would likely not cover secondary losses such as loss of reputation or damage to a firm's brand that could be much more devastating. Without mandatory breach disclosure, many firms preferred to keep quiet and forego insurance that might require them to disclose the breach as part of the claims process.

III. Political Economy of Healthcare Cybersecurity & Healthcare Cyber Insurance

This section discusses the political economy of healthcare cybersecurity and cyber insurance including an overview of the healthcare industry ecosystem and both the benefits of healthcare technology adoption and costs associated with healthcare cybersecurity and cyber breaches. Its purpose, used in later analysis, is to identify the primary healthcare-sector cyber-attack targets, their special attributes that make them vulnerable to attack, and the measures of the magnitude of healthcare cyber-attacks based on both direct and indirect costs.

A. Five Ps of the Healthcare Cybersecurity Ecosystem (Targets)

The healthcare-sector in the United States is vast, employing 20.5 million workers at an estimated 784,626 U.S. firms – roughly 15.9% of the total U.S. workforce, and 10.9 % of total U.S. private sector firms in 2017 (Census,gov 2017). However, the domain of this analysis is much broader than the sector itself, encompassing the five Ps of the healthcare cybersecurity ecosystem: 1) Providers, 2) Partners, 3) Payers, 4) Pharmaceutical firms, and 5) People/Patients.

Providers are a broad category ranging from very large health systems that include one or more hospitals and thousands of employees, to individual practices that often have staffs of less than ten people. In between are private health insurers, individual hospitals, nursing homes, ambulatory and larger group practices. Each has widely varying IT use and its own unique set of cybersecurity strengths and weaknesses. These are based on such factors as the number of employees, the services they provide, the sensitivity of the PHI they collect, their billing processes, the types and connectivity of medical equipment used, the size of their technology budget, and their ability to train staff on cyber safety.

The second "P" of the healthcare cybersecurity ecosystem are "Partners," usually referred to in the HIPAA regulations as "business associates" (45 CFR § 160.103). Per DHHS, a "business associate" (BA) is a person or entity, other than a member of the workforce of a provider or other covered entity, which performs functions or activities on behalf of, or provides certain services to, a covered entity that involves access by the BA to PHI. Examples of BAs include claims processors, accounting services, lawyers, medical transcriptionists, and pharmacy benefits managers (DHHS 2003). The HIPAA

Privacy Rule allows covered providers and health plans to disclose PHI to a BA if they obtain satisfactory assurances that the BA will implement appropriate HIPAA security controls to prevent unauthorized use or disclosure of the PHI, including conducting regular risk assessments. Despite these safeguards, BAs remain a major risk to healthcare providers who depend on them for support and other services. Nearly half of the Top 25 breaches recorded on the OCR Breach Portal since 2009 involve BAs (OCR 2021).

The third "P", or "Payers," includes both private and public insurance organizations that reimburse providers, pharmacies, and other organizations for healthcare services. Private insurance organizations include health maintenance organizations (HMOs), preferred provider organizations (PPOs), drug benefit companies, and dental insurers. First among these groups are the "Big Five" managed care organizations: UnitedHealth, Anthem, Aetna, Humana, and Cigna Corporation. Public insurance is dominated by Medicare, administered by the Centers for Medicare & Medicaid Services (CMS), and Medicaid, which is administered by 50 state Medicaid agencies, under the supervision of CMS. What make payers particularly susceptible to cyber-attack are the vast amounts of PHI and financial information they collect and store. Nearly all healthcare firms in the U.S. connect to all of these systems in order to file claims and get paid – making these systems aggregation hubs for possible massive breaches. Not surprisingly, some of the largest healthcare breaches in U.S. history have struck private health insurers. In 2015 three of the Top 5 all-time healthcare breaches occurred at Anthem Inc. (#1), Premera Bluecross (#3), and Excellus BlueCross BlueShield (#5), combined exposing the records of nearly 100 million individuals (OCR 2021). Public payers are also not immune to

cyber-attacks. Nationwide, state Medicaid programs suffered many breaches over the period 2009 to the present. Hackers also victimized CMS who is responsible for Healthcare.gov - marketplace of the Affordable Care Act. On at least two occasions, hackers attacked the website, including a 2018 breach that accessed the files of 93,600 people and forced CMS to shutdown enrollment for a week (Sweeney 2018). Curiously, this breach does not show up on OCR's Breach Portal.

The fourth "P", or "pharmaceutical companies" and other healthcare suppliers - a broad category that encompasses those companies that develop, produce, and distribute drugs, as well as other supplies and equipment used by healthcare providers in the treatment of patients. Unlike healthcare providers and BAs, their activities are primarily regulated by the Food & Drug Administration (FDA) that can fine firms for violations of their safety guidelines. Pharmaceutical companies include biotech firms engaged primarily in research and development to create new drugs, devices, and treatment methods, as well as mainstream companies like Merck and Pfizer, that tend to focus more on manufacturing and marketing an existing portfolio of prescription and over-the-counter drugs. There are also companies that focus primarily on the retail distribution and sale of drugs and other supplies like CVS and Walgreens. Other healthcare suppliers are firms that develop, manufacture, distribute, and support medical devices, equipment and supplies for hospitals and other providers. Firms in this category include Medtronics and Siemens. These firms can also overlap into the pharmaceutical subcategory, like Johnson & Johnson selling both drugs and supplies. Because many of these companies are

involved in scientific research, cyber thieves are often looking to steal their most valuable asset – their intellectual property.

Medical devices connected to the Internet are also susceptible to cyber-attack. The FDA has released numerous safety warnings identifying vulnerabilities in a variety of medical devices (FDA 2020). Pharmaceutical and supply companies are also not immune to more general untargeted malware and ransomware attacks. On June 27, 2017 Merck, had its systems infected with NotPetya ransomware. The attack affected more than 30,000 company laptop computers and crippled Merck's vaccine production facilities for two weeks (Voreacos et al, 2019). Thus, this subsector is vulnerable to a wide range of targeted and untargeted cyber-attacks that not only can expose patient PHI, but also can allow the theft of intellectual property, the disruption of drug production, or even the manipulation of patient data that could result in the loss of life.

People, including patients and healthcare workers are the final "P" of the healthcare ecosystem. Cybersecurity research over the past ten years has consistently shown that human factors are the weakest link in the protection of health data (Spitzner 2021). People make mistakes and often unwittingly reveal their personal information, credit card numbers or logon credentials. Social engineering, phishing and business email compromises -- all of these attacks rely on people falling victim to manipulation. Further exacerbating this problem is the general lack of awareness about cyber risks by both healthcare workers and patients alike. One of the most challenging cybersecurity aspects of the healthcare workplace is the large number of employees from different departments or firms that have easy access to patient medical records. Usually, employees in this

records chain have full access to patients' medical data. This extended access increases the risk of record exposures that are most commonly due to human error. Unintentional exposure can occur if an employee falls for a phishing scam, voluntarily providing PHI, opening a file or clicking on a link that infects their computer or their firm's network with ransomware or other types of malware. Employees can also deliberately expose or maliciously steal patient data. In fact, up until 2018, a majority of all healthcare cyber incidents (58%) involve inside actors – making it the only industry with this unique distinction (Verizon 2018, p.7). The motive for employees to steal PHI is usually financial, providing them with a convenient means to commit identity theft or medical fraud. Under HIPAA, such activities are breaches subject to civil or criminal prosecution.

Patients can experience financial, mental, and even physical harm from a privacy breach or other cyber-attack that disrupts normal healthcare operations. Cyber disruptions of healthcare operations can also have a negative impact on patient safety. The WannaCry ransomware attack in 2017 disrupted the normal operations of more than 80 hospitals in the United Kingdom for four days, causing the cancellation of thousands of scheduled surgeries. One generalized solution for this problem is to make both patients and employees more aware of the cyber risks to PHI. Both patients and employees need to be educated on basic "cyber hygiene" including using strong passwords and being aware of phishing scams. Healthcare employers need to educate their employees on their roles and responsibilities in protecting patient privacy and preventing cyberattacks. This includes enforcing policies and establishing a risk culture where cybersecurity becomes

an integral part of patient care. The challenge is balancing the benefits of healthcare connectivity with the cost of investing in cybersecurity, rather than in direct patient care.

B. Benefits of Healthcare Information Technology & Cybersecurity

During the early-2000s, many U.S. industries were rapidly adopting computerization and the use of the Internet to provide easy access to data, reduce costs, and improve operational efficiencies. Yet, despite this revolution in other industries, the healthcare technologically lagged significantly behind. Healthcare continued to be a mostly paper-based industry, with doctors still writing prescriptions by hand, patient charts and records being stored in long lines of paper folders, and claims filed and bills sent in envelopes via the U.S. Post Office.

When Congress passed the HITECH Act in 2009, the goal was to encourage the healthcare-sector to follow other industries by implementing computer information technology that would increase accessibility to mission-critical data, automate labor-intensive and inefficient processes, and minimize human error. Most important, was Congress' desire to have providers adopt Electronic Health Record (EHR) systems and utilize them in a "meaningful" way. The concept of meaningful use rested on five pillars of health outcomes policy priorities: 1) improving quality, safety, efficiency, and reducing health disparities; 2) engaging patients and families in their health; 3) improving care coordination; 4) improving population and public health, and 5) ensuring adequate privacy and security protection for PHI (RegisteredNursing.org 2021).

Arguably, the most important capability of EHR is Health Information Exchange (HIE) – the ability of healthcare providers and other healthcare entities to electronically

share records and coordinate care with each other, as well as give patients easier access to their health information. Electronic sharing of health information is particularly important and challenging because the healthcare system is highly fragmented. Patients receive care and healthcare services from multiple entities in a variety of settings, and therefore typically have data collected and stored in a variety of locations. HIE can facilitate the sharing of information via EHRs, which can result in much more cost-effective and better quality care. HIE can also make the healthcare system more efficient by reducing the number of costly redundant diagnostic tests.

Patients also benefit from HIE. HIE allows patients to securely find and use vital health information, enhancing care delivery, and empowering them to make informed decisions regarding their health. New HIE communications capabilities, such as educational videos and text reminders, give patients options through which they can receive health information and become more engaged in their care. This has been especially important during the COVID-19 pandemic when people have been restricted in their ability to visit their doctor in-person or directly receive care from other healthcare entities. Innovations in telemedicine now make it possible for patients to access mental health therapy, family planning, or other types of care from a healthcare professional whenever they need it from the safety and convenience of their homes.

However, despite the incentives offered by the HITECH Act, the adoption of EHR was slower than expected, hampered by several issues. First, implementation of EHR could seriously disrupt healthcare workflows, resulting in mistakes and delays that diminished rather than improved the quality of care. Many physicians and staff were

resistant to altering their accustomed procedures, bulking at changes they saw as of minimal benefit to either their patients or their practices (Buntin et al. 2011).However, the cost of implementation remained the primary impediment to adoption, especially among small practices (Goldzweig et al. 2009). These costs included not only high upfront acquisition costs, but also ongoing costs for annual software licenses, training, support and maintenance. There was also the inevitable cost of lost productivity that accompanied initial startup. By 2015 when "certified EHR," meeting the criteria for Meaningful Use was required under HITECH, the adoption rate was over 95% for hospitals, but less than 78% for office-based physicians (HealthIT.gov 2017). The need for privacy and cybersecurity safeguards added an additional layer of cost and complexity that was particularly burdensome to small healthcare entities. Overtime, even these firms were able to build business cases that allowed them to implement certified EHR and needed cybersecurity. Funding for this came from both operational savings and new fees from insurers that rewarded investments in efficiency and safety, including actions that reduced the total cost of care.

C. Costs of Healthcare Cyber Breaches & Investment

Evidence suggests that healthcare is one of the most targeted and least prepared industries in the U.S. when it comes to cyber-attacks. Data from the Verizon Data Breach Investigation Reports from 2017 to 2020 showed that healthcare was either the first or the second most breached sector each year (Figure 6.1). Healthcare stands in the lower third of industries in the deployment of cybersecurity (Ponemon/IBM 2020), and spends only about 4 to 7% of IT budgets on cybersecurity, compared to about 15% by other sectors

(Morse 2019). In 2020, healthcare had the highest average time to identify and contain a breach at 329 days (Ponemon/IBM 2020), and consistently had the highest total cost per breach compared to every other sector (see Figure 6.2).

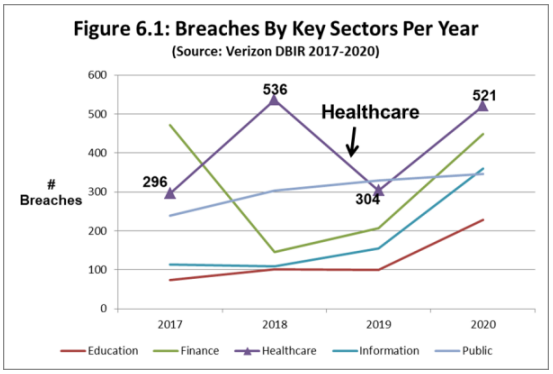


Figure 6.1: Breaches by Key Sectors Per year

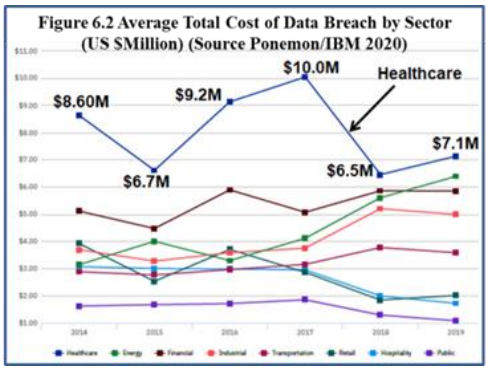


Figure 6.2: Average Total Cost of Breach by Sector

Healthcare has the highest total cost for a data breach for several reasons. First, because of healthcare is a highly regulated sector, government investigations following an incident can be time consuming, expensive to defend, and sometimes results in hefty fines for HIPAA violations. Second, because of the lengthy average time for many healthcare-sector companies to identify and contain a breach, cyber criminals can often extract large amounts of PHI before their activities are shutdown. Finally, because medical data often contains special information including policy numbers, diagnosis codes, and billing instructions, it is especially valuable to sell on the black market, sometimes selling for 10 or 20 times the value of credit card numbers (Contos 2016). HIPAA/HITECH makes it compulsory for healthcare companies to provide affected patients with written breach notification, and many breached healthcare firms also

provide credit and identity theft monitoring. As a result, the average cost per breach record is also much higher than for any other sector, reaching $429 per record in 2020.

Not surprisingly, because of the healthcare-sector's high cyber insurance take up rate, it annually files more claims and had more claims payouts than any other industry. For example, NetDiligence, a provider of cyber risk services to the insurance industry, has collected claims data from sixteen cyber insurance clients over the period 2015 to 2019 (NetDiligence 2020). Those clients provided 3,399 claims from firms they insured in 18 different industrial sectors. Of those claims, 893 were from the healthcare-sector firms representing 26.3% of the total – more than triple every other sector except for Professional Services.

NetDiligence also provides sector details on the average and range of losses claimed by size of company. Ninety-eight percent (98%) of claims in their database are for small- and medium-sized enterprises (SMEs) classified as having less than $2 billion in annual revenue. In reality, most healthcare firms are small practices and suppliers with annual revenue of less than $50 million. Of the 893 healthcare-sector claims, 880 were from SMEs with claims ranging from $10,000 to $7.1 million, and an average claim amount of $82,000 (NetDiligence 2020, p. 25). Claimed losses are before self-insured retentions (SIRs), including deductibles and copays that averaged $40,000 for SMEs, and $2.2 million for large companies, meaning that there was likely a large margin between claimed losses and actual insurance payouts. NetDiligence also provides by sector the average costs of crisis services including forensics, breach notification, credit monitoring, public relations and data restoration. What is interesting is for healthcare SMEs, the

average cost for breach notification and credit monitoring is higher than any other sector, once again confirming the high per record cost of healthcare PHI breaches.

A subset of the NetDiligence data provides some per sector costs for ransomware claims including averages for ransom amounts, costs for crisis services, and total incident cost. The total number of ransomware claims was 920 representing 27% of all claims for the period 2015 to 2019. SMEs filed all but four of the claims, with the vast bulk of these being from very small firms (NetDiligence 2020, p. 44). Every sector experienced at least one ransomware attack, with a severe uptick in incidents beginning in 2018. Once again, the healthcare-sector had more ransomware claims than any other sector. Recent data from cyber insurer Coalition shows that ransomware has risen to become the top type of cyber-attack against healthcare firms, encompassing 47% of all reported incidents (Ayers 2020).

There are also other indirect or "hidden" costs to healthcare firms resulting from a cyber-attack including the loss of reputation, theft of intellectual property, lowered credit rating and, in the case of publically traded healthcare companies, declining stock price. The effects of a PHI breach can be devastating to a healthcare practice, resulting in a loss of future patients and associated revenue. Some healthcare practices have gone bankrupt and shutdown operations altogether. For example, a medical clinic in California shut its doors after a ransomware attack (Townsend 2019). Moody's Investors Service uses cybersecurity threats and disruption as a key factor affecting hospital credit ratings (CPrime 2020), and publicity surrounding breaches have been shown to adversely affect stock prices, with the stock price in publicly traded healthcare firms falling an average of

0.7% following a cyber incident (CGI 2017, p. 11). On top of all this is the possibility that a cyber-attack could cause first- or third-party bodily injury or death.

Given the high direct and indirect costs of a cyber breach to healthcare-sector firms, it is predicted that the global healthcare cybersecurity market will grow by 15 percent year-over-year over the next five years, and reach $125 billion cumulatively by 2025 (Morgan 2020). However, given the rapidly expanding landscape of healthcare cybersecurity vulnerabilities, and the unique nature of healthcare cyber threats, it is likely that healthcare-sector companies will need more than new technology to deal with evolving cybersecurity risks.

IV. Healthcare Cybersecurity Vulnerabilities, Threats & Risks

This section looks at the unique healthcare-sector vulnerabilities, threats and risks that make it especially susceptible to cyber-attacks. It is meant to build on the Chapter 2 Section II literature review discussing the general components of cyber risk that impact all sectors, outlining the similarities and differences that will allow empirical comparisons in later sections

A. Healthcare Cybersecurity Vulnerabilities

The most unique aspect of the healthcare-sector and the core of its cyber vulnerability is the essential role it plays in the happiness and well-being of peoples' lives. A cyber-attack against the healthcare entity can not only expose confidential information, it can also delay care, cause misdiagnoses, result in unnecessary pain and suffering, or even lead to bodily injury or death. For this reason, healthcare privacy and security is more highly regulated than any other industry. Mandatory breach reporting

makes healthcare cyber-attacks more publicly visible. Further, when cyber-attacks do occur, they often get more media attention versus breaches in other sectors. Without mandatory breach reporting, firms in other sectors try to avoid public disclosure that might harm their reputation and brand. Thus, the statistical data showing the healthcare-sector as more targeted than other sectors is likely biased due to its unique level of transparency.

The healthcare-sector is also very large and highly segmented, with many small providers and suppliers constantly interacting with each other and with a few large healthcare organizations. This structure has resulted in the creation of many highly fragmented IT networks that increase the chances of a breach. While other industries such as retail sales and financial services have similar size and degree of segmentation, none arguably has the high degree of collaboration and interconnection that exists among multiple healthcare entities. This high degree of interconnection means a weak spot in the network security of one entity can be a door for hackers to infiltrate the networks of others. Conversely, it also means when one healthcare provider invests in anti-virus software, firewalls, and staff cybersecurity training, there is an enhanced spillover effect that benefits the cybersecurity of many other healthcare entities.

The collaboration and interconnectivity among healthcare entities also results in the collection, sharing and storage of large amounts of patient records in various locations, with unrestricted access for most employees. Further, to comply with legal requirements, healthcare organizations often store medical information for many years. Extended access to medical records increases the potential for privacy breaches, and the probability and

consequences of a breach increase directly with the volume and duration of storage. To deal with this data storage issue, many healthcare entities are moving their data to the cloud. While in theory the cloud is a more secure environment, the concentration of PHI has made such sites alluring targets for hackers, and cloud security is only as good as the strength of user passwords.

Weak user passwords are only the tip of the iceberg when it comes to healthcare's biggest vulnerability - healthcare workers. As will be discussed in the next section, healthcare is the only industrial sector that up until 2019 had more internal actors behind breaches than external (Verizon 2017-2019). Healthcare workers are the preeminent vulnerability to their employers primarily due to their non-malicious but negligent behavior. They sometimes lose, have stolen or improperly dispose of physical media such as paper files, laptops or thumb drives that contain large amounts of PHI. Healthcare workers are busy, and often leave their computers logged on and unattended.to, allowing unauthorized people easy access to patient files. Busy healthcare workers also often fall prey to social engineering, typically phishing attacks, delivered by email

In 2017, the Health Care Industry Cybersecurity (HCIC) Task Force identified several additional vulnerabilities of concern. These include lack of resources; ubiquitous use of legacy equipment and outdated software; over-reliance on complex technologies without understanding the risks; the proliferation of software vulnerabilities in commonly used medical devices and applications; and potential future issues tied to the expanded us of telemedicine (HCIC 2017).

One way to deal with the healthcare worker vulnerability is through user training, and the hiring of trained information security staff to monitor employee activity and identify potential threats. With operating margins often below one percent, most healthcare organizations lack the financial resources to hire and retain in-house information security personnel, adequately train workers, and implement technology needed to address current and emerging cybersecurity threats (HCIC 2017, pp. 1-2). Oftentimes, understaffed organizations with limited technological resources may not know that they have experienced a breach until long after it has occurred.

Another vulnerability associated with limited financial resources relates to the way that healthcare organizations acquire and use medical technology. Such technology is typically very expensive. Oftentimes, to offset the cost, healthcare entities rush new equipment and software into service without adequate evaluation of cybersecurity risks or the allocation of required resources to ensure the technology's cyber safety. This technology can become entrenched in key healthcare functions, and not replaced when it becomes obsolete. Legacy technology often has unsupported operating systems, such as Windows XP, and no longer receives patches to fix vulnerabilities. This makes these devices particularly susceptible to malware attack. This was the case in 2017 when WannaCry ransomware infected more than 300,000 devices in 150 countries through file-sharing protocols in outdated Windows XP and Windows 8 operating systems.

Vulnerabilities are not limited to older legacy medical devices. All medical devices face a certain amount of cybersecurity risk. Medical devices connected to the Internet are particularly vulnerable. This includes bedside equipment, implantable devices, and

consumer IoT devices that measure heart rate and other vital signs. The more connectivity, the greater the risk posed. Often, the devices do not run anti-virus software, are difficult to patch, and still run factory-set passwords found in device documentation (Gallagher Healthcare Practice 2017)

Recent studies found that the average medical device has 6.2 vulnerabilities (Carlson 2019) and that 74% of endpoints on a hospital's network are connected medical devices that are typically invisible to network security (Sherman et al. 2020). In addition to data security and privacy impacts, patients could also be physically affected (i.e., illness, injury, death) by cybersecurity threats exploiting medical device vulnerabilities. Harm can come from the device itself, impeded hospital operations, or the inability to deliver care. Malware can alter patient data on a diagnostic device. Device software can be reprogrammed to change its functionality. Denial of service attacks can make the device unavailable (HCIC 2017, p. 18).

In addition to connected medical devices, other healthcare related technologies have vulnerabilities that make them susceptible to cyber-attack. For example, the Covid-19 pandemic has dramatically increased in the use of telemedicine. Beginning in March 2020, U.S. consumer telemedicine adoption skyrocketed from 11% in 2019 to 46%, with patients using telehealth to replace cancelled healthcare visits (Bestsennyy et al. 2021). This surge was fueled by a decision of DHHS to lift several restrictions on the use of communication apps – such as FaceTime, Zoom and Skype — for telemedicine (Jercich 2020). HIPAA rules require that providers integrate encryption and other safeguards into their interactions with patients – but many of these platforms left confidential and

medical information exposed to hackers. These vulnerabilities can allow hackers to Zoom Bomb calls or lurk in virtual meetings to steal patient PHI.

Hospitals and other healthcare facilities are also integrating IT connectivity into their building controls and plant operations, including facility security monitoring. In March 2021, hackers infiltrated security camera data from Verkada, giving them access to live feeds of 150,000 surveillance cameras in companies and several hospitals (Drees 2021). This breach also highlights the immense vulnerabilities that healthcare and all other industries share regarding suppliers of hardware, software, and services. In 2020, investigators discovered that hackers were exploiting vulnerability in the SolarWinds Orion Cybersecurity Platform used by 33,000 high-profile customers. The malware infected the systems of at least nine federal agencies including the National Institute of Health (Wilson 2020) and many other SolarWinds customers including the California Department of State Hospitals (Poulsen et al. 2020). As a result of this breach, OCR in December 2020 issued a warning to all healthcare organizations to be on the lookout for SolarWinds and other global supply-chain cyberattacks (Davis 2020). This came on the heels of an FBI warning in October 2020 that the US hospitals were facing "imminent" threat of ransomware attacks by cybercriminals and other malevolent actors (The Guardian 2020).

B. Healthcare Cybersecurity Threat Actors & Actions

This section examines the healthcare cyber threat landscape and how it has evolved, particularly over the period 2019 to 2021. It builds on the general overview of cybersecurity threats outlined in the literature review including compromises of

confidentiality, integrity, and availability (CIA) by various malicious actors, especially advanced persistent threats (APTs).

1. Healthcare-sector Advanced Persistent Threats (APTs)

The Threat Actor Encyclopedia defines an APT as "a stealthy cyberattack in which a person or group gains unauthorized access to a network and remains undetected for an extended period" (ThaiCERT 2021). Traditionally, the term has been associated with state-sponsored actors, however, over the last few years, non-state criminal organizations have been recognized as part of the APT club. In the United States, there are over 50 private sector cybersecurity companies gathering threat intelligence, and identifying and tracking threat adversaries as part of their business model. These companies, including FireEye/Mandiant, Crowdstrike, MITRE, Microsoft, Symantec, McAfee, Cisco/Talos, IBM and many others that use proprietary and open source techniques to identify threat actors though the process of attribution.

The attribution process involves collecting and analyzing both technical forensic indicators of compromise (IOCs), as well as operational intelligence data regarding the attacker's behavior. Technical forensic IOCs, typically collected through automated processes, attempt to analyze any metadata connected to the attack including IP addresses, URLs, file hashes and known malicious domain names. Operational intelligence involves human analysts looking at attacker behavior including sector and systems targeted, access methods, malware used, and even time of day when an attack typically occurs. This data helps provide contextual insights into who the adversaries are, what their motive is, and how they plan, conduct, and sustain cyber campaigns.

The attribution process is difficult and inherently limited. Attackers technically try to hide their identity by spoofing their IP address or using proxy servers to confuse forensic investigation. They can also change their behavior, subtly alter their malware, or even borrow tools or coordinate with other adversaries to try to throw investigators off their trail. Despite these attempts at concealment, cybersecurity companies along with government cybersecurity teams have identified and named over 300 distinct APTs (EternalLiberty 2021).

The tables below identified those APTs recognized as having targeted healthcare-sector companies in the past ten years. For each APT, the tables give the common name, the date when they first appeared, their base country (if known), and the TTPs they characteristically use. Based on this data, Google searches then identified healthcare attacks attributed to each APT.

2. State-Sponsored APTs

State-sponsored APTs (Table 6.1) usually have a political motive for their attacks. Most often, this is espionage with the goal of extracting trade secrets or other types of intellectual property. For example, Chinese APTs often target research centers, such as NIH by ***Hidden Lynx*** in 2013 (Higgins 2013), and pharmaceutical companies like Bayer by ***Winnti Group*** in 2019 (Weiss & Burger 2019) to get proprietary data on vaccine trials or new drug developments. Chinese APTs also look to gather information on US citizens. Such was the case in 2015 when ***Shell Crew*** carried out three of the biggest healthcare breaches of all time against Anthem, Premera Blue Cross, and CareFirst Blue Cross Blue Shield, resulting in the extraction of over 90 million patient records. One clue

that state-sponsored APTs carried out these hacks was that none of this valuable health data ever appeared for sale on the black market (Smith 2015, p. 52).

The motive for state-sponsored APT attacks can also be to cause disruption under the ruse of criminal financial gain. Such was the case in 2017 when North Korean APT ***Lazarus Group*** launched the WannaCry ransomware attack that disrupted the operation of the United Kingdom's National Health Service, and hospitals in over 150 countries around the world. The ransom requested was so small, and the encryption so easily undone that attention soon turned to North Korean nationals as the likely culprits. In addition, the malware used was similar to an attack on Sony Pictures by the North Korean APT in 2014 (Johnson 2017). Similarly, the NotPetya ransomware attack later in 2017 that crippled global drug maker Merck was eventually attributed to Russian APT ***Telebots***. Ironically, because the perpetrator was a nation-state, insurers dubbed the attack an "act of war" excluded from coverage (Lemos 2020).

Table 6.1: State Sponsored APTs (Sources: See In-Text References)

Common Name	Active Since	Country	Tools/TPPs	Mandient/ FireEye	CrowdStrike	MITRE ATT&CK	Prominent Healthcare Attacks	Year(s)
Comment Crew Unit 61398	2006	China	Spear Phishing Custom Backdoors	APT1	Comment Panda	G0006	141 Companies in 20 sectors including healthcare	2012
DarkHotel	2004	North Korea	Zero Day Vulnerability Spear Phishing	Fallout Team	Shadow Crane	G0012	World Health Organization	2020
Hidden Lynx	2009	China	BLACKCOFFEE Malware Zero Days, GhostRAT Hacking-For Hire	APT17	Aurora Panda	G0025	National Institute of Health (VOHO Campaign)	2013
Lazarus Group Covellite	2009	North Korea	WannaCry Ransomware Spear Phishing	Bureau 121	Labyrinth Chollima (Microsoft Zinc)	G0032	Astra-Zeneca/Oxford Vaccine UK National Health System CarePartners Hospice Bayer medical devices	2020 2017
menuPass	2009	China	Data exfiltration using RDP & TCP	APT10	Stone Panda	G0045	Bharat Biotech Serum Institute of India Covid-19 Vaccine Research	2020
Orangeworm	2015	North Korea	Kwampirs backdoor Social Engineering Adobe Flash	APT37	Ricochet Chollima	G0067	Abbott Cardiac Monitors X-Ray & MRI Machines	2018
Shell Crew	2011	China	Supply-chain attacks Strategic web (SWC) Phishing Watering Holes	APT19	Deep Panda	G0009	Anthem Premera Blue Cross Carefirst Blue Cross	2015
Sofacy	2004	Russia	SOURFACE downloader EVILTOSS Backdoor	APT28	Fancy Bear (Microsoft Stontium)	G0007	US Anti-Doping Agency COVID-19 Vaccine Research	2018 2020
Telebots	2009	Russia	NotPetya Ransomware	Sandworm Team	Voodoo Bear	G0034	Merck Heritage Valley Health Systems	2017
Wekby	2009	China	GhostRAT Zero Day Exploits	APT18	Dynamite Panda	G0026	Community Health Services	2014
Winnti Group	2012	China	Spear Phishing Custom Backdoors	APT41	Wicked Panda	G0044	Bayer Pharmaceutical Moderna	2019 2020
The Dukes YTTRIUM	2008	Russia	Phishing emails	APT29	Cozy Bear	G0016	COVID-19 Vaccine Research	2020
Zirconium	2020	China	Java & Adobe Flash Vulnerabilities	APT31	Judgement Panda	N/A	COVID-19 Vaccine Research	2020

3. *Organized Crime APTs*

Organized crime APTs (Table 6.2) nearly always have a financial motive for their attacks. For most of the "early" period of healthcare cyber breaches, criminals relied on the simple theft of computer equipment, storage devices, or paper records primarily by internal actors, to obtain PHI records. Thieves used this PHI for identity theft or sold them on the black market to the highest bidder. Beginning in 2015, the number of breaches by external criminals began to rise, attacking healthcare systems in a variety of ways. Initially, they employed "password spraying," brute force attacks with commonly used passwords, to see if they could gain access to a system. Later they developed social engineering techniques to get insiders to reveal logon credentials. A primary social engineering technique was the use of phishing emails to get a victim to click on a link to a URL hosting a hidden malware payload. Successful phishing emails look authentic, and the sender's identity is frequently spoofed so as to appear to be sent by a trusted individual or organization.

Cyber criminals also developed new types of malware to exploit a wide variety of devices and applications. Foremost among the threats to healthcare firms was the development and use of crypto malware or "ransomware" that can encrypt and prevent access to critical computer system files in order to extort money from a victim.

Over time, the black market value of PHI declined. By February 2019, cybersecurity firm FireEye reported that hackers were selling 50,000 patient records stolen from a US-based health care institution for $500, or a penny a record (FireEye 2019, p. 4). By 2016, cyber criminals were beginning to change their business models. In February 2016,

organized crime APT ***Gold Lowell***, using SamSam ransomware, infected the computer systems of Hollywood Presbyterian Medical Center. Eventually, the medical center paid the attackers a ransom of $17,000 in exchange for the key to unlock their systems. ***Gold Lowell*** over the next two years used SamSam ransomware to attack at least five other healthcare firms including MedStar Health, and AllScripts, before two Iranian men were indicted in 2018 (DOJ 2018).

Between 2016 and 2019, ransomware attacks against healthcare entities increased 35 percent with cyber criminals targeting direct patient care facilities such as hospitals and health care centers (Team RiskIQ 2020, p. 3). Cyber criminals may have preferred these facilities because they were more likely to pay to prevent disruption to patient care. Since 2016, over 230 new strains of ransomware have been identified (NJCCIC 2021) along with the emergence of many new crime gangs often connected with a specific ransomware strain and characteristic TTPs.

Table 6.2: Organized Crime APTs (Sources: See In-Text References)

Common Name	Active Since	Tools/TPPs	Country	Mandient/ FireEye	CrowdStrike	MITRE ATT&CK	Prominent Healthcare Attacks	Year(s)
Ako (Ranzy) MedusaLocker Gang	2019	Windows Ransomware	N/A	N/A	N/A	N/A	North Shore Pain Management	2020
Avaddon Gang	2020	RaaS Data Leakage Extortion DDOS Attack	N/A	N/A	N/A	N/A	Capital Medical Center Bridgeway Senior Healthcare	2021
Babuk Locker Gang	2021	Babuk Ransomware Windows Restart	N/A	N/A	N/A	N/A	Cardiva Medical Devices	2021
Barrista	2014	Strategic Web Compromises (SWC)	China	APT22	Wicked Spider	G0120	Cancer Research Center	2018
Dharma Gang	2017	Dharma Ransomware RDP Abuse RaaS	N/A	N/A	N/A	N/A	Altus Bay Hospital	2018
DopplePaymer Gang	2019	DopplePaymer Ransomware	Russia	N/A	Dopple Spider	N/A	University Hospital Düsseldorf (woman's death)	2020
Egregor Gang	2020	Egregor Ransomeware RaaS Data Leakage Extortion DDOS Attack	Eastern Europe or Russia	N/A	Twisted Spider	N/A	GBMC HealthCare Dax-Côte d'Argent Hospital (France)	2020
EKANS/Snake Gang	2019	EKANS/Snake Ransomware SCADA/ICS devices	N/A	N/A	N/A	N/A	Fresenius (European Hospital)	2020
FIN 11 (CLOP Gang)	2016	CL0P Ransomware Double Extortion Spray-and-Pay	N/A	FIN11	N/A	N/A	Nova Biomedical	2020
FIN4	2013	Capturing credentials to access email	Romania or USA	FIN4	Wolf Spider	G0085	Merck Allergen	2014
SamSam Gang Gold Lowell	2015	SamSam Ransomware	Iran	N/A	Boss Spider	N/A	Hollywood Presbyterian Kansas Heart Hospital LabCorp MedStar Health OrthoNebraska Hospital Allscripts	2016
Maze Cartel Lockbit Gang RagnarLocker Gang Suncrypt Gang Conti Gang	2015	Maze Ransomware Lockbit Ransomware RagnarLocker Ransomware Suncrypt Ransomware Conti Ransomware Windows-Based DDOS	N/A	FIN6	Skeleton Spider Viking Spider	G0037	New Jersey's Medical Diagnostics Laboratories Stockdale Radiology University Hospital New Jersey Leon Medical Centers Nocono General Hospital Rehoboth McKinley Christian	2020 2021
Mespinoza (Pysa) Gang	2019	Mespinoza (Pysa) Ransomware	N/A	N/A	N/A	N/A	Assured Imaging Nonin Medical	2020
Mount Locker Gang	2020	Ransomware-as-a-Service (RaaS) Data Leakage Extortion	N/A	N/A	N/A	N/A	Sonoma Valley Hospital	2020
NetfilimGang	2020	Netfilim Ransomware	N/A	N/A	N/A	N/A	Fresenius (European Hospital)	2020
NetWalker Gang	2019	Netwalker Ransomware Human Operated RaaS	N/A	N/A	Circus Spider	N/A	University of California San Fransisco School of Medicine Wilmington Surgical Associates Crozer-Keystone Health System	2020
RANSOMEXX (DEFRAY777)	2020	Defray777 Ransomware Linux Systems Virtual machine SW	N/A	N/A	Sprite Spider	N/A	Mutuelle Nationale des Hospitaliers (France)	2021
REvil (Sodinokibi) Gang	2019	GandCrab Sodinokibi/REvil ransomware-as-a service & data leaking	Russia	N/A	Pinchy Spider	G0115	CTS (Dental IT Service) 10X Genomics	2019 & 2020
Evil Corp TAT505	2006	BitPaymer ransomware WastedLocker Phoenix CryptoLocker Ransomwares Phishing RDP compromise Big Game Hunting	Russia	TEMP.Warlock	Indrik Spider Graceful Spider	G0092	UK National Health Services CNA Insurance	2017 2021
TA542	2014	Emotet Malware RSA key exchange	Eastern Europe	N/A	Mummy Spider	N/A	Lithuanian National Public Health Center	2020
TEMP.MixMaster Ryuk Gang Tricknot Gang	2017	TrickBot, Ryuk Ransomware	Eastern Europe	UNC1878	Wizard Spider Grim Spider	G0102	Universal Health Systems St. Lawrence Health Systems Sky Lakes Medical Center University of Vermont Health	2020

In April 2017, the ***Dharma Gang*** used its unique variant of ransomware to attack Texas-based ABCD Pediatrics, the first of many healthcare-sector victims. In September 2018, Dharma struck again attacking Texas-based Altus Baytown Hospital and now

manually installing their ransomware using RDP. In this case, Altus was able to recover it files using data backups. By this time, other ransomware gangs were using "hands-on-keyboard" manual techniques to conduct targeted ransomware attacks against healthcare entities.

In August 2017, the first recorded hands-on installation of BitPaymer ransomware was conducted by ***Evil Corp*** against several UK National Health Service hospitals. Evil Corp demanded a high ransom of 53 bit coins (approximately $200,000). Due to the targeted nature of BitPaymer attacks, the ransomware is custom-built for each operation (Frankoff and Hartley 2018). These new tactics of selectively targeting large organizations for high ransomware payouts with customized malware shifted the business model for ransomware gangs, with a new focus on what became known as "Big Game Hunting." Ransomware gangs began to organize their criminal enterprises, sharing tools and specializing in certain eCrime services. Specialty eCrime firms became access brokers, selling stolen credentials, exploit kits, and phishing services on criminal forums. Gangs such as ***REvil*** and ***Egregor*** developed Ransomware-as-a-Service (RaaS) offerings, and new techniques such as double extortion where a victim's data is stolen before being encrypted, and leaked to a dedicated leak site (DLS) unless a second ransom is paid. Double extortion and the use of DLS were adopted by at least 23 ransomware operators in 2020 (CrowdStrike 2021, p. 19).

These new techniques allowed ransomware gangs to pursue even bigger game, including cloud service providers. In May 2020, Blackbaud, a cloud service provider to nonprofits, experienced a ransomware attack by an unidentified criminal group. Among

the victims were more than six dozen US healthcare providers who had over 8 million records exposed, making it the largest healthcare data breach of 2020 (HIPAA Journal 2021). This breach was the worst in a horrible year of unprecedented healthcare cyberattacks linked to the COVID-19 pandemic.

4. *COVID-19 Pandemic and Healthcare Cyberattacks*

The COVID-19 Pandemic provided both state-sponsored and organized crime APTs a unique opportunity to conduct targeted cyberattacks against healthcare providers, pharmaceutical companies, vaccine storage and transport facilities, and anxious members of the public.

The global competition to develop and distribute vaccines triggered a wave of state-sponsored cyberattacks targeting COVID researchers. Earlier on in the pandemic, WHO was targeted by ***DarkHotel***, a North Korean APT who may have been looking for information on vaccine tests or trial cures (Seals 2020). Then, in July 2020, the U.S., U.K. and Canadian governments issued a joint advisory stating that known Russian APT "***the Dukes***" targeted several organizations in all three countries that were working on COVID-19 vaccine development (NCSC 2020). Later in the year, Moderna, along with both Pfizer and BioNTech had vaccine data stolen from the server of the European Medicines Agency (EMA) - the drug regulator for the European Union (Liu 2020). Later, hackers leaked the data to the Internet, changing it prior to posting in a way that could undermine trust (Cerulus 2021).

Both state-sponsored and criminal APTs are using fear about the pandemic and curiosity about vaccine availability as a lure in targeted spear-phishing attacks. Beginning

in April 2020, North Korean APT ***Lazarus Group*** began distributing COVID-19-themed phishing emails. They also established phishing domains that appear to be COVID-19 research companies in the US, UK, and South Korea (CrowdStrike 2021). In November 2020, the North Korean APT tried to break into the systems of AstraZeneca through a phishing campaign targeted at the British drug maker's employees. The hackers posed as recruiters approaching AstraZeneca staff with fake job descriptions laced with malicious code (Stubbs 2020). In another spear-phishing campaign, hackers targeted the vital "cold chain" that protects coronavirus vaccines during storage and transport. The phishing emails looked like a request sent on behalf of Gavi, a public-private alliance that supplies vaccines to poor countries (Ikeda 2020).

Cyber criminals are also using COVID-19 phishing emails to try to exploit hospital employees and patients during the COVID-19 pandemic. Pandemic-related themes exploited people looking for information on COVID testing and treatment, lured people with scams offering personal protective equipment, and provided fake pandemic advice from hackers pretending to represent the CDC. Phone systems were hacked sending fake voicemail "vishing" messages to remote workers in an attempt to get logon credentials (HIPAA Journal 2020).

Among the most prolific and profitable uses of COVID phishing emails by cyber criminals was in delivering ransomware to busy and often overwhelmed healthcare providers. In 2020, there were an estimated 15,701 attempted ransomware attacks against healthcare-sector companies (TrendMicro 2021). Organized crime APTs **Maze** and ***REvil*** gangs were particularly active in targeting healthcare during the early days of the

pandemic. In March, the REvil gang hit biotech research firm 10x Genomics with a ransomware attack. The firm is part of an international alliance sequencing cells from patients who recovered from the COVID-19. 10x Genomics was able to restore normal business operations without significant impact, but REvil ended up posting some of data it stole from the company (Davis April 2020).

As COVID-19 hospitalizations soared during the second half of 2020, there were more ransomware attacks in healthcare than any other industry (Davis October 2020). Ransomware gangs adjusted their business models, betting that healthcare organizations would swiftly pay ransoms to restore lifesaving operations (Evans and McMillan 2021). In June 2020, the ***NetWalker Gang*** infected several servers at the University of California School of Medicine – a leading COVID-19 response group working on antibody testing and clinical trials. The School eventually paid ***NetWalke*****r** a ransom of $1.14 million – the largest healthcare ransom in 2020 – to unlock their systems (Davis June 2020). Another ransomware gang extremely active during the latter half of 2020 into 2021 was ***Conti***, a member of the ***Maze Cartel***, which used a spear phishing email to infect Leon Medical Centers, a network of 8 medical centers in Florida with ransomware and steal 2 million patient files. When the victim refused to pay the ransom, Conti published the data on a leak site, including the names of patients who had tested positive for COVID-19 (DataBreaches.net 2021).

Plausibly the most serious healthcare ransomware attack in 2020 was conducted by the ***Ryuk Gang***, which in September 2020 infected the computer network of Universal Health Services (UHS). The attack resulted in computer system failures in over 400

locations and cost the firm an estimated $67 million in pretax dollars, most of which they believed would be recovered from their insurance coverage (Reed 2021). The event triggered calls for an investigation by Senator Mark Warner (D-VA), (HIPAA Journal October 2020), and a class action lawsuit (Berger Montague 2021). Despite the magnitude of this cyberattack, no patient data was compromised, and thus UHS was not required to report the breach to OCR and have it posted on the OCR Breach Portal. This incident illustrates the high cost of healthcare breaches and the weakness of HIPAA and HITECH regulations in preventing such events.

C. Healthcare Cybersecurity Risks & Healthcare Cyberattack Database (HCAD)

Section II-D of the Chapter 2 Literature Review provides the risk equation:

Risks = Vulnerabilities x Threats x Likelihood x Impact or R = f(V, T, L, I)

This section will examine healthcare cybersecurity risk using the vulnerability and threat information from the previous two sections, and a newly created database of over 5600 healthcare cyberattack incidents covering the period 2005 to 2021. The ***Healthcare Cyberattack Database (HCAD)*** will be used to examine the frequency and impact of various types of cyber-attacks, by assorted threat actors, against different healthcare vulnerabilities. The goal is to identify key healthcare-sector cyber risk patterns, variances in losses, and clues as to what safety actions might help healthcare entities avoid attacks and mitigate losses.

1. The Healthcare Cyberattack Database (HCAD)

As of August 31, 2021, the Healthcare Cyberattack Database (HCAD) consists of 5,609 cyberattack incidents, affecting 392,370,978 PHI records that have occurred at

public and private healthcare entities located in all 50 U.S. states, the District of Columbia, and Puerto Rico.

The incident data was created from a number of sources. The primary source is OCR's Breach Portal (OBP) that records all breaches of unsecured (e.g. unencrypted) PHI affecting 500 or more individuals, reported to DHHS between 2009 and the present. The data consists of 4,171 breaches of which 821are "under investigation" and 3,350 are "closed and archived." The second major source is the Privacy Rights Clearinghouse (PRC), a database of over 9000 U.S. data breaches that occurred between 2005 and 2020, of which 4,581 are healthcare related. Unlike the OBP, PRC's data contains older events, as well as healthcare breaches affecting less than 500 individuals. This primary source data was supplemented and enhanced by healthcare incident data collected from media sources such as HealthcareInfoSecurity.com, DataBreaches.net and Becker's Health IT, as well as state breach reporting sites. There was considerable incident overlap among the sources, and data edited to eliminate duplicates. The same entity can often have incidents listed under different names (e.g., Boston Children's Hospital vs. Children's Hospital Boston). In addition to the name of the breached entity, the OBP data also contains the state where the entity is located, the number of individuals affected, the incident submission date, and basic information on the entity type and breach type. If it is a closed and archived, there also can be additional information and the actions taken. In addition to having incidents from multiple sources, what make the HCAD unique is that the four OBP entity types are divided into 27 subtypes (e.g., doctor, hospital, etc.). Breach types

have also been updated to include ransomware attacks, a category of hacking attacks not specifically identified in the OBP.

The HCAD data analysis below identifies the evolution and current day patterns of cyberattack risk experienced by the healthcare-sector over the period 2005 to the present. This data will later be used to consider how insurance influences healthcare cyber safety.

2. *Initial Analysis of HCAD Risk Patterns*

This section provides an initial analysis of HCAD data with a focus on the elements of cyber risk including identification of specific vulnerable healthcare-sector populations, the evolution of threats, the frequency of various types of cyber-attacks against different types of healthcare entities, and known impacts of these attacks in terms of records compromised and actual costs.

One initial observation is that the number of breaches reported to the OBP and other sources are noticeably small compared to the large number of potential healthcare targets. Even at its peak in pandemic year 2020, with 663 OBP Breaches and 810 total HCAD breaches, only eleven healthcare firms in ten thousand (11:10,000) experienced a reportable data breach.[10] Possibly many additional breaches involved non-PHI records, encrypted data, affected less than 500 individuals or otherwise did not meet DHHS OCR requirements for reporting. Nevertheless, data from the insurance sector (discussed later) indicates that the level of claimable breaches may be more than ten times higher – possibly an indication that the insurers likely have a better understanding of the frequency and cost of healthcare cyber risk than regulatory authorities.

[10] With 784,626 U.S. healthcare firms (see p. 2), for 663 OCR Breach Portal (OBP) postings in 2020, the frequency was 11 per 10,000

Prior to 2014, the number of breaches caused by internal actors due to the loss or theft, or unauthorized insider access annually exceeded breaches caused by external hacks by a ten to one margin (Figure 6.3). Beginning in 2014, external hacks began to close the gap, exceeding internal breaches in 2019 and by a margin of more than 2.5 times in 2020. In 2015, internal breaches leveled out, possibly indicating better grasp on how to manage internal breach risk.

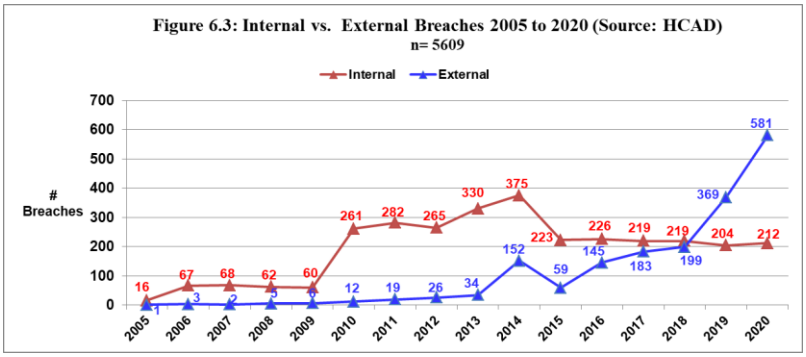


Figure 6.3: Internal vs. External Breaches 2005 to 2020 (HCAD)

Examination of the number of records breached by breach type (Figure 6.4) shows that external breaches became significantly more impactful beginning in 2015, dropped in 2016 through 2018, only to again increase dramatically in 2019. Likewise, records compromised for internal breaches have remained steady, at a lower level than external breaches, from 2015 on.

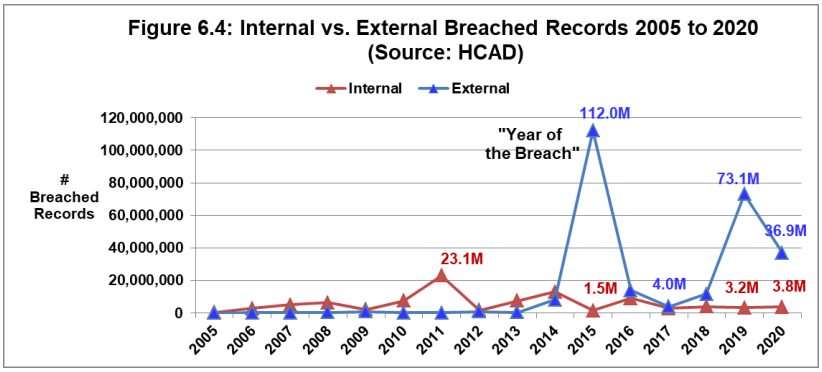


Figure 6.4: Internal vs. External Breached Records 2005-2020 (HCAD)

Focusing on external breaches by subtype (Figure 6.5) and records compromised by external subtype (Figure 6.6), there is the emergence of ransomware in 2016, the increase in both standard hacks and ransomware in 2019, near parity in number and the emergence of ransomware as the predominate cause of records compromise in 2020 (HCAD 2021).

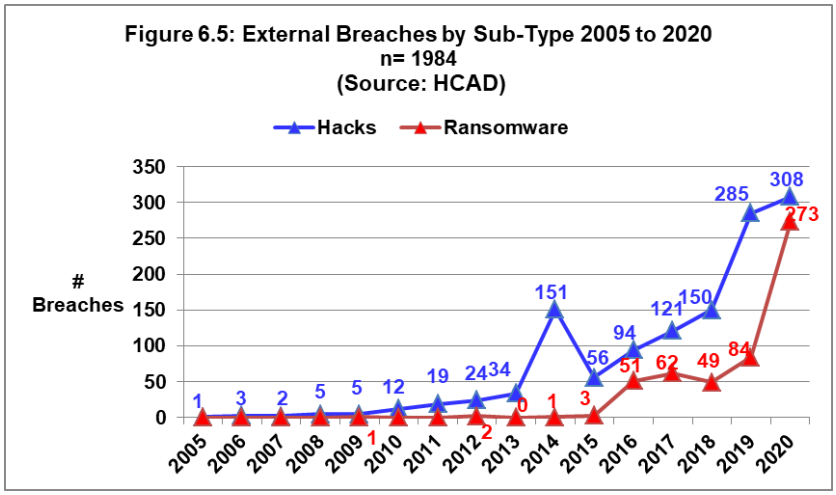


Figure 6.5: External Breaches by Sub-Type (2005 to 2020)

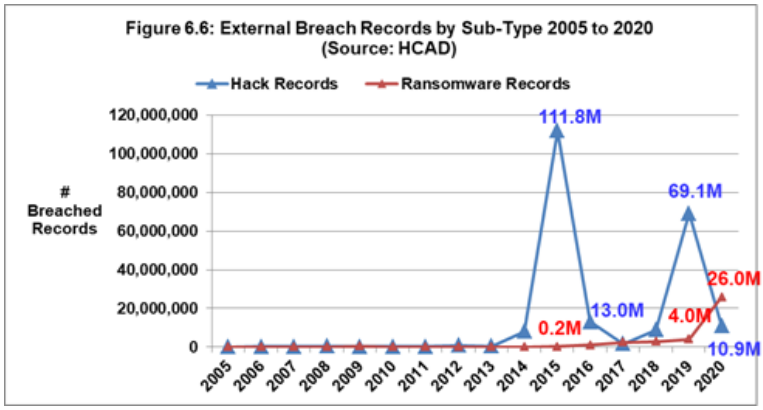


Figure 6.6: External Breach Records By Type (2005-2020)

Another observation is that many HCAD healthcare organizations had multiple breaches, with forty-four (44) experiencing seven or more breaches (Table 6.3), These organizations represent less than one percent of all HCAD entities, but experienced more than ten percent of the total breaches and 28.8 percent of the total records exposed. Further, five organizations, including the Veterans Administration, Blue Cross Blue Shield, Kaiser, Texas Health and UnitedHealth had twenty of more breaches each over the period 2005 to present.

Table 6.3: Firms Experiencing Multiple Breaches 2005 to Present (HCAD 2021)

# Breaches	# Entities	Total #	# Records	Companies	Average/ Company	Average/ Breach
58	1	58	838,924	Veterans Administration	838,924	14,464
38	1	38	1,606,820	BlueCross BlueShield	1,606,820	42,285
31	1	31	564,613	Kaiser Health Plan	564,613	18,213
24	1	24	390,590	Texas Health	390,590	16,275
20	1	20	106,021	UnitedHealth	106,021	5,301
19	1	19	4,559,062	University of California	4,559,062	239,951
18	1	18	909,516	Personal Touch	909,516	50,529
17	2	34	289,737	University of Texas, University of Pittsburg Medical	144,869	8,522
16	3	48	1,487,722	Humana, Walgreens. Aetna	495,907	30,994
14	2	28	199,140	CVS, Mount Sinai	99,570	7,112
12	1	12	67,253	Walmart	67,253	5,604
11	1	11	50,564	Indiana University Health	50,564	4,597
10	6	60	9,925,832	Advocate, HealthNet, Henry Ford Health, RiteAid, St. Vincent Health, University of Florida	1,654,305	165,431
9	3	27	1,078,681	Molina Health, NYU Health,Triple S	359,560	39,951
8	10	80	80,048,946	Anthem, Baptist Health, Cigna, Delta Dental, Healthcare Services, Louisiana State Health, Memorial Health, Montefiore Medical Center Johns Hopkins, WellCare	8,004,895	1,000,612
7	9	63	10,885,646	Allina, LabCorp, Community Health Network, Florida Hospital, Health Fitness, California Dept. of Health, Cook County Hospital. North Carolina Dept. of Health, Yale health	1,209,516	172,788
6 or Less	4427	5038	279,361,911	Various	63,104	55,451
TOTALS	**4471**	**5609**	**392,370,978**			
7+ Breaches	**44**	**571**	**113,009,067**			
% 7+ Breaches	**0.98%**	**10.18%**	**28.80%**			

The OCR Breach Portal categorizes breaches into four covered entity types: 1) Healthcare Providers, 2) Health Plans, 3) Healthcare Clearing Houses, and 4) Business Associates. The HCAD subdivides these categories into 27 subcategories (Table 6.4). Most of the subcategories are self-explanatory. Business associates are divided into those entities that provide administrative support such as billing and claims processing, and technology support such as network services and data storage. Healthcare providers include individual practitioners (e.g. doctors, dentists, and optometrists), group practices, hospitals/medical centers that are located in one place, and health systems that involve facilities in multiple locations. Other healthcare provider subcategories include private healthcare support functions including ambulances, medical associations, community support groups, home healthcare/hospices, laboratories, medical equipment manufacturers, medical schools, mental health/treatment facilities, wellness centers, pharmaceutical companies/drug distributors, rehabilitation/physical therapy centers, senior care facilities, and medical supply companies. The list also differentiates between private entities from public healthcare providers including county/municipal health departments, state health services, and federal facilities such as Veterans Administration hospitals. Private health insurer breaches dominate the health plan category, but also include public entities such as CMS.

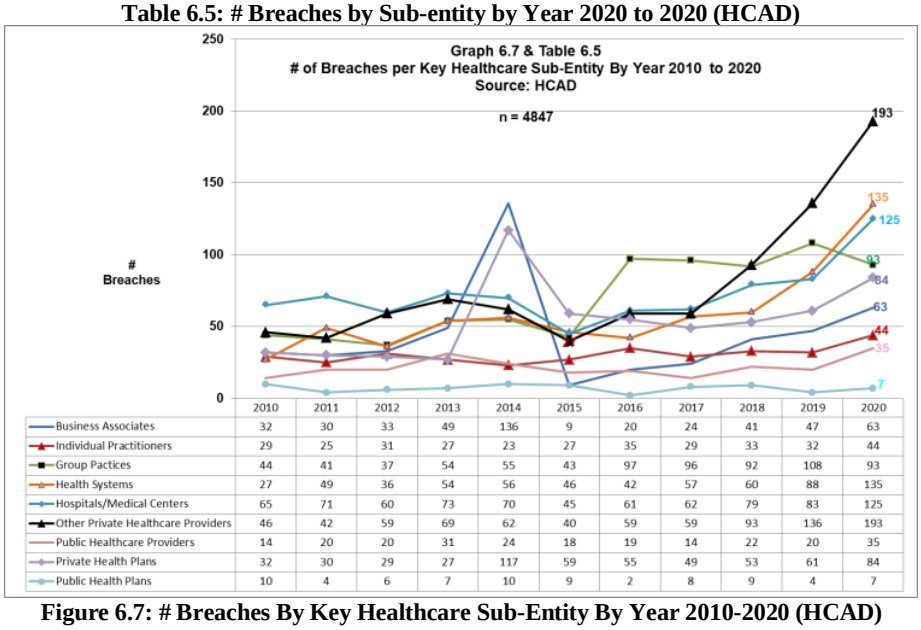
Table 6.4 Breaches By Healthcare Sub-Entities - 2005 to present (HCAD 2021)

Entity	Sub-Entity	# Breaches	%	# Records	%	Average
Business Associate	Administration/Finance	380	6.77%	63,717,439	16.24%	167,677
	Technology	166	2.96%	21,124,779	5.38%	127,258
Healthcare Clearing House	Healthcare Clearing House	7	0.12%	1,586,654	0.40%	226,665
Healthcare Provider	Ambulance/Emergency Response	18	0.32%	200,615	0.05%	11,145
	Association/Foundation/Research	60	1.07%	1,177,992	0.30%	19,633
	Blood Donation	4	0.07%	890,893	0.23%	222,723
	Community Support Services	122	2.18%	909,582	0.23%	7,456
	County/City Public Health	134	2.39%	1,837,350	0.47%	13,712
	Federal Government	67	1.19%	5,909,722	1.51%	88,205
	Group Practice	880	15.69%	22,903,166	5.84%	26,026
	Health System	783	13.96%	65,904,846	16.80%	84,170
	Home Healthcare/Hospice	87	1.55%	1,455,237	0.37%	16,727
	Hospital/Medical Center	968	17.26%	18,673,282	4.76%	19,291
	Individual Practicioner	358	6.38%	6,250,141	1.59%	17,458
	Laboratory	78	1.39%	14,399,411	3.67%	184,608
	Medical Equipment	44	0.78%	1,361,374	0.35%	30,940
	Medical Schools	61	1.09%	1,054,735	0.27%	17,291
	Mental Health/Recovery	127	2.26%	1,325,168	0.34%	10,434
	Nutrition/Wellness/Fitness	24	0.43%	28,237	0.01%	1,177
	Pharmaceutical/Drug Stores	127	2.26%	3,351,477	0.85%	26,390
	Radiology/Imaging	42	0.75%	2,645,650	0.67%	62,992
	Rehabilitation/Physical Therapy	68	1.21%	322,427	0.08%	4,742
	Senior Care	72	1.28%	1,207,334	0.31%	16,769
	State Healthcare	81	1.44%	2,889,060	0.74%	35,667
	Supplier	67	1.19%	2,257,421	0.58%	33,693
Health Plan	County/City Public Health	9	0.16%	31,560	0.01%	3,507
	Federal Government	4	0.07%	75,863	0.02%	18,966
	Private Insurer	693	12.36%	137,741,801	35.10%	198,762
	State Health Plans	78	1.39%	11,137,762	2.84%	142,792
	TOTALS	**5609**		**392,370,978**	**100.00%**	

Examination of the data in Table 6.4 shows that larger sub-entities that house significant amounts of PHI are the primary targets of breaches. Six sub-entities: private insurers, health systems, hospital/medical centers, administrative and technology business associates, and group practices account for nearly 70 percent of breaches and over 84 percent of breached records. Since there are only about 6000 hospitals (AHA 2021) and less than 1000 private health plans (III 2021) and health systems (AHRQ 2017) in the US, the likelihood of attacks against these sub-entities appears to be much greater. Conversely, there are over 36,000 U.S. group practices (AHRQ 2019, p. 8), making the likelihood of a cyberattack comparatively lower.

However, review of the data for key sub-entities by year (Figure 6.7 and Table 6.5) show some hidden patterns in the numbers. Both business associates and private health plans spiked in 2014, only to plummet in 2015 and then rise more gradually through 2020. Certain sub-entities including individual practitioners and public health plans have little change over the period. Group practice breaches, while high, stay flat from 2016 on. Notable is the dramatic increase in cyber-attacks against hospitals, health systems, and "other private healthcare providers." This sub-category includes mental health/addiction recovery, home healthcare/hospice/senior care, laboratory, pharmaceutical companies/drug stores, radiology/imaging companies, and medical equipment/suppliers. What makes this sub-category unique is that it often involves vulnerable populations such as mentally ill or elderly, and, companies that have recent PHI or research data that is especially valuable such as test results, prescriptions, or intellectual property.

Table 6.5: # Breaches by Sub-entity by Year 2020 to 2020 (HCAD)

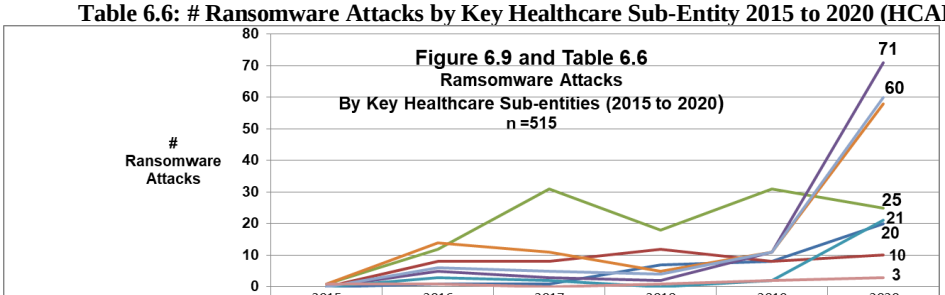


	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Business Associates	32	30	33	49	136	9	20	24	41	47	63
Individual Practitioners	29	25	31	27	23	27	35	29	33	32	44
Group Pactices	44	41	37	54	55	43	97	96	92	108	93
Health Systems	27	49	36	54	56	46	42	57	60	88	135
Hospitals/Medical Centers	65	71	60	73	70	45	61	62	79	83	125
Other Private Healthcare Providers	46	42	59	69	62	40	59	59	93	136	193
Public Healthcare Providers	14	20	20	31	24	18	19	14	22	20	35
Private Health Plans	32	30	29	27	117	59	55	49	53	61	84
Public Health Plans	10	4	6	7	10	9	2	8	9	4	7

Figure 6.7: # Breaches By Key Healthcare Sub-Entity By Year 2010-2020 (HCAD)

Such populations and information have become particularly susceptible to extortion and ransomware attacks that became more frequent in 2016, and the dominant form of attack during the COVID pandemic. Figure 6.8 and Table 6.6 document 515 healthcare ransomware attacks identified during the period 2015 to 2020, and detailed in Appendix B. The data shows that ransomware went from almost nothing in 2015, to 268 attacks in 2020. Hospitals were early targets of ransomware in 2016, with high profile attacks against Hollywood Presbyterian Medical Center and Kansas Heart Hospital, resulting in both five-figure extortion payments and substantial downtime. During the period 2017 to 2019, group practices lead all subgroups with 80 ransomware attacks, only to subside in recent years. Health systems, other private healthcare providers, hospitals, private health plans and business associate all peaked in 2020, in each case being 2.5 to 6 times higher than 2019. Individual practitioners and both public healthcare providers and plans experienced comparatively few ransomware attacks possibly reflecting preparedness, but more likely their lack of desirability as extortion targets.

Table 6.6: # Ransomware Attacks by Key Healthcare Sub-Entity 2015 to 2020 (HCAD)



	2015	2016	2017	2018	2019	2020
Business Associates	0	1	1	7	8	20
Individual Practitioners	0	8	8	12	8	10
Group Practices	1	12	31	18	31	25
Health Systems	0	5	3	2	11	71
Private Health Plans	0	3	2	0	2	21
Hospitals/Medical Centers	1	14	11	5	11	58
Other Private Healthcare Providers	0	6	5	4	11	60
Public Healthcare Providers	1	1	0	1	2	3

Figure 6.8: Ransomware Attacks by Key Healthcare Sub-Entity 2015 to 2020 (HCAD)

Finally, when available, cyber-attack impact data is included in HCAD, both in terms of PHI records compromised and actual monetary costs associated with federal and state fines, legal settlements, extortion payments paid, and number of days of operational downtime.

The cost equation for ransomware attacks is a little different. Such attacks can compromise PHI records, and in about 70 percent of the cases are reported to the OCR Breach Portal (HCAD 2021). However, the other 30 percent of attacks, including the high profile attack against the Kansas Heart Hospital in 2016, do not involve the compromise of PHI and are often not reported to the OBP. These attacks often result in class action lawsuits, but in most cases are so recent that no settlements have to date been reached. The most immediate costs are ransoms paid (if any), and the amount of downtime experienced by the healthcare entity resulting from the attack. Ransoms paid are rarely publicly reported. However, downtimes are much more visible since there is usually a clear starting point when disruptions first happen, and affected entities are usually anxious to report when operations are restored. In March 2021, analytics firm Comparitech using data from media sources and ransomware recovery company Coveware estimated that the average downtime by 2020 quarter ranged from 15 to 21 days (Bischoff 2021). Based on this downtime alone, they go on to estimate that the cost of healthcare-sector ransomware attacks in 2020 was $20.8 billion, and over $31 billion since 2016 (Bischoff 2021).

Cyber insurers, are arguably in the best position to understand the costs associated with healthcare ransomware attacks. With a healthcare cyber insurance take-up rate of 67

percent (see p. 2), ransomware attack costs are reasonably claimed by policyholders. This includes claims for ransom paid and business interruption. It may also include claims for recovering data and notifying patients, and potential claims for litigation costs and regulatory fines. There has been some speculation that the availability of insurance to pay ransoms may actually encourage attackers to target insured entities (Dudley 2019). Targeted companies may also be more inclined to pay ransom to get their systems back online sooner if they have insurance coverage (Bajak 2021). To deal with this problem, both insurers and government regulators are promoting a strategy not to pay ransoms, and instead encourage investment in resources to prevent ransomware attacks from occurring, and to recover quickly when they take place so as to minimize downtime and business interruption.

Thus, based on the evidence, healthcare cyber threats and risks have evolved considerably since the enactment of HITECH in 2009. In response, insurers have adapted their underwriting practices, coverage, pre-breach risk management practices and post-breach mitigation services to help clients reduce the frequency and impact of losses, and improve their own bottom lines.

V. Managing Healthcare Cybersecurity Safety

This section examines how public mechanisms, including regulation, legislation and litigation have influenced healthcare-firm cyber behavior. It is followed with a discussion of the ways private cyber insurance regulates healthcare-sector cyber safety through pre-coverage screening, policy mechanisms, and premiums; and how insurance coverage adapts to evolving healthcare-sector cyber risks.

Cybersecurity does not exist in a vacuum. Implementing cybersecurity measures in the healthcare-sector has consequences affecting other aspects of patient safety. There is a fundamental tradeoff between data security and data access. Security protocols that hamper the ability of healthcare providers to get vital patient information in an easy and timely manner can negatively affect patient care. Healthcare firms also have economic tradeoffs between investing in cybersecurity technology and services versus acquiring resources to enhance patient treatment. As described in earlier sections, the financial cost of cybersecurity can be especially burdensome to small healthcare firms that lack the resources to implement expensive cybersecurity solutions. Cybersecurity needs and capabilities vary not only based on the healthcare firm size, but also on its organizational subtype and mission. Good healthcare cybersecurity maximizes patient safety, optimizes the financial investment between cyber and treatment-enhancing resources and technologies, and ideally customizes functionality to meet each firm's characteristics and needs.

General-purpose controls and safeguards to manage cyber security include maintaining up-to-date anti-virus and operating systems software, deploying firewalls, implementing password and access management (including MFA), encrypting sensitive data, educating employees on safe practices, and conducting regular audits and risk assessments were described in the literature review and are applicable to nearly all public and private sector firms. What makes the U.S. healthcare-sector unique is the federal regulatory mechanisms under HIPAA/HITECH that require healthcare firms to implement these practices, report breaches when they occur, and has the power to punish

firms that have HIPAA/HITECH violations through civil monetary fines and even criminal prosecution.

A. Government Regulatory Cyber Safety Actions

This section examines the role of government regulators in managing the cyber safety of public and private sector healthcare entities. While there are at least 20 different federal agencies, as well as numerous state and local institutions, that oversee the cyber activities of the healthcare industry (HCIC 2017, pp.12-13), this section will focus on the regulatory activities of the OCR and their oversight of HIPAA/HITECH Privacy, Security, and Breach Notification Rules.

1. *OCR and HIPAA Privacy and Security Rules*

As previously discussed, Congress in 1996 enacted HIPAA, and subsequently DHHS developed and finalized the HIPAA Privacy and Security Rules. Initially, the OCR administered the Privacy Rule, and the CMS oversaw the Security Rule. However, over time, DHHS recognized that there was overlap between the two rules, and, subsequently, the DHHS Secretary delegated authority for oversight and enforcement of both rules to OCR in 2009 (DHHS 2009).

The Privacy Rule went into effect in April 2003 and established national standards for how healthcare organizations use and disclosure patient PHI. It protected all PHI held or transmitted by a covered entity (CE) or its business associate (BA), in any form or media. The Security Rule that went into effect in April 2005, established nationwide standards for safeguarding PHI that is in electronic format (ePHI). Most important, both

rules require that all CEs have in place appropriate physical, technical, and administrative safeguards to ensure CIA of PHI.

The Security Rule defines physical safeguards as "physical measures, policies, and procedures to protect a CE's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion." (45 CFR § 164.310). When evaluating and implementing these standards, CEs must consider all physical access to ePHI. With the increasing use of mobile devices and remote access, this includes outside of the medical facility at any location where employees access ePHI. Specifically, physical safeguard standards include: 1) facility access controls, 2) workstation use, 3) workstation security, and 4) device and media controls (CMS 2007).

The Security Rule defines technical safeguards as "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it" (45 CFR § 164.304). These are technical standards designed to protect the confidentiality, integrity and availability of ePHI. Specifically, technical safeguards include access control, audit controls, data integrity checks, user authentication, and transmission security. Since the Security Rule is based on the fundamental concepts of flexibility, scalability and technology neutrality, no specific requirements for types of technology to implement are identified. The Security Rule allows CEs to use any security measures that are reasonable and appropriate to implementing the standards such as choice of firewall, anti-virus, and encryption techniques (CMS 2007A).

Administrative safeguards are the largest section within the HIPAA Security Rule, making up over half of the total requirements. The Security Rule defines administrative

safeguards as, “administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of the CE’s workforce in relation to the protection of that information” (45 CFR § 164.308). Administrative safeguard standards include security management, assigned security responsibility, workforce security, information access management, security awareness and training, security incident procedures, contingency plan, evaluation, and business associate agreements. This section requires CEs to appoint an employee responsible for security oversight. It also outlines requirements for security awareness training. CEs are also required to have incident-response procedures, and to have contingency plans for data backup, disaster recovery, and emergency mode operations. They also must have written contracts with all BAs.

Arguably most important, they must implement security management procedures including conducting “an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the covered entity” (§ 164.308(a)(1)(ii)(A)). After conducting the risk assessment, they must then develop a risk management strategy on how to address entity specific security risks and vulnerabilities (§ 164.308(a)(1)(ii)(B)); and to “regularly review records of information system activity” to determine if any ePHI is used or disclosed in an inappropriate manner (§ 164.308(a)(1)(ii)(D)).

However, while the Security Rule requires CEs to conduct a risk assessment, develop a risk management strategy, and conduct regular audits to confirm ePHI protection, it does not clearly state or prescribe what they must do to guarantee

compliance with the Security Rule. This lack of specificity, especially regarding the risk assessment, plagued the Security Rule from its inception. Audits conducted by OCR of 166 CEs and 41 BAs in 2016-2017 showed that most "failed to implement the HIPAA Security Rule requirements for risk analysis and risk management" (DHHS December 2020, p. 4). To try to rectify this situation, DHHS began working with private sector and government partners, to develop a Healthcare-sector Cybersecurity Framework (HSCF), to provide guidance for CEs to conduct risk assessments. The basis for the HSCF was a national cybersecurity framework first released by the National Institute of Standards and Technology (NIST) in 2014.

2. *OCR, HSCF, NIST CsF and the Security Risk Assessment (SRA) Tool*

Under the National Infrastructure Protection Plan (NIPP), last updated by the Department of Homeland Security in 2013, the DHHS has responsibility for coordinating critical infrastructure security and resilience activities for the Healthcare and Public Health (HPH) Sectors. In 2015, DHHS established a Joint Cybersecurity Working Group (JCWG) to develop the HSCF

The HSCF is based in part on the NIST Cybersecurity Framework (CsF) first released in 2014 and updated in 2018 (NIST 2021). The NIST CsF is a voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. It describes five desired cybersecurity outcomes: 1) Identify, 2) Protect, 3) Detect, 4) Respond, and 5) Recover. It then outlines a series of steps that organizations need to take to evolve their cybersecurity maturity level from partial (lowest acceptable) to adaptive (highest). The NIST CsF also lists all of

the various standards that firms can adopt to satisfy 23 categories and 108 subcategories of cybersecurity actions such as access control, identity management, and training to improve cybersecurity readiness and higher cybersecurity maturity. In 2016, OCR created a direct crosswalk document between the NIST CsF and the HIPAA Security Rule (OCR 2016), mapping each administrative, physical and technical safeguard standard to a relevant NIST CsF subcategory. However, they added a disclaimer that entities "who have aligned their security program to the NIST CsF should not assume that by so doing they are in full compliance with the Security Rule" (OCR 2016, p. 2). In 2018, OCR developed a downloadable Security Risk Assessment (SRA) Tool (HealthIT.gov 2021) to walk CEs through each HIPAA safeguard requirement, with questions tailored to a firm's unique characteristics. However, despite this tool, DHHS still refused to guarantees its use as legal evidence of HIPAA Security Rule compliance. As a result, many healthcare CEs and BAs remain in limbo regarding what actions they needed to take to comply with HIPAA security standards. Complicating this issue is OCR's ability to monitor and enforce compliance, and the relevance of the HIPAA Security Rule in the face of ever evolving healthcare cybersecurity risks, including ransomware.

3. *HITECH EHR Incentive Program and Breach Reporting Rule*

On February 17, 2009, President Obama signed the *Health Information Technology for Economic and Clinical Health (HITECH) Act* into law One of the primary goals of HITECH was to incentivize healthcare entities to adopt electronic health record (EHR) systems.

The HITECH Act created the EHR Incentive Programs to encourage "eligible" Medicare and Medicaid providers to adopt certified EHR technology (CEHRT) (CMS 2021) and use it in a meaningful manner. Beginning in 2011, Eligible Practitioners (EPs) that demonstrated meaningfully use of CEHRT could receive up to $44,000, and Eligible Hospitals (EHs) up to $6.37 million in incentive payments.. By November 2015, 307,656 EPs and 4,498 EHs had attested to meaningful receiving over $19.5 billion in incentive payments (Murphy 2016).

However, in encouraging the use of EHR, Congress also recognized the need to strengthen ePHI protections under the HIPAA Privacy and Security rules. HITECH strengthened ePHI protection in several ways. First, under the EHR Incentive Program, EPs were required to attest that they conducted a risk analysis as required by HIPAA, and Congress authorized CMS to conducts audits to verify compliance. Second, Subtitle D of the Act included enhanced ePHI security and privacy protections, through several provisions that strengthen the civil enforcement of the HIPAA rules. Congress increased civil penalties for HIPAA violations and ordered DHHS to issue regulations for breach notification by CEs subject to HIPAA and their BAs.

Under the Breach Notification Rule (45 CFR §§ 164.400-414) a breach is defined as "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI" (45 CFR 164.402). The Rule requires HIPAA CEs and their BAs to provide notification following a breach of unsecured PHI. Unsecured PHI has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology (e.g.

encryption) or other DHHS approved methods. Following a breach of unsecured PHI, CEs must provide notification of the breach to affected individuals, the DHHS, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

Covered entities must notify affected individuals no later than 60 days following the breach discovery. Further, CEs must also notify DHHS of breaches of unsecured PHI. If a breach affects 500 or more individuals, CEs must notify DHHS without unreasonable delay and in no case later than 60 days following a breach. However, if a breach affects fewer than 500 individuals, the CE may notify the DHHS of such breaches on an annual basis - no later than 60 days after the end of the calendar year of breach discovery (DHHS 2013). Thus, legally, CEs are required to notify DHHS of all breaches of unsecure PHI, including breaches of less than 500 records.

4. *OCR Audit Program*

Section 13411 of the HITECH Act authorizes and requires DHHS to provide periodic audits to ensure that CEs and BAs comply with the Privacy and Security Rules. In response, OCR implemented a pilot program to conduct 115 audits of CEs from 2012 to 2013. The 115 CEs audited included: 47 health plans, 61 health care providers, and 7 health care clearinghouses, ranging in size and type. The results showed that a majority of CEs audited, particularly small entities, showed significant deficiencies with regard to all of the HIPAA Rules (OCR 2013).

OCR completed a second round of audits in 2017 involving 166 CEs and 41 BAs. For Phase 2 audits, OCR identified pools of CEs that represented a wide range of health

care providers, health plans, and health care clearinghouses to better assess HIPAA compliance across the industry. OCR divided health plans into group plans and issuers and categorized providers by type including hospital, practitioner, skilled nursing facility, health system, or pharmacy. The audit rated each entity on a score of 1 (full compliance) to 5 (not compliant), with a score of 3 indicating minimally compliance (DHHS 2020, p. 10). Once again, audits found that all types of audited entities failed to implement effective risk analysis and management strategies required by the Security Rule, and most failed to adequately safeguard PHI as required by the Privacy Rule (DHHS 2018). DHHS released a full report on the Phase 2 audits in December 2020.

5. *OCR and HIPAA Enforcement Rule*

In 2009, DHHS, under the HITECH Enforcement Rule, significantly increased the civil monetary penalties (CMPs) for HIPAA violations (DHHS 2009), and granted OCR full authority for Rule administration and enforcement. Under this authority, OCR was required to conduct periodic audits for HIPAA/HITECH compliance, investigate HIPAA complaints and reported breaches, and could impose CMPs for HIPAA violations. OCR can also provide education and technical assistance to help CEs and BAs comply with HIPAA and HITECH requirements. It can also refer possible HIPAA criminal violations to the Department of Justice.

Per the FY2021 DHHS Annual Report, in 2020 OCR had 157 full time employees and a budget of less than $30 million. Employees located at headquarters and eight regional offices handle not only HIPAA compliance and enforcement, but also administer and enforce federal anti-discrimination laws and DHHS-sponsored religious freedom

initiatives. Thus, the resources available to conduct HIPAA audits and investigations are extremely limited.

OCR enforces the HIPAA Rules by investigating written complaints filed with OCR, and by conducting compliance reviews of circumstances brought to its attention through submitted breach reports, media stories or referrals from other federal agencies. For the period 2015 to 2020, OCR closed 146,624 complaints averaging over 24,000 per year. The complaints go through a triage process where a central intake unit reviews all complaints as submitted and determines whether a complaint presents an eligible case for enforcement. They then decide to decline to investigate, provide "technical assistance" in lieu of an investigation, or forward the complaint to a regional office for review and potential investigation. Over this period, nearly 95 percent were resolved without investigation by the central intake either immediately after review (68.9%) or after providing technical assistance (26.0%). The remaining 7,440 complaints were investigated, with 2,189 (1.49%) found to have no violation, and 5,251 (3.6%) having violations requiring technical assistance or other corrective action.

OCR must investigate all breaches submitted to its breach portal. Over the period 2009 to 2020, it had over 3700 breaches involving 500 or more PHI records posted – increasing from just 18 in 2009 to 645 in 2020. Over the period 2015 to 2020, OCR closed 2,234 investigations, including 2,107 identified through the breach portal and 107 from media reports or referred by other agencies. A total of 1968 incidents (88.1%) were found to have compliance violations requiring technical assistance or other corrective

actions, with the other 266 incidents either having no violations or closed by OCR due to lack of jurisdiction or other reasons.

All told over the period 2015 to 2020, OCR conducted 9,674 investigations – 7,440 from complaints and 2,234 from compliance reviews. They found compliance violations in 7,219 - nearly three quarters of all investigations (74.6%) requiring corrective action and, potentially resulting in settlements or CMPs. However, over the six years, OCR reached less than sixty resolution settlements involving CMPs – in less than one percent of all investigations.

The low number of settlements since 2009 has given the healthcare industry the impression that OCR HIPAA enforcement is weak – unlikely to catch most offenders and dispensing mainly slaps-on-the-wrist when violations occur. DHHS, though OCR and other agencies, provides useful guidance and tools to promote risk assessments and safeguard adoption as required by the Security Rule. Still, evidence suggests that many covered entities have failed to comply with these and other simple precautions, leaving many exposed to future breaches.

B. Healthcare Cybersecurity Litigation & Cyber Safety

This section analyzes the impact of public and private litigation in managing the cyber safety actions of healthcare entities. This includes federal and state data breach investigations and settlements under HIPAA/HITECH and other privacy statutes, and civil liability lawsuits and class actions under tort and common law.

To conduct this analysis, an additional dataset of over 250 public and private healthcare statutory settlements and civil suits (HCAD-L) was created (see Appendix C).

HCAD-L data fields include name of healthcare entity defendant, year of breach, type of breach, number of breach records involved (if known), type of entity, case names, type of case (e.g. class action), case status (continuing/dismissed/settled), judgement year, and settlement amount (if any).

1. *Federal & State Healthcare Data Breach Litigation & Settlements*

As previously discussed, OCR is the federal agency responsible for HIPAA enforcement. However, since the passage of HITECH Act in February 2009, state attorneys general (SAGs) also have the authority to bring civil actions on behalf of state residents for violations of the HIPAA Rules. This authority allows SAGs to obtain damages on behalf of state residents, and work with OCR and other states to enjoin further HIPAA violations. Further, all 50 states have enacted data breach notification and privacy laws (NCSL 2021), giving SAGs more authority to investigate and litigate healthcare and other sector data breach and privacy violations.

The HCAD-L dataset contains 117 public data breach actions – 81 federal and 36 state covering the period 2005 to present (Figure 6.9). These actions led to resolution agreement and civil monetary penalty payments totaling $241.8 million - $144.2 million for federal actions and $97.6 million from state actions (Figure 6.10).

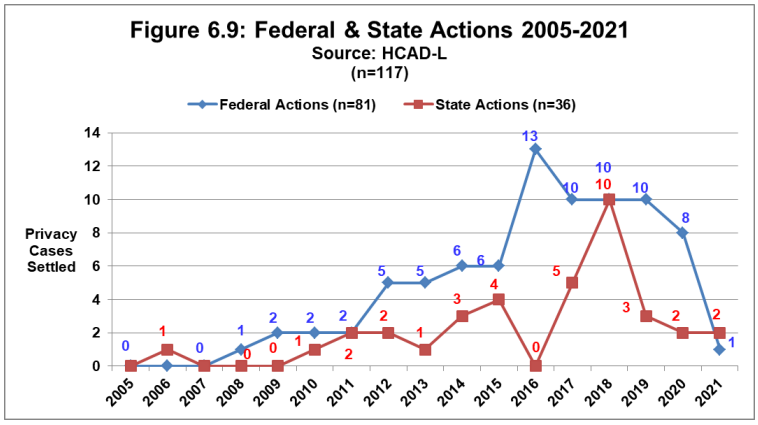


Figure 6.9 Federal & State Actions (2005-2021)

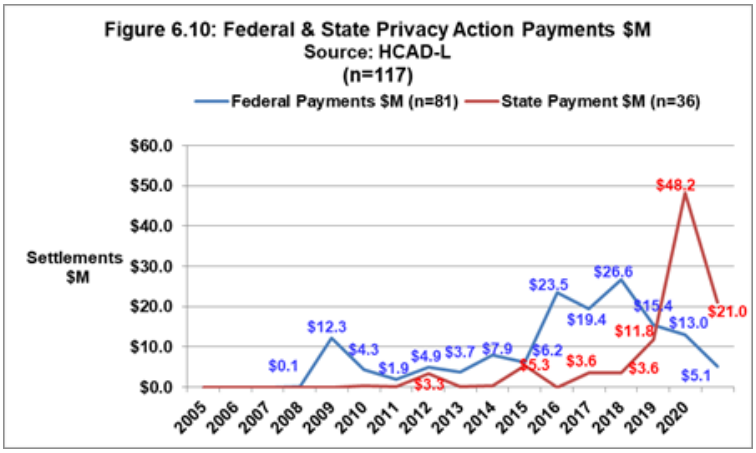


Figure 6.10 Federal & State Privacy Actions Payments

The DHHS Resolution Agreements and Civil Money Penalties webpage provides details on all 81 HIPAA security enforcement actions taken by OCR since its first action in 2008. Of the 81 actions, 77 were resolved through a negotiated Resolution Agreement – a written understanding where the entity agrees to comply with the terms of a Corrective Action Plan (CAP), with compliance monitored by OCR over a three-year period. In addition, all agreements include a resolution payment ranging from $25,000 to $16 million.

On average, the federal actions documented in HCAD-L took nearly three and a half years to go from initial breach report to final resolution. HCAD-L also shows that federal actions have occurred against a wide variety of entities ranging in size from individual doctors to huge health systems. However, over 70% of federal actions have targeted four types of entities: health systems (24.7%), health plans (21.0%), hospitals and medical centers (14.8%) and group practices (11.1%), making these entities at highest risk for HIPAA investigations and fines.

The HCAD-L state action data shows less variety in types of entities targeted, with three types making up over 70 percent: health plans (33.3%), hospitals and medical centers (25.0%) and health systems (13.9%). Business associates, either administrative or technology, are also prominent state targets, combined comprising over 16 percent of state investigations.

State investigations are completed quicker than federal investigations, taking on average two and a quarter years from initial breach report to final execution. From a risk perspective, over 60% of all state actions have taken place in four states: Massachusetts (19.4%), New York (16.7%), Califonia (13.9%), and New Jersey (11.1%). Further, over the last few years, many states have banded together to negotiate massive multi-state settlements, with six such settlements resulting in nearly 80% of all state CMPs. Notable multi-state settlements include Anthem ($39.5 million) and Premera Blue Cross/Blue Shield ($10 million) in 2015, and most recently American Medical Collection Agency ($21 million) in 2021. With the passage of the California Privacy Rights Act (CPRA) in

2020, and data breach and privacy laws in other states, the trend towards more frequent state actions and harsher settlements is expected to accelerate.

2. *Individual & Class Action Liability Lawsuits*

While litigation following a data breach now seems common, with lawsuits filed after nearly every major breach, the jurisprudence in the area is actually only about ten years old. The first major class action decision involving Providence Health in 2012, like many subsequent decisions, ended in dismissal. Data breach litigation, like other types of liability lawsuits, can drag on for years from filing, discovery, initial decision, refiling, appeals, to final settlement or dismissal. Major class action lawsuits, including Advocate Healthcare (4 million records) and Horizon Healthcare (3.7 million records), originally filed in 2013, still are being adjudicated. In fact, nearly two-thirds of all lawsuits in HCAD-L filed since 2005, continue to be litigated.

The HCAD-L dataset contains 130 private data breach litigation actions extracted from media sources including HIPAA Journal, ClassAction.org, and The National Law Review, and from case summaries found on the web. As of May 31, 2021 it consists of 96 class action lawsuits and 34 non-class action lawsuits covering the period 2005 to present (Figure 6.11). Over this period, 27 lawsuits resulted in dismissals, 21 lawsuits resulted in settlements, and a staggering 83 lawsuits are still in litigation. Most settlements have come in the past three years (Figure 6.12), and, to date, no class action cases have ever gone to a jury. Settlement totals for the 21 settled cases are $273.9 million – far more than either federal or state settlement totals.

This amount is skewed by the $115 million Anthem settlement in 2017. Still, with 83 cases outstanding, the potential liability risk from existing cases could be a trillion dollars or more.

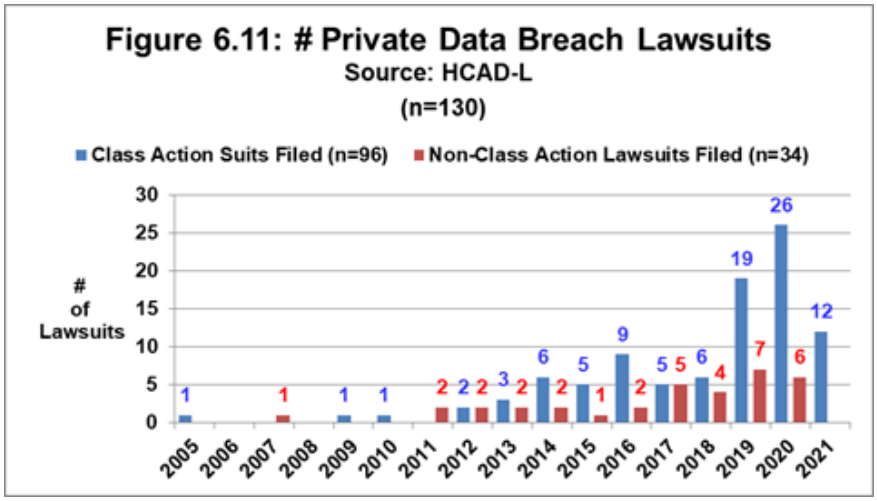


Figure 6.11: # Private Sector Data Breach Lawsuits (Source: HCAD-L)

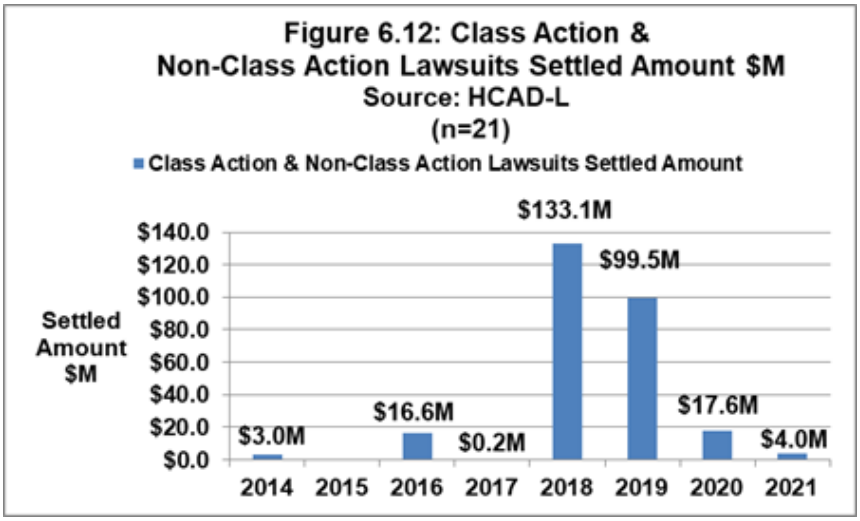


Figure 6.12: Class Action & Non-Class Lawsuit Settlements (Source: HCAD-L)

Prior to 2017, data breach liability cases rarely saw the light of day. Lawyers filed very few cases and, if they did, they often were dismissed. The risk of a company facing litigation following a data breach was fairly low due to the difficulty plaintiffs had establishing Article III standing - the legal right for a person or persons to bring a claim in court. Article III of the U.S. Constitution gives the courts the power to determine the criteria for standing. Over time, these criteria have come to consists of three elements: 1) an injury-in-fact that is concrete and particularized, as well as actual or imminent; 2) the injury must be traceable to the defendant's act; and 3) it must be "likely" that a favorable decision will compensate or otherwise rectify the injury (Bryan and Lamoureux 2020).

In 2017, agreement was reached in the largest healthcare data breach in U.S. history – Anthem. At $115 million, the amount set the benchmark for healthcare data breach settlements; however, after $38 million in attorney's fees, most of the 19.1 million plaintiffs in the class action mostly only receive free credit monitoring for two years and possibly a small amount for out-of-pocket expenses (McGee 2017). In the wake of the Anthem settlement, several other notable healthcare data breach lawsuits were settled during the period 2018 to 2020 including Premera Blue Cross ($74 million), Aetna ($17.2 million), Banner Health ($8.9 million), and UCLA Health ($7.5 million),. The HCAD-L dataset also shows considerable overlap with firms making both large private settlements and HIPAA settlements with DHHS and some states.

With the emergence of ransomware as the dominate form of cyber-attack, the pace of data breach litigation filings has accelerated. From 2017 to 2019, the number of class action lawsuits filed increased by more than 300 percent. Per HCAD-L, in 2020 and

2021, 86.4% of data breach lawsuits filed involved external hacker attacks, and of these attacks 65.8% involved ransomware. Ransomware provides plaintiff lawyers with at least two additional ways to demonstrate patient harm in order to establish case standing. First, ransomware often disrupts healthcare operations, causing ambulance diversions, delaying surgery, and threatening patient safety in a variety of ways. Second, because ransomware gangs often leak stolen PHI, through the exposure of sensitive information they are providing the evidence of harm necessary for plaintiffs to establish standing. Cyber criminals are leaking data stolen from hacks they perpetrated years previously, breathing new life into data breach litigation previously abandoned. Plaintiff attorneys are filing cases quicker, with one case filed the day after the defendant announced the breach (Morrison Foerster 2021). Often plaintiff lawyers file lawsuits in multiple jurisdictions, making defendants subject to multi-district litigation, and requiring judges to consolidate class action suits.

The HCAD-L dataset also contains non-patient related data breach litigation. High profile cyber-attacks against healthcare BAs have spawned a wide variety of different types of lawsuits. For example, in May 2020, LabCorp shareholders took legal action against LabCorp and its Board over the loss in share value caused by the breach at American Medical Collection Agency in 2019 exposing the records of 10,251,784 patients (HIPAA Journal 2020). At least 23 consumer class action suits have been filed against cloud provider Blackbaud for the May 2020 ransomware attack, and against nearly one hundred Blackbaud healthcare entity customers.

Thus, data breach litigation has evolved from a relatively mild potential risk into an increasingly active, costly and multipronged threat. Not only do healthcare firms have to worry about class actions brought by patients whose data was stolen, but also state and federal regulator actions, shareholders suits, and lawsuits resulting from the behavior of their business partners. This includes cybersecurity companies, cloud providers and insurance companies, who may enhance their ability to manage cyber risk but also create vulnerabilities that can be exploited.

Faced with this growing risk of data breach litigation, as well as the costs of operational business disruption, many healthcare entities are turning to insurance for relief.

VI. Healthcare Cyber Insurance & Private Sector Healthcare Cybersecurity Safety

This section investigates the specific role that insurance plays in managing the cyber safety of healthcare-sector entities. Section VI-A describe the demand-side of cyber insurance and the relationship between cyber-attacks against healthcare entities and their take-up of cyber insurance over the period 2015 to 2020. Section VI-B then looks at the supply-side of cyber insurance and the experiences that insurers have had managing cyber insurance claims.

A. Healthcare Cyber Insurance Market Demand & Take-Up

This section discusses the market demand for healthcare-sector cyber insurance, and the subsequent take-up rates by healthcare companies. First, this data is used to examine the relationship between cyber-attacks as documented in HCAD, and the estimated number of cyber policies issued over the period 2015 to 2020. Ratios of breaches per sub-

entity and per policy year are established to identify trends. Later, this data is used in a series of regression analyses to demonstrate cyber insurance take-up's correlation with measures of cyber safety.

Marsh Analytics, a division of insurance broker and risk advisor Marsh & McLennan, regularly produces a report on the take-up rates for cyber insurance for specific industry segments including healthcare. The General Accounting Office (GAO) used the Marsh data in a May 2021 report on the U.S. cyber insurance market (GAO 2021). The Marsh data showed that the U.S. industry-wide take-up rate for cyber insurance for all Marsh clients rose from 22% in 2015 to 47% in 2020, while the take-up rate for healthcare clients rose from 54% to 67% during the same period (Table 6.7). As shown, the healthcare sector has a higher take-up rate than any other industry except education (2018-2020) and Hospitality (2020). Putting these take-up rates into perspective, you have to know the number of firms in each sector, and sub-sector of interest. This allows the calculation of the estimated number of cyber policies issued per sector over this the past five years. Data from the 2018 U.S. Census Statistics of U.S. Businesses (SUSB 2018) provides the number of firms per sector, and this is matched with the cyber insurance take-up rates provided by Marsh. The number of cyber policies per year per sector for the period 2015 to 2020 is then extrapolated from this data. The data in Table 6.7 shows that healthcare likely had more cyber insurance policy coverage than any other key industry between 2016 and 2019, and more than all other key sectors except Hospitality in 2020.

Table 6.7: Take-Up & Est. # Cyber Policies All Firms & Key Sectors (Marsh 2018/GAO 2021 & SUSB 2018)

	2015 Take-Up Rate	2016 Take-Up Rate	2017 Take-Up Rate	2018 Take-Up Rate	2019 Take-Up Rate	2020 Take-Up Rate	2018 SUSB # Firms	2018 SUSB Code	2015 Est. # Cyber Policies	2016 Est. # Cyber Policies	2017 Est. # Cyber Policies	2018 Est. # Cyber Policies	2019 Est. # Cyber Policies	2020 Est. # Cyber Policies
All Firms	22%	26%	31%	38%	42%	47%	6,141,649	All	1,351,163	1,596,829	1,903,911	2,333,827	2,579,493	2,886,575
Healthcare	**54%**	**56%**	**63%**	**62%**	**65%**	**67%**	**674,200**	**62**	**364,068**	**377,552**	**424,746**	**418,004**	**438,230**	**451,714**
Education	41%	45%	54%	65%	74%	79%	95,554	61	39,177	42,999	51,599	62,110	70,710	75,488
Wholesale/Retail Sales	22%	29%	32%	39%	46%	48%	936,797	44-45	206,095	271,671	299,775	365,351	430,927	449,663
Communications Technology	18%	50%	51%	51%	55%	62%	82,241	51	14,803	41,121	41,943	41,943	45,233	50,989
Professional Services	25%	31%	36%	31%	35%	40%	821,129	54	205,282	254,550	295,606	254,550	287,395	328,452
Manufacturing	11%	12%	24%	30%	41%	45%	246,155	31-33	27,077	29,539	59,077	73,847	100,924	110,770
Financial	24%	25%	28%	27%	31%	33%	239,280	52	57,427	59,820	66,998	64,606	74,177	78,962
Hospitality	33%	36%	46%	57%	61%	73%	683,514	71-72	225,560	246,065	314,416	389,603	416,944	498,965
Power & Utilities	27%	31%	38%	41%	46%	48%	6028	22	1,628	1,869	2,291	2,471	2,773	2,893
Other	12%	16%	21%	31%	36%	43%	2,356,751	Var.	282,810	377,080	494,918	730,593	848,430	1,013,403

The 2018 SUSB firm data can also be used to estimate the number of cyber policies taken-up by each healthcare sub-entity originally presented in Table 6.4 (page 36). Note that some healthcare sub-entities are not classified under the primary SUSB Healthcare category (62). This includes Medical Equipment, Suppliers, Wellness, Pharmaceutical/Drug, and Medical Schools that are, respectively, in SUSB Manufacturing (33), Trade (42-44), and Education (61); with policies allocated based on the take-up rates in those categories. State and local governments initially self-insured but, after a rash of ransomware attacks, quickly adopted private insurance. All federal government sub-entities self-insure, and therefore have no private insurance.

In Table 6.8, an algorithm is used to calculate the number of policies per healthcare sub-entity per year, taking into account the size of the sub-entity based on the number of employees. Data from Marsh and other insurance analytics providers indicates that the take-up rates among large firms is very high, and is lower among small firms. For this analysis, large firms (500+ full time employees) were assumed to be fully insured (100% take-up) including most hospitals, insurers, and health systems. The vast majority of all other healthcare providers are small- to medium-sized enterprises (SMEs) with less than

500 full time employees. These firms were assigned the Marsh take-up rates for the healthcare sector.

Table 6.8: Take-Up Rates Used for Healthcare Sub-Entities and Business Associates

Type Healthcare Sub-Entity	SUSB Code	# Sub-Entities	2015 Take-Up	2016 Take-Up	2017 Take-Up	2018 Take-Up	2019 Take-Up	2020 Take-Up
Large Healthcare	62	10,338	100%	100%	100%	100%	100%	100%
SME Healthcare	62	683,205	51%	56%	63%	62%	65%	67%
Federal Government	N/A	12,409	0%	0%	0%	0%	0%	0%
State Government	N/A	3,605	20%	38%	46%	54%	68%	78%
Local Government	N/A	3,031	20%	38%	46%	54%	68%	78%
Education	61	1,823	43%	45%	54%	65%	74%	79%
Manufacturing	33	8,966	11%	12%	24%	30%	41%	45%
Wholesale/Retail Trade	42-44	42,941	21%	29%	32%	39%	46%	48%
	TOTAL	**766,318**						
Business Associates								
Medical Informatiion	51	33,520	18%	50%	51%	51%	55%	62%
Medical Administration	54	333,457	25%	31%	36%	31%	35%	40%

These take-up rates are then used to estimate the number of cyber insurance policies covering various healthcare sub-entities for the period 2015 to 2020 (Table 6.9). This policy data, coupled with the HCAD breach data for the same period, provides some preliminary evidence of the potential vulnerability of various healthcare sub-entities to cyber-attack. For every sub-entity, the number of breaches per 1000 sub-entity firms is calculated, with results ranging from less than one attack per thousand firms for Administrative (0.39), Community Support (0.53), and Doctors (0.81), to more than 450 attacks per thousand firms for Health Systems (655), and Private Health Plans (478). The average number of breaches per sub-entity is 4.16, with seventeen sub-entities falling below this average and ten being above.

Table 6.9 includes an index for those sub-entities that have cyber insurance showing the number of cyber breaches per hundred thousand policy years (total breaches/sum of 2015-2020 policies). The results show an average of 120 breaches per hundred thousand policy years, with sixteen insured sub-entities being below this index, and ten above. However, two outliers skew this average – Health Systems and Private Health Plans – each with over 7000 breaches per 100,000 policy-years. This index suggests that some sub-entities, especially those with many small firms, might benefit from insurance in minimizing the frequency of cyber breaches, while other sub-entities, particularly those with a predominance of large firms might not benefit from insurance safety practices at all. Subsequent sections further explore the relationship between cyber insurance and firm cyber safety looking at cyber insurance premiums, loss ratios, claims frequencies; and culminating in a series of regression analyses in Section VI-D.

Table 6.9: Cyber Insurance Take-Up Rate for Healthcare Sub-Entities & # of Breaches 2015-2020

#	Healthcare Sub-Entity:	SUSB ID	# Entities	Estimated 2015 Policies	Estimated 2016 Policies	Estimated 2017 Policies	Estimated 2018 Policies	Estimated 2019 Policies	Estimated 2020 Policies	# Breaches 2015	# Breaches 2016	# Breaches 2017	# Breaches 2018	# Breaches 2019	# Breaches 2020	TOTAL	Breaches Per 1000 Sub-Entities	Breaches per 100K Policy Years
1	Federal Government	GOVT	12,409	0	0	0	0	0	0	6	4	4	5	6	4	29	**2.34**	N/A
2	Administration/Finance/Clearinghouse	54	333,457	83,364	103,372	120,045	103,372	116,710	133,383	5	14	11	30	34	37	131	**0.39**	20
3	Community Clinics	62	1,400	714	784	882	868	910	938	1	0	1	1	1	2	6	**4.29**	118
4	Community Support Services	624	135,766	69,241	76,029	85,533	84,175	88,248	90,963	4	5	12	7	19	25	72	**0.53**	15
5	County/City Public Health	GOVT	3,031	606	1,152	1,394	1,637	2,061	2,364	9	13	5	11	12	27	77	**25.40**	836
6	Dentists	621	49,092	25,037	27,492	30,928	30,437	31,910	32,892	12	13	11	12	12	27	87	**1.77**	49
7	Doctors	621	100,916	51,467	56,513	63,577	62,568	65,595	67,614	13	18	14	14	11	12	82	**0.81**	22
8	Eye	621	9,987	5,093	5,593	6,292	6,192	6,492	6,691	2	5	6	7	9	8	37	**3.70**	102
9	Group Practices	621	186,289	95,007	104,322	117,362	115,499	121,088	124,814	47	107	105	101	113	103	576	**3.09**	85
10	Health Systems	N/A	637	637	637	637	637	637	637	40	38	58	61	85	135	417	**654.63**	10911
11	Home Healthcare/Hospice	6216	24,414	12,451	13,672	15,381	15,137	15,869	16,357	6	7	5	9	13	31	71	**2.91**	80
12	Hospital/Medical Center	622/6214	22,270	11,358	12,471	14,030	13,807	14,476	14,921	44	50	54	69	76	123	416	**18.68**	513
13	Private Insurer Health Plans	62/524114	762	762	762	762	762	762	762	58	53	49	52	62	90	364	**477.69**	7962
14	Laboratory/Blood Donations	621511	3,282	1,674	1,838	2,068	2,035	2,133	2,199	4	3	5	4	23	10	49	**14.93**	410
15	Medical Equipment	3391	8,966	986	1,076	2,152	2,690	3,676	4,035	2	3	4	4	5	8	26	**2.90**	178
16	Medical Schools/Nursing Schools	6113	1,823	784	820	984	1,185	1,349	1,440	4	4	4	5	4	12	33	**18.10**	503
17	Mental Health/Recovery	6232	10,889	5,553	6,098	6,860	6,751	7,078	7,296	2	5	6	7	32	25	77	**7.07**	194
18	Nutrition/Wellness	44619	11,553	2,426	3,350	3,697	4,506	5,314	5,545	0	1	2	4	2	3	12	**1.04**	48
19	Pharmaceutical/Drug Stores	446110	22,702	11,578	12,713	14,302	14,075	14,756	15,210	5	12	8	19	11	20	75	**3.30**	91
20	Radiology/Imaging	621512	4,201	2,143	2,353	2,647	2,605	2,731	2,815	1	3	0	5	4	10	23	**5.47**	150
21	Rehabilitation/Physical Therapy	6231/6239	12,740	6,497	7,134	8,026	7,899	8,281	8,536	2	5	8	12	9	12	48	**3.77**	104
22	Senior Care	6233	18,085	9,223	10,128	11,394	11,213	11,755	12,117	2	4	5	9	6	13	39	**2.16**	59
23	Medical Suppliers	42345	42,941	9,018	12,453	13,741	16,747	19,753	20,612	8	6	2	8	7	12	43	**1.00**	47
24	Technology	51	33,520	6,034	16,760	17,095	17,095	18,436	20,782	3	8	12	11	14	24	72	**2.15**	75
25	State Healthcare/Plans	GOVT	3,605	721	1,370	1,658	1,947	2,451	2,812	12	7	17	15	7	13	71	**19.69**	648
26	Ambulance/Emergency Response	62191	6,890	3,514	3,858	4,341	4,272	4,479	4,616	1	1	0	1	2	3	8	**1.16**	32
27	Association/Foundation/Research	62/8132	18,581	9,476	10,405	11,706	11,520	12,078	12,449	2	4	3	2	4	17	32	**1.72**	47
	TOTAL		714,361	331,810	378,593	424,861	423,869	449,330	466,030	295	393	411	485	583	806	2,973	**4.16**	120

B. Healthcare Cyber Insurance Supply – Premiums, Loss Ratios and Claims Frequencies

This section describes the cyber insurance supply-side economics including the number and types of policies issued, premiums collected, claims submitted and settled, and the estimated profit or losses experienced by cyber insurers over the period 2016 to 2020. While a direct relationship between specific cyber-attacks and insurance cannot be established, it does provide information on general trends including the frequency and magnitude of claims, and the impact that ransomware and associated litigation may be having on insurance availability and premiums. It also reviews key measures that insurers are including with their coverage to incentivize safety.

Data for this section's analyses come primarily from the National Association of Insurance Commissioners (NAIC) statutory Cybersecurity Insurance Filing Supplement, a detailed survey conducted annually by NAIC since 2016 . The purpose is to determine premiums and losses by lines of business, and to give an accurate view of the insurer's available reserves for losses. NAIC requires U.S. domiciled insurers to report the following information:1) number and type of policies in-force, 2) direct premiums written and earned, 3) number and type of claims reported, 4) direct losses paid and incurred and 5) defense and cost containment expenses paid and incurred (NAIC 2020). Data collected was from 3,120 insurers over the period 2016 to 2020, including 692 insurers selling standalone policies, and 2,428 selling coverage packaged with other types of insurance, usually as an "endorsement" on an existing policy. NAIC identifies each insurer by

ownership-type - either shareholder-owned (Stock) or policyholder-owned through a mutual corporation or risk retention group.

The NAIC data has several limitations. First, only domiciled insurers licensed or "admitted" in US states are required to file the annual supplement. Non-US insurers that garner premiums for US risks are not reflected in this data. Also, many next-generation "InsurTechs," that use technology to underwrite cyber insurance on behalf of admitted carriers, are not included. Thus, the NAIC data represents a sizable portion of the US market, but is not comprehensive. There is also a lag in the data of 15 to 18 months due to the varied ways that insurers report results. Thus, cyber-insurance premiums, claims and losses during 2020 often reflect policies written in 2019.

This data provides key measures of cyber insurance supply including growth in written and earned premiums, the number of cyber insurance providers, the number of policies sold, and changes to average premium cost over time. It also facilitates the calculation of several key indicators of insurer risk-management performance including loss ratios, claims-to-policy ratios, and changes to average claims payments over time. To illustrate the data's utility, it is used below to analyze the U.S. cyber insurance market as a whole and in looking at key groupings of insurers that provide cyber coverage to different sized firms within the healthcare sector.

Since NAIC began collecting cyber insurance data in 2016, the US cyber insurance market has grown significantly in premiums collected, in the number of admitted insurers offering coverage, and the number of policies issued (Table 6.10). Direct and estimated premiums more than doubled from $1.36 billion in 2016 to $2.75 billion in 2020, as did

the number of policies from 2.11 million to 4.02 million over the same period. The number of domiciled insurers selling cyber insurance grew by 42.9 percent from 434 to 620, with the biggest growth being among those firms that sell packaged (PKG) policies, with over 90 percent of policies sold as an endorsement on existing coverage. Despite this huge difference in PKG vs. standalone (SA) policies sold, SA policies had far higher written annual premiums, 1.6 times that of PKG in 2020. Larger companies prefer SA policies because they typically offer higher levels of coverage (up to $100 million per incident) and usually have clearer policy language with coverage tailored to a firm's specific needs. Due to this customization and higher coverage, the average premium for a SA policy is 25 to 30 times higher than for the additional add-on premium for a PKG.

Table 6.10: Market for US Domiciled Cyber Insurers – 2016 to 2020 (NAIC 2021)

Year	Direct Standalone (SA) Premiums Written	Direct & Estimated Packaged (PKG) Premiums Written	Total Direct & Estimated Premiums Written	# SA Insurers	# PKG Insurers	# Insurers Sell Both SA & PKG	Total # Cyber Insurers	# SA Policies	Average Premium per SA Policy	# PKG Policies	Average Premium per PKG Policy	Total # of Policies
2016	$920,686,506	$434,486,139	$1,355,172,645	54	306	74	434	152,636	$6,032	1,957,934	$222	2,110,570
2017	$994,272,631	$865,049,208	$1,859,321,839	58	386	74	518	103,455	$9,611	2,500,514	$346	2,603,969
2018	$1,109,811,451	$898,274,206	$2,008,085,657	60	416	79	555	124,098	$8,943	2,872,906	$313	2,997,004
2019	$1,260,889,293	$990,407,390	$2,251,296,683	59	449	87	595	161,389	$7,813	3,175,726	$312	3,337,115
2020	$1,618,722,178	$1,135,034,324	$2,753,756,502	63	473	84	620	196,661	$8,231	3,819,757	$297	4,016,418

Note from the above data, the average premium for both SA and PKG policies declined from 2017 levels. This is an indication of a "soft" cyber insurance market with the growing number of insurers competing on premium price – possibly at the expense of reasonable risk management precautions. The NAIC data (Table 6.11) shows a marked decline in performance between 2017 and 2020. Claims losses and defense/cost control

costs (DCC) for all policies increased two to four times over the period, far exceeding premium growth.

Two measures used by the insurance industry to gauge financial performance and underwriting profitability are the loss ratio and the combined ratio. The loss ratio divides the claims losses and the DCC costs by the amount of premiums earned or paid. The NAIC data shows that for the industry as a whole the loss ratios increased dramatically for both SA and PKG policies between 2017 and 2020, respectively from 35.4% to 72.8% for SA, and from 28.7% to 58.5% for PKG. NAIC does not collect the expense ratio for cyber insurance firms needed to calculate the combined ratio. The expense ratio measures how much the insurer spends on taxes and policy administration, including risk assessment and underwriting costs for premium determination. AON in 2021 estimated the average cyber-insurer expense ratio to be 27.3% for SA and 30.3% for PKG. ***This study will use an expense ratio of thirty percent - meaning that cyber insurers with loss ratios of more than 70 percent are likely unprofitable***.

For the period 2016 to 2019 cyber insurance overall was profitable with loss and expense ratio (combined ratios) of less than 80 percent. However, all of this changed in 2020 with the SA combined ratio likely exceeding 100 percent, and PKG combined ratio approaching 90 percent. In fact in 2020, nearly a quarter of all SA providers likely had combined ratios of over 100 percent indicating they likely had sizable losses during that year (Table 6.11).

Table 6.11: Performance of US Domiciled Cyber Insurers – 2016 to 2020 (NAIC 2021)

Year	Standalone (SA) Direct Losses Incurred	SA Defense & Cost Control (DCC)	SA Loss Ratio with DCC	Package (PKG) Estimated Loss Paid & Reserve	PKG Defense & Cost Control (DCC)	PKG Loss Ratio with DCC	# SA Claims 1st Party	# SA Claims 3rd Party	Total # SA Claims	SA Claims to Policy Ratio	Average SA Claims Payment with DCC	# PKG Claims 1st Party	# PKG Claims 3rd Party	Total # PKG Claims	PKG Claims to Policy Ratio	Average PKG Claims Payment with DCC
2016	$273,274,432	$77,221,880	43.2%	$164,202,979	$15,803,694	48.1%	1,536	1,240	2776	1.82%	$41,628	1,696	1,430	3,126	0.16%	$25,839
2017	$259,809,577	$50,831,479	35.4%	$170,837,288	$40,621,514	28.7%	2,428	1,657	4085	3.95%	$51,148	3,662	1,401	5,063	0.20%	$28,258
2018	$367,726,899	-$15,961,788	34.3%	$269,727,425	$23,774,635	36.7%	3,581	2,250	5831	4.70%	$56,232	5,074	1,838	6,862	0.24%	$42,556
2019	$498,053,231	$35,515,017	47.1%	$234,717,432	$135,715,570	41.4%	5,664	4,284	9948	6.16%	$53,984	6,325	2,212	8,533	0.27%	$32,367
2020	$919,443,533	$116,297,311	72.8%	$398,398,277	$189,714,643	58.5%	8,799	3,108	11907	6.05%	$86,964	7,665	2,532	10,197	0.27%	$51,960

The NAIC data also shows that the frequency and severity of cyber claims increased significantly between 2016 and 2020. Given the growth in the number of policies, it is not surprising to see a corresponding increase in the number of claims. However, to get a true gage of frequency, one needs to look at the ratio of claims-to-policies. The NAIC data shows that for SA, the frequency of claims increased from 18.2 claims per thousand policies in 2016, to 61.6 claims per thousand policies in 2019 – slightly decreasing in 2020. Likewise, the frequency of PKG claims also increased slightly from 1.6 to 2.7 claims per thousand between 2016 and 2019, and stayed steady in 2020. Thus, while early increases in the loss ratios between 2016 and 2019 are partially attributable to increase claims frequency, the large increase in 2020 is not.

The other factor affecting loss ratios is the severity of claims measured by the average claim amount. Here the NAIC data shows a doubling of average claim amount between 2016 and 2020 for both SA and PKG policies, with the biggest increase of over 50 percent occurring between 2019 and 2020. This is almost certainly due to the large increase in ransomware attacks, further indicated by the large increase in the number of first-party claims that cover business interruption, ransom payments, breach notification, and system recovery expenses.

To react to the ransomware-induced deterioration of loss ratios, the market has significantly hardened, with premiums reportedly rising 30 to 40 percent or more, and cyber insurers making other underwriting and policy adjustments to try to return to profitability. Some have implemented positive safety steps by increasing underwriting scrutiny including more in-depth risk assessments. Others have taken a step backwards by trying to reduce administrative expenses to improve profitability. Insurers are also decreasing coverage levels and increasing deductibles and co-pays, placing more of the financial risk on the insured.

Looking specifically at the supply and performance of healthcare cyber insurance, this study divides the NAIC data into three components. Group #1 includes cyber insurers that exclusively serve the healthcare sector (Table 6.12). Since every healthcare entity must carry malpractice insurance, specialty insurers provide this coverage, often through mutual corporations or RRGs. With their unique understanding of healthcare risks, these firms were some of the first to offer healthcare cyber insurance. The NAIC data contains a little over sixty insurers that fall into this category. Most offer cyber-insurance packaged with existing coverage. The amount of premiums is very small compared to the rest of the cyber insurance market – about 1.3 percent of the total market. However, the number of healthcare cyber policies is very high – representing half of the 2020 healthcare sector policies estimated in Table 6.7 (p. 56). The policy premiums are very small – averaging less than $750 per policy for SA and less than $200 for PKG. Consequently, the coverage provided is often small - sometimes as low as $50,000 per policy year.

Table 6.12: Market for Healthcare-Specific Group #1 Cyber Insurers – 2016 to 2020 (NAIC 2021)

Year	Direct Standalone (SA) Premiums Written	Direct & Estimated Packaged (PKG) Premiums Written	Total Direct & Estimated Premiums Written	# SA Insurers	# PKG Insurers	Total # Cyber Insurers	# SA Policies	Average Premium per SA Policy	# PKG Policies	Average Premium per PKG Policy	Total # of Policies
2016	$4,572,588	$21,202,663	$25,775,251	10	52	62	6,187	$739	184,155	$115	190,342
2017	$1,640,478	$30,641,685	$32,282,163	7	54	61	6,236	$263	190,407	$161	196,643
2018	$2,659,666	$30,229,821	$32,889,487	8	58	66	8,849	$301	202,854	$149	211,703
2019	$5,339,301	$29,379,276	$34,718,577	11	55	66	10,477	$510	208,723	$141	219,200
2020	$8,910,916	$30,006,458	$38,917,374	10	54	64	14,677	$607	228,830	$131	243,507

Certain aspects of the performance of these healthcare-specific insurers (Table 6.13) are interesting and surprising. Like the previous industry-wide data, there is a sharp increase in claims losses between 2016 and 2020. However, regarding loss ratios, unlike the previous data, SA outperforms PKG. SA stays profitable all five years while PKG posts losses in 2019 and 2020. Part of the rising loss ratios for both SA and PKG relate to rising DCC expenses that in the case of PKG is larger than claims losses during several years. This almost certainly relates to the rise in public and private breach litigation discussed in Section V-B. Standalone policies have seen an increase in the frequency of claims, rising from less than one claim per thousand policies in 2017, to 7.8 claims per thousand policies in 2020. Yet the intensity of SA claims generally decreased, dropping to $28,702 per claim in 2020. Even though the loss ratio for the PKG as a whole was poor in 2019 and 2020, there was a decrease in both the frequency and the impact of claims between those two years. Part of the explanation for this is that about a quarter of the companies had major losses due to defense costs unrelated to new claims; while about half of the companies had no claims losses or defense expenses at all. Possibly the latter was due to good luck or maybe good underwriting risk management on the part of the

insurers. Once again, first party claims far exceed third party claims indicating the likely impact of ransomware attacks.

Table 6.13: Performance of Healthcare-Specific Group #1 Insurers 2016 to 2020 (NAIC 2021)

Year	Standalone (SA) Direct Losses Incurred	SA Defense & Cost Control (DCC)	SA Loss Ratio with DCC	Package (PKG) Estimated Loss Paid & Reserve	PKG Defense & Cost Control (DCC)	PKG Loss Ratio with DCC	# SA Claims 1st Party	# SA Claims 3rd Party	Total # SA Claims	SA Claims to Policy Ratio	Average SA Claims Payment with DCC	# PKG Claims 1st Party	# PKG Claims 3rd Party	Total # PKG Claims	PKG Claims to Policy Ratio	Average PKG Claims Payment with DCC
2016	$579,832	$376,535	22.8%	$5,633,622	$4,189,954	52.2%	9	3	12	0.19%	$12,543	428	37	465	0.25%	$4,880
2017	-$795,257	$493,507	-20.3%	$7,666,117	$9,484,778	61.7%	4	1	5	0.08%	$80,018	999	143	1,142	0.60%	$8,999
2018	$217,961	$204,349	20.1%	$9,346,932	$8,415,625	59.9%	30	1	31	0.35%	$11,861	1,266	60	1,326	0.65%	$9,182
2019	$837,094	$535,732	34.6%	$12,160,267	$12,492,193	89.5%	45	2	47	0.45%	$40,725	1,172	84	1,256	0.60%	$16,647
2020	$2,376,503	$2,004,095	58.4%	$10,239,829	$14,167,938	80.4%	95	19	114	0.78%	$28,702	1,120	57	1,177	0.51%	$13,491

The second component of the NAIC dataset used to analyze healthcare-sector cyber insurance comes from the Betterley Reports – an annual survey of cyber insurance for the healthcare market conducted since 2017. The ***Betterley Cyber Insurance for Healthcare Market Survey- 2020 edition*** provides policy and coverage details from 181 insurers operated by twenty large cyber-insurance groups including AIG, AXA, Chubb, CNA, Travelers, and Zurich. These large groups wrote over 70 percent of the direct and estimated cyber insurance premiums in 2020. The report focuses on cyber insurance offerings for fourteen types of healthcare providers (e.g. hospitals, labs, etc.) and ten types of managed care organizations (e.g. health plans, etc.).

Like the overall industry and healthcare-specific component, Group #2's (Table 6.14) direct and estimated premiums grew substantially from 2017 to 2020, even though the actual number of cyber insurers stayed nearly the same. Average premium costs, especially for SA are much higher that the industry average, indicating that the SA insurers in particular cater to larger entities requiring higher levels of coverage and

service. The group also shows the soft market between 2018 and 2019 with declining average premium rates, and a sudden hardening with average premiums increasing substantially in 2020. Most striking is the decline in the number of PKG policies between 2019 and 2020, which is further evidence of the hardening market due to ransomware, as insurers and large–firm insureds turned to SA coverage with its more stringent underwriting standards and clearer policy language regarding cyber claims events.

Table 6.14: Market for Betterley Group #2 Cyber Insurers - 2016 to 2020 (NAIC 2021)

Year	Direct Standalone (SA) Premiums Written	Direct & Estimated Packaged (PKG) Premiums Written	Total Direct & Estimated Premiums Written	# SA Insurers	# PKG Insurers	Total # Cyber Insurers	# SA Policies	Average Premium per SA Policy	# PKG Policies	Average Premium per PKG Policy	Total # of Policies
2016	$808,917,949	$240,416,997	$1,049,334,946	52	91	143	51,175	$15,807	347,256	$692	398,431
2017	$848,626,832	$593,951,402	$1,442,578,234	60	118	178	56,959	$14,899	530,287	$1,120	587,246
2018	$952,941,663	$587,030,555	$1,539,972,218	56	113	169	60,371	$15,785	737,671	$796	798,042
2019	$1,023,046,476	$634,317,196	$1,657,363,672	61	121	182	76,018	$13,458	802,606	$790	878,624
2020	$1,215,494,399	$719,192,974	$1,934,687,373	59	122	181	84,826	$14,329	757,345	$950	842,171

The performance of the Group #2 (Table 6.15) mirrors that of the industry-wide review. Losses for both SA and PKG coverage have generally grown at a faster pace than premiums, though the group remained profitable between 2016 and 2019. Then in 2020, loss ratios for SA exceeded 70 percent and for PKG lingered just under 70 percent indicating that many of the group's insurers were in the red. In fact, nearly 20 percent of these cyber insurers lost money in 2020. The main factor was dramatic increases in claim severity, with average claims with DCC increasing for both SA and PKG by over 60 percent. In addition, the frequency of claims increased for PKG by 36.8 percent, while

SA, remained at a very high frequency of 88.3 claims per thousand policies. Again, ransomware attacks were likely the primary cause of these losses.

Table 6.15: Performance of Betterley Group #2 Cyber Insurers 2016 to 2020 (NAIC 2021)

Year	Standalone (SA) Direct Losses Incurred	SA Defense & Cost Control (DCC)	SA Loss Ratio with DCC	Package (PKG) Estimated Loss Paid & Reserve	PKG Defense & Cost Control (DCC)	PKG Loss Ratio with DCC	# SA Claims 1st Party	# SA Claims 3rd Party	Total # SA Claims	SA Claims to Policy Ratio	Average SA Claims Payment with DCC	# PKG Claims 1st Party	# PKG Claims 3rd Party	Total # PKG Claims	PKG Claims to Policy Ratio	Average PKG Claims Payment with DCC
2016	$247,350,358	$73,042,711	45.3%	$151,857,663	$10,663,221	77.1%	1,195	1,021	2,216	4.33%	$50,437	339	1,107	1,446	0.42%	$25,839
2017	$237,821,479	$43,111,911	37.3%	$110,268,292	$24,690,061	27.2%	1,768	1,394	3,162	5.55%	$59,178	1,202	923	2,125	0.40%	$28,258
2018	$332,998,304	-$23,329,353	35.1%	$215,017,106	$11,313,084	43.3%	2,746	1,644	4,390	7.27%	$59,116	1,926	1,392	3,286	0.45%	$42,556
2019	$438,648,206	$27,837,499	49.4%	$126,734,321	$107,158,062	41.0%	3,926	3,728	7,654	10.07%	$64,996	2,269	1,566	3,835	0.48%	$32,367
2020	$767,483,274	$51,950,286	75.4%	$272,533,880	$170,080,458	69.8%	5,214	2,277	7,491	8.83%	$109,348	3,197	1,754	4,951	0.65%	$51,960

The final component of the NAIC dataset consists of the other 450+ cyber insurers not in the other two components. While not specifically identified as serving the healthcare-sector, this component does contain large cyber specialty and reinsurance companies including Lloyds, Munich RE, Swiss RE, and Berkshire Hathaway. What makes this group unique is that several have recently either acquired or formed partnerships with InsurTechs to offer technology-enhanced cybersecurity underwriting and pre-breach cybersecurity assessment services. This component wrote about 28.3 percent of the direct and estimated cyber premiums in 2020.

As shown in Table 6.16, Group #3 has far more policies than either Group #1 or #2. This is especially true for PKG with nearly 75 percent of all packaged policies falling within this group. In terms of average premiums, SA average premiums are higher than Group #1 and lower than Group #2, indicating that the firms served are likely medium in sized. Conversely, for PKG, the average premiums are very low, indicating that the firms served are likely small in size.

Table 6.16: : Market for Other Group #3 Cyber Insurers – 2016 to 2020 (NAIC 2021)

Year	Direct Standalone (SA) Premiums Written	Direct & Estimated Packaged (PKG) Premiums Written	Total Direct & Estimated Premiums Written	# SA Insurers	# PKG Insurers	Total # Cyber Insurers	# SA Policies	Average Premium per SA Policy	# PKG Policies	Average Premium per PKG Policy	Total # of Policies
2016	$107,195,969	$172,866,479	$280,062,448	66	237	303	95,274	$1,125	1,426,523	$121	1,521,797
2017	$144,005,321	$240,456,121	$384,461,442	66	288	354	40,260	$3,577	1,779,820	$135	1,820,080
2018	$154,210,122	$281,013,830	$435,223,952	75	324	399	54,878	$2,810	1,932,381	$145	1,987,259
2019	$232,503,516	$326,710,918	$559,214,434	74	360	434	74,894	$3,104	2,164,397	$151	2,239,291
2020	$394,316,863	$385,834,892	$780,151,755	78	381	459	97,158	$4,059	2,833,582	$136	2,930,740

Examining the performance of Group #3 insurers (Table 6.17), both SA and PKG stayed profitable for the period 2016 to 2019, with PKG also staying profitable in 2020. Conversely, the SA loss ratio in 2020 grew significantly to over 75 percent, with both claims losses and DCC rising sharply. Both SA and PKG insurers seemed to manage the frequency and severity of claims better than the other two groups. Group #3 SA's claims-to-policy ratio increased from 22.8 to 44.3 per thousand, but this is much better than Group #2. Group #3's PKG claims-to-policy ratios were better than all groups including the industry-wide numbers with frequency ranging from 0.9 to 1.6 claims per thousand policies. Group #3's average claims payments were also lower than the industry average with average claims staying below $48,000 for SA and below $26,000 for PKG. Possibly this group's performance was aided by InsurTech assistance, or more probably by the fact that this group had smaller non-healthcare clients that suffered less from ransomware attacks. Still, Group #3's 2020 SA policy performance indicates that it was not immune from ransomware attacks or the continued litigation associated with these attacks.

Table 6.17: Performance of Other Group #3 Cyber Insurers – 2016 to 2020 (NAIC 2021)

Year	Standalone (SA) Direct Losses Incurred	SA Defense & Cost Control (DCC)	SA Loss Ratio with DCC	Package (PKG) Estimated Loss Paid & Reserve	PKG Defense & Cost Control (DCC)	PKG Loss Ratio with DCC	# SA Claims 1st Party	# SA Claims 3rd Party	Total # SA Claims	SA Claims to Policy Ratio	Average SA Claims Payment with DCC	# PKG Claims 1st Party	# PKG Claims 3rd Party	Total # PKG Claims	PKG Claims to Policy Ratio	Average PKG Claims Payment with DCC
2016	$25,344,242	$3,802,634	45.3%	$6,711,694	$950,519	5.3%	332	216	548	0.58%	$6,642	929	286	1,215	0.09%	$3,568
2017	$22,785,301	$7,226,441	37.3%	$52,902,879	$6,446,675	27.9%	656	262	918	2.28%	$13,735	1,461	335	1,796	0.10%	$16,016
2018	$34,510,634	$7,163,216	35.1%	$45,363,387	$4,045,926	19.9%	805	605	1,410	2.57%	$43,909	1,882	386	2,250	0.12%	$21,906
2019	$58,567,931	$7,141,786	49.4%	$95,822,844	$16,065,315	37.8%	1,693	554	2,247	3.00%	$17,541	2,884	562	3,442	0.16%	$16,654
2020	$149,583,756	$62,342,930	75.4%	$115,624,568	$5,466,247	35.5%	3,490	812	4,302	4.43%	$47,858	3,348	721	4,069	0.14%	$25,309

The reminder of this section will look at specific policy, coverage, underwriting mechanisms, and pre-/post-breach services that insurers use to manage cyber safety. This analysis focuses on one insurer in each of the three groups described above. Data on coverage, premiums, limits, deductibles, and risk services comes from the NAIC System for Electronic Rates & Forms Filings (SERFF). Appendix D gives a summary of the first and third party coverage for each insurer and Appendix E lists each insurer's pre-breach and post-breach value-added services. Appendix F provides an overview of the performance of each insurer.

The three insurers selected for in-depth examination of their cyber coverage and safety incentives include The Doctors Company (TDC) from Group #1, Tokio Marine Holdings (TMH) Group from Group #2, and Munich Re with its associated InsurTechs.

1. *The Doctors Company (TDC) Group*

The Doctors Company (TDC) Group is a physician-owned medical malpractice insurer consisting of two RRGs under the name The Doctors Company, and a specialty insurance company – TDC Specialty Insurance. In 2020, the TDC Group wrote 14% of Group #1's direct and estimated premiums and 5% of policies with an average premium of $478. Thus, most customers are SMEs. In 2018, TDC Specialty launched a standalone

cyber insurance product called CyberGuard® Plus for Healthcare Professionals. It targets "those healthcare providers and organizations that embrace and demonstrate a culture of compliance and risk management" (TDC 2020). Thus, unlike any other standalone cyber coverage, TDC's specifically addresses the unique exposures faced by healthcare organizations. Further, outside firms that specialize in healthcare cybersecurity matters provide their risk management, breach response, and risk mitigation services. The policy includes cyber-specific claims features, the ability to purchase additional coverage options, and limits up to $5 million.

Potential healthcare clients are required to be current TDC malpractice insurance customers. In addition to providing information for that insurance, they also need to fill out a detailed CyberGuard Plus application dealing specifically with their healthcare cyber exposures. Questions focus on regulatory compliance and how recently the firm conducted a HIPAA audit. It also asks about the number of patient records stored electronically, and whether records are encrypted while stored and when transmitted. They also ask about network system controls including the use of firewalls, anti-virus, intrusion detection, and multi-factor authentication; and whether the healthcare firm has policies for updating and patching software, procedures for testing network security controls, an incident response plan, and backup data and systems in case of an outage. The applicant must also provide information on business associates including cloud and other service providers, and state if they have contracts with these vendors requiring HIPAA compliance. They also ask about prior cyber insurance, incidents, and claims history.

The underwriting guidelines state that they are targeting clients that have detailed controls in place that help mitigate their risk of cyber incidents. Other key areas of consideration include compliance with HIPAA/HITECH, incident and claims history, in-force breach response plan, hardware and software used, and if vendor management policies are in place (TDC 2020).

According to TDC's Rules and Rates Manual filed with the State of California there are two core packages available: "Select" and "Premium" (TDC 2020A). Customizable limits and retentions are available within the Premium package. The standard limit for both packages is $1 million with a base deductible of $5000. Base premiums start at $1075 for Select and $1450 for Premium. Only Premium coverage has the right to purchase increased limits up to $5 million, and to buy increased sub-limits for business interruption. Both packages cover data breach response, breach notification, business interruption, extortion, cybercrime, regulatory defense and fines, and various types of data security, privacy and media liability (Appendix D). Premium optionally covers reputational income loss, property damage, and bodily injury caused by a cyber incident. Premium clients can also purchase optional coverage for certified acts of terrorism.

The premium charged depends on a number of ratings factors including the number of physicians covered by policy, the customizable limits, sub-limits, and deductibles, and specific risk profile and safety actions taken by the insured. Up to a 15 percent credit or debit can be applied to the annual premium for assessed level of preparedness, amount of PHI, use of encryption, compliance with privacy regulations, use of network intrusion detection and access controls, and overall perceived quality of cyber policies, procedures,

network security, and vendor management. The maximum premium credit/debit is 25 percent.

TDC provides its insureds access to value added pre-breach services at a discounted price through a panel of third-party vendors (Appendix E). These services include HIPAA compliance review and training, network security audits and assessments, crisis preparedness training, and incident response planning. Conducting these activities is then a factor in providing discounts.

All policies are claims-made with the typical policy term of one year. Clients also have the option of purchasing extended reporting up to three years. Based on the NAIC data, the performance of TDC's CyberGuard standalone product has been excellent over the first two years since its inception. Loss ratios with DCC both years are under 15 percent, indicating the product was highly profitable. Direct written premiums more than doubled as did the number of active policies, while the average premium decreased by 25 percent indicating that TDC was trying to grow the business through competitive pricing. However, in 2020 the frequency of claims increased six-fold and defense and cost containment (DCC) payments were significantly higher than claims payments. Yet while TDC Specialty Insurance performed well, the performance the Doctors Group as a whole did not. The Group experienced major losses in 2019 and 2020 at one of its RRGs, driven almost exclusively by DCC costs.

2. *Tokio Marine Holdings (TMH) Group*

Tokio Marine Holdings (TMH) Group, a Lloyds Syndicate member, consists of nine shareholder-owned insurance and specialty insurance companies selling a diversified

portfolio of both packaged and standalone cyber coverage. In 2020, TMH wrote 4% of Group #2's direct and estimated premiums and 6% of the policies with average annual premium of $1.650. TMH offers a general cyber insurance policy under the name NetGuard Plus, and a healthcare-specific cyber policy under the names e-MD® and MEDEFENSE® Plus. All policies have aggregate limits up to $10 million with a minimum deductible of $1000. The target market for the healthcare products are group practices, allied health facilities, hospitals, long-term care facilities mental health facilities and solo physicians. Clients range in size considerably from very small firms paying annual premiums of less than $150, to a few huge firms with specialty premiums averaging nearly $1 million a year.

TMH's first party and third party coverage (Appendix D) is similar to TDC Specialty with a few notable additions. E-MD and MedDefense include coverage for both first party and third party property damage including replacement of hardware due to system failures and malware "bricking" events that make computers untrustworthy. First party coverage also includes compensation for reputational harm, phishing fraud losses, and reimbursement of rewards leading to the capture of cyber criminals. Uncommon third party coverage includes payment of damages and related defense costs for bodily injury caused by a cyber event.

TMH's cyber application is similar in detail and healthcare specificity to TDC Specialty. However, TMC asks more detailed questions on the client's IT staffing, email controls, use of multifactor authentication and encryption, frequency of software

patching, phishing controls and training, vulnerability scanning, intrusion detection, and government HIPAA investigations.

When TMH finds a deficiency, it has partnerships with key cybersecurity vendors such as CrowdStrike to help clients implement next-generation anti-virus software, multifactor authentication, cloud data backup, etc.; and conduct risk assessments, HIPAA compliance reviews, phishing simulations, and penetration testing (Appendix E). While clients must pay for these services, the cost is at a TMH negotiated discount, and clients can get reduced premium rates if they implement certain security controls before the policy binds.

TMH's underwriting diligence in screening clients and assisting them in implementing pre-breach security controls seems to be paying off on its bottom line. For the period 2016 to 2019, the NAIC data shows that Tokio Marine Group as a whole was highly profitable with loss ratios including DCC of less than 36 percent (Appendix F). Even in 2020, when most other cyber insurers showed losses, TMH Group had a profit of nearly 20 percent. The NAIC data also shows that claims frequency actually decreased by nearly 75 percent between 2016 and 2020, slightly offset by a significant but manageable increases in claims severity. Most important, TMC and its clients avoided the spotlight, with no catastrophic claims during the entire period.

3. *Munich Re*

Munich Re consists of seven shareholder-owned insurance and specialty insurance companies selling a diversified portfolio of both packaged and standalone cyber coverage. In 2020, they wrote 2.2% of Group #3's direct and estimated premiums and

just 0.32% of policies, with an average premium $1,878 in 2020. Thus, their clients are similar in size to TMH Group.

While Munich Re's U.S. cyber insurance activity is relatively small, it is distinguished by a few unique attributes. First is the quality of Munich Re's U.S. presence. Munich Re's primary assets in the US are Hartford Steam Boiler (HSB) Inspection and Insurance Company, and HSB Specialty Insurance. Evidence from the nuclear insurance case study showed that HSB was at the forefront of developing inspections and standards for nuclear reactors and has a long history of requiring detailed risk assessments prior to extending insurance to emerging technologies. Second, Munich Re is the world's largest reinsurer of property and casualty policies with direct written premiums of over $23 billion in 2018. Subsequently, they are a major reinsurer of U.S. cyber insurance policies. Finally, Munich Re is actively pursuing partnerships with key technology companies such as Google, and investing in emerging InsurTechs like Zeguro and At-Bay - moves that will influence the evolution of cyber insurance in the future

In 2016, HSB introduced a new cyber insurance product Total Cyber™ - a claims-made standalone policy geared towards small- to medium-sized businesses and institutions that generate less than $100 million in annual revenue. When originally released the premiums rates for this program were developed "in the absence of data specific to this coverage" (HSB 2016). For early policies, HSB started with initial premiums based on the applicant's annual revenue or operating expenses (four tiers). These base premiums were then modified using factors for desired limits (up to $5 million), sub-limits on seven coverages offered (up to $500,000), requested deductibles

(up to $50,000), and the determined industry hazard (four classes), with the highest mark-up for entities that collect and store high volumes of sensitive data. The premium then was further adjusted using fifteen (15) individual risk factors associated with the insured's perceived level of cyber maturity, with up to ten percent premium credit or debit for each factor. Over the past five years, the rates and coverage have been modified numerous times based initially on competitive pressure, and later on the need to better account for the risks associated with certain industries. In the most recent update to rates in March 2021, hospitals and nursing homes had the highest risk factor, with a mark-up of 4.01 times the base rate (HSB 2021). This is actually an improvement from February 2020, when the mark-up was 15 times the base rate (HSB 2020). Other firms that collect and store high volumes of PHI had markups of from 3.01 to 12.65 over the same period.

Today, HSB's Total Cyber offers eight types of first party and third party coverage (Appendix D). The coverage itself is very similar to offerings from Tokio Marine. What is different is that they sell the coverage in modules, with each module having its own premium, customizable limits, sub-limits, deductibles and industry rating factors. The individual risk factors have been increased to twenty-one, with more emphasis on unusual exposers that might make the insured more vulnerable to ransomware attacks. There is also unique optional coverage such as covering the costs for a forensic accountant and for crypto-jacking events, and paying for improvements to the insured's computer system following a computer attack to mitigate future losses The overall aggregate limit has also been increased to $10 million.

The Total Cyber application is not healthcare specific, but does ask questions on medical records storage and HIPAA compliance. The questions asked address specifically the individual risk factors used to determine the premium. To provide risk management (Appendix E), HSB gives clients complimentary access to Zeguro's Cyber Safety™ - a cybersecurity solution that includes security training, assistance with creating security policies, and quarterly scans of the client's website for vulnerabilities. Zeguro also has a cybersecurity product targeted at the healthcare industry, focused on HIPAA compliance, and resells Total Cyber to healthcare firms.

During the first four years of Total Cyber's product availability, HSB and Munich Re's US cyber insurance business was highly profitable with group-wide loss ratios with DCC of less than 13 percent (Appendix F). However, in 2020, Munich Re Group was slightly unprofitable, driven primarily by losses at HSB Specialty. In 2020, HSB doubled its premiums written from the previous year, but the frequency and magnitude of losses also increased more than 50 percent.

In 2017, HSB began offering a second cyber insurance product called Cyber Suite™ - a turnkey product sold by other carriers, and reinsured by HSB. Over ten insurers in Group #3 sell Cyber Suite including Acuity, Westfield, Columbia, IMT, Prosight, and MSIG – all of which report separate cyber insurance results to NAIC. At least one Group #1 healthcare-specific cyber insurer, the Dentist Company Insurance Company (TDIC) also resells Cyber Suite. The product sells as a claims-made endorsement to existing insurer policies, has an average annual premium of $409, making it primarily targeted at small- to medium-sized firms.

Cyber Suites coverage and risk management services are similar to Total Cyber, but with much lower aggregate limits and sub-limits, and fewer risk tiers (Appendices F &G). Aggregate limits range from $50,000 to $1 million, deductibles ranging from $1,000 to $10,000, and sub-limits for cyber extortion, reputational harm, and identity recovery between $10,000 and $25,000. Healthcare entities are listed under Risk Tier 3, with average premium mark-ups of 25 percent. Like Total Cyber, Cyber Suite customers have access to Zeguro's Cyber Safety, and also NetDiligence's eRisk Hub® website with additional training and risk management tools.

Examination of HSB's multi-state filing memo indicates that Cyber Suite was highly profitable during its initial first two years of availability with loss ratios of less than 30 percent. Likewise, examination of the NAIC reports of over twenty Cyber Suite resellers shows universal profitability for the period 2018 to 2020, with all loss ratios including DCC below 35 percent.

In 2016, Munich RE and HSB helped launch At-Bay, an InsurTech with the goal of pairing cyber insurance with cyber risk management to create "insurance for the digital age" (At-Bay 2021). As a Managing General Underwriter (MGU), At-Bay underwrites and sells an enhanced version of HSB's Total Cyber, with coverage limits up to $10 million to firms with revenue up to $5 billion. In addition to Total Cyber's coverage capabilities, At-Bay's coverage includes comprehensive privacy coverage including violations under the EU's General Data Protection Regulation (GDPR), and endorsements to address specific exposures for the insured (At-Bay 2021). Yet, what makes At-Bay's coverage unique is that they provide security scans and active

monitoring of all client systems throughout the life of the policy, at no additional cost. If they identify a new vulnerability, they reach out with actionable measures to swiftly mitigate the risk (At-Bay 2021A). The goal is to prevent losses before they happen. As an MGU, At-Bay does not have to submit NAIC filings, so their cyber insurance performance is unavailable.

Finally, in March 2021, Munich RE announced a partnership with Google and Allianz Global Corporate & Specialty (AGCS) to offer cyber risk solutions to business customers of Google Cloud. The collaboration was designed to improve cyber insurance underwriting by drawing real-time security data from the cloud. Google Cloud users enrolled in Google's "Risk Protection Program" can access the cyber insurance component called Cloud Protection Plus +, which will insure U.S.-based clients against cyber events within their own corporate environment as well as incidents related to Google Cloud. The Risk Protection Program includes Risk Manager, a new tool that helps determine a customer's security risk posture on the cloud. Rather than general risk information gleaned through a more traditional underwriting process, Munich RE is now able to tap into Google Cloud's proprietary assessment tools to fuel more accurate underwriting and receive reports directly from clients via the Risk Manager tool. Thus, premium pricing and coverage can be directly tied to the client's unique risk profile (Munich RE 2021).

Thus, what you see from these groups is the recognition of the challenges underwriters face in dealing with the constantly evolving technology and cyber risks. Understanding the unique risks healthcare providers face allows them to offer better

coverage and more capacity, while increasing their profitability by reducing the frequency and severity of losses.

VII. Role of Insurance in Managing Cyber Safety (Evidence)

This section uses econometric modeling to examine the relationship between the take up of cyber insurance by U.S. healthcare sector entities and their management of cyber safety during the period 2015 to 2020. The analysis uses count panel data from the Healthcare Cyber Attack Database (HCAD). The panel consists of 15,144 observations from 2,524 healthcare entities over the six-year period. It is very strongly balanced with no missing data. The entities have been subdivided into 27 sub-entities (SUBCODE) representing all of the key healthcare provider types (e.g. Doctor, Hospital, etc.) and healthcare support companies (e.g. Admin, Medical Equipment). A list of summary statistics is given in Appendix G.

There are two key dependent variables representing cyber safety. The first is ***Attacks*** denoting the number (frequency) of cyber-attacks experienced by each entity, each year. The second is ***AttRec*** representing the number of records impacted (magnitude) by each attack, each year. Each attack in the dataset is rated as either being internal or external (EXTHACK), and if external, whether it involved ransomware (RANSOM).

The key independent variable is INSPOL10K which is the estimated number of insurance policies issued each year by sub-entity divided by 10,000. The estimate is based on the population of each sub-entity as derived from the 2018 U.S. Census Statistics of U.S. Businesses (SUSB 2018) times the take-up rates for policies by sector as determined by Marsh Analytics each year and used by the GAO in a May 2021 report

(GAO 2021). The dataset also includes indicator variables denoting if the firm is large with less more than 500 full time employees (FTE500), public or private (PUBorPRIV), and whether it is non-profit or for profit (NPFP).

The following sections detail the theory, observations, hypotheses and analytical analysis conducted on each dependent variable. In interpreting the results of each regression, **the key item to look at is the sign of each coefficient. A significant negative coefficient indicates the possible positive influence of insurance on cyber safety by reducing the frequency and magnitude of attacks.**

A. Theory, Observations, and Hypotheses

The literature review discusses how cyber insurance, in theory, can incentivize the insured to invest in their own cybersecurity through insurer premium discrimination and other mechanisms – clients that invest in their own cybersecurity are rewarded with lower premiums and better terms and conditions. Conversely, some scholars argue that cyber insurance can cause a moral hazard problem where clients, knowing they are insured, behave recklessly and actually reduce their investment in self-protection, believing insurance will offset any cyber-attack losses. For example, evidence suggests that cyber insurance covering ransomware attacks makes it more likely victims will pay the ransom, and hackers will target clients with insurance for that reason.

The literature and data from HCAD also suggests that certain types of healthcare entities might benefit more from cyber insurance than others. In this dissertation, it is hypothesized that small healthcare sector firms with less than 500 employees might benefit more from cyber insurance safety incentives than larger firms. Further, many

public sector entities (e.g. government) fully or partially self-insure. Thus, it is hypothesized that private for-profit firms are more likely to be influenced by cyber insurance than public non-profit/not for profit entities. Based on the above description, the following hypotheses will be tested:

H1: Cyber insurance will have a small but significant impact on reducing the frequency & magnitude of cyber-attacks against healthcare sector entities

Given the growth in the number of cyber-attacks over the period 2015 to 2021, it is not unexpected that cyber insurance might have a negative impact on the frequency and magnitude of cyber-attacks for some firms under certain circumstances such as ransomware attacks.

H2: Cyber insurance will have a more significant impact on reducing the frequency & magnitude of cyber-attacks against small private healthcare firms vs. large and/or public sector entities

Small healthcare firms include individual practitioners such as doctors and dentists, most group practices, and business associates including administrative, suppliers, and diagnostic testing companies (e.g. labs, imaging, etc.). Large healthcare entities include health systems, insurers, hospitals, and those operated by local, state, and federal governments.

H3: Cyber insurance will have a more significant impact on reducing the frequency of non-ransomware and internal cyber-attacks than on ransomware and external hacks.

We test our hypotheses empirically using Poisson regression and negative binomial regressions.

B. Poisson Regression & Frequency of *Attacks*

The attack count data is Poisson distributed with values each year ranging from zero to five. Tests were conducted using, if appropriate, ***xtpoisson*** with fixed-effect (FE), random effect (RE) and the "pooled" xi: Poisson models, with normal and robust standard errors (SE). Once again, the sign (+/-) of the coefficients is of particular interest indicating if insurance significantly increases (+) or decreases (-) the log likelihood of ***Attacks*** holding other variables constant.

The first model looks only at the interaction of *Attacks* and the primary independent variable INSPOL10K using FE, RE, xi: Poisson, with normal and robust SE.

Table 6.18 (Model #1): Regression of Attacks & INSPOL10K

Attacks	(1) xtpois_FE1	(2) xtpois_FE1 Robust	(3) xtpois_RE1 Normal	(4) xtpois_RE1 Robust	(5) xipois1	(6) xipois1 Robust
INSPOL10K	0.2560149***	0.2560149***	-0.0145530***	-0.0145530***	-0.0145530***	-0.0145530***
	(0.0348301)	(0.0338250)	(0.0038775)	(0.0019081)	(0.0038775)	(0.0037604)
_cons			-1.5695750***	-1.5695750***	-1.5695603***	-1.5695603***
			(0.0236511)	(0.0172327)	(0.0236509)	(0.0234950)
lnsig2u			-1.537e+01	-1.537e+01		
			(10.4538921)	(.)		
Wald chi2	54.03***	57.29***	14.09***	58.17***	14.42***	14.98***
Deg of Free	1	1	1	1	1	1
# of Obs	15,144	15,144	15,144	15,144	15,144	15,144

Standard errors in parentheses
* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

As shown in Model #1, all coefficients for INSPOL10K are small but significant; however, coefficients for the FE models are positive, vs. negative coefficients for RE and xi: Poisson models. A Hausman test of the FE versus RE models soundly rejected the null that the RE model was the better model. Thus, for this regression, we will use the FE model with robust standard errors that controls for heteroscedasticity. The Pearson

Goodness of Fit soundly fails to reject the null hypothesis of a good-fitting model – indicating a good fit. The VIF shows a mean value of "1" indicating no collinearity.

The second model includes the time-invariant NPFP indicator dummy variable with "0" equaling nonprofit and "1" indicating for profit. The introduction of a time-invariant dummy variable makes FE modeling inappropriate. The remaining analyses with dummies will use RE and pooled xi: Poisson modeling with normal and robust SE. As shown in Model #2, like Model #1, all coefficients for INSPOL10K are small, significant; with negative coefficients for all RE and xi: Poisson models. The NPFP coefficients are all negative and significant. The alpha test included with the RE regression indicates that the RE regression is the same as the pooled regression. This is further confirmed by the Hausman test and visual observation. The Pearson Goodness of Fit soundly fails to reject the null of a good fitting model – indicating a good fit. The mean VIF of 2.06 indicates no collinearity between the INSPOL10K and NPFP variables. These results support Hypothesis #1 and the for-profit aspects of Hypothesis #2.

Table 6.19 (Model #2): xtpoisson/xi: Poisson Regression of Attacks, INSPOL10K and NPFP

Attacks	(1) xtpois_RE2	(2) xtpois_RE2 Robust	(3) xipois2	(4) xipois2 Robust
INSPOL10K	-0.0106572**	-0.0106572***	-0.0106571**	-0.0106571**
	(0.0043185)	(0.0025620)	(0.0043184)	(0.0041991)
NPFP	-0.0852221**	-0.0852221***	-0.0852263**	-0.0852263**
	(0.0412532)	(0.0287743)	(0.0412529)	(0.0402187)
_cons	-1.5357025***	-1.5357025***	-1.5356862***	-1.5356862***
	(0.0285186)	(0.0178159)	(0.0285184)	(0.0281255)
/ lnsig2u	-1.537e+01 (10.4566065)	-1.537e+01 (.)		
Wald chi2	18.49***	83.20***	18.69***	19.77***
Deg of Free	2	2	2	2
# of Obs	15,144	15,144	15,144	15,144

Standard errors in parentheses
* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

The third model introduces the PUBorPRIV time invariant dummy variable where "0" equals public and "1" equals private, along with dropping ransomware attacks (RANSOM==0).

Table 6.20 (Model #3): xtpoisson Regression of Attacks, INSPOL10K and PUBorPRIV (RANSOM==0)

Attacks	(1) xtpois_RE3	(2) xtpois_RE3 Robust	(3) xipois3	(4) xipois3 Robust
INSPOL10K	-0.0196940***	-0.0196940***	-0.0196941***	-0.0196941***
	(0.0044837)	(0.0025125)	(0.0044837)	(0.0044671)
PUBorPRIV	-0.1057702*	-0.1057702**	-0.1057726*	-0.1057726*
	(0.0611004)	(0.0440730)	(0.0610999)	(0.0603633)
_cons	-1.6143537***	-1.6143537***	-1.6143398***	-1.6143398***
	(0.0551466)	(0.2615386)	(0.0551463)	(0.0542561)
lnsig2u	-1.401e+01	-1.401e+01		
	(8.7745868)	(6.046e+05)		
Wald chi2	27.83***	84.21***	28.42***	28.58***
Deg of Free	2	2	2	2
# of Obs	14,643	14,643	14,643	14,643

Standard errors in parentheses
* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

The results in Model #3 show better insurance performance vs. non-ransomware attacks with an increasing negative coefficient for INSPOL10K , and negative coefficient for PUBorPRIV. For Model 3, the alpha test included with the RE regression indicates that the RE regression is the same as the pooled regression. This is further confirmed by the Hausman test and visual observation. The Pearson Goodness of Fit soundly fails to reject the null of a good fitting model – indicating a good fit. The mean VIF of 1.84 indicates no collinearity between the INSPOL10K and PUBorPRIV variables. These results support Hypothesis #1 and the non-ransomware aspects of Hypothesis #3.

The fourth model includes both the PUBorPRIV and NPFP time invariant dummy variables along with the removal of external attacks (EXTHACK==0) – thus for internal

breaches only. The results in Model #4 show better insurance performance vs. internal attacks with an increasing negative significant coefficient for INSPOL10K , and significant negative coefficient for PUBorPRIV in all but the xi: Poisson robust model.

Table 6.21 (Model #4): xtpoisson/xi: Poisson Regression of Attacks, INSPOL10K, PUBorPRIV & NPFP (EXTHACK==0)

Attacks	(1) xtpois_RE4	(2) xtpois_RE4 Robust	(3) xipois4	(4) xipois4 Robust
INSPOL10K	-0.0382912***	-0.0382912***	-0.0382912***	-0.0382912***
	(0.0076277)	(0.0074127)	(0.0076277)	(0.0076013)
PUBorPRIV	-0.1619426*	-0.1619426*	-0.1619425*	-0.1619425
	(0.0973649)	(0.0866145)	(0.0973651)	(0.0991927)
NPFP	0.0606222	0.0606222	0.0606221	0.0606221
	(0.0730072)	(0.0745438)	(0.0730074)	(0.0746592)
_cons	-2.2798263***	-2.2798263***	-2.2798303***	-2.2798303***
	(0.0815520)	(0.1308330)	(0.0815521)	(0.0834665)
lnsig2u	-1.120e+01	-1.120e+01		
	(11.6050949)	(1.470e+04)		
Wald chi2	33.89***	44.21***	35.70***	34.22***
Deg of Free	3	3	3	3
# of Obs	13,314	13,314	13,314	13,314

Standard errors in parentheses
* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

For Model 4, the alpha test included with the RE regressions indicates that the RE regression is the same as the pooled regression but with less significance. This is further confirmed by the Hausman test and visual observation. However, in this model, the Pearson Goodness of Fit rejects the null, indicating a less robust model. The mean VIF of 2.95 indicates no collinearity among the INSPOL10K, PUBorPRIV and NPFP variables. These results support Hypothesis #1 and the internal attack aspects of Hypothesis #3.

The next model takes the variables from Model #1 with SUBCODE factors.. Also the time invariant dummy variable FTE500 has been added with “0” indicating small firms of less than 500 employees, and “1” indicating large firms with more than 500 employees. The Federal Government (SUBCODE=1) was used as the control since it is

the only sub-entity with no cyber insurance. This allows a comparison of sub-entities with insurance to be compared to one without. A series of regressions was then conducted to determine the best mix of significant sub-entity coefficients using RE and xi: Poisson with both normal and robust standard errors. The results are shown in Model #5. It shows significant negative coefficients for many small healthcare entities including doctors, dentists, group practices, as well as administrative business associates and small community support organizations. Conversely, large organizations, including health systems, health insurers, and state government health agencies have significant positive coefficients. The Pearson Goodness of Fit failed to reject the null indicating a good fitting model. The mean VIF of 5.56 indicates no collinearity between the INSPOL10K, and the rest of the selected dummy variables. The model was run using clustered standard errors, and there is no sign of autocorrelation. These results support Hypothesis #1 and Hypothesis #2.

Table 6.22 (Model #5): xtpoisson Regression with Attacks, INSPOL10K & other Subcode Variables

Attacks	(1) xtpois_RE6	(2) xtpois_RE6Rob	(3) xipois6	(4) xipois6Rob
INSPOL10K	0.0780954***	0.0780954***	0.0780643***	0.0780643***
	(0.0154693)	(0.0099031)	(0.0154701)	(0.0129064)
Admin	-0.8526935***	-0.8526935***	-0.8523808***	-0.8523808***
	(0.1779414)	(0.1057389)	(0.1779476)	(0.1517559)
Community	-0.7437407***	-0.7437407***	-0.7435210***	-0.7435210***
	(0.1767545)	(0.0900840)	(0.1767592)	(0.1591608)
Dentist	-0.2700887**	-0.2700887***	-0.2700370**	-0.2700370**
	(0.1139428)	(0.0273816)	(0.1139432)	(0.1050755)
Doctor	-0.5278895***	-0.5278895***	-0.5277390***	-0.5277390***
	(0.1361763)	(0.0530006)	(0.1361785)	(0.1225008)
GroupPrac	-0.9331135***	-0.9331135***	-0.9328012***	-0.9328012***
	(0.1714554)	(0.1060371)	(0.1714620)	(0.1467063)
HealthSys	0.2925423***	0.2925423***	0.2925031***	0.2925031***
	(0.0604199)	(0.0422440)	(0.0604202)	(0.0589472)
Insurer	0.2866264***	0.2866264***	0.2865875***	0.2865875***
	(0.0632353)	(0.0571954)	(0.0632355)	(0.0632248)
StateGov	0.3494125***	0.3494125***	0.3493770***	0.3493770***
	(0.1235508)	(0.0883768)	(0.1235509)	(0.1178908)
_cons	-1.7429185***	-1.7429185***	-1.7428773***	-1.7428773***
	(0.0359279)	(0.0190010)	(0.0359284)	(0.0325040)
lnalpha	-1.614e+01	-1.614e+01***		
	(79.4234999)	(0.2900843)		
Wald chi2	68.63***	42126***	68.46**	81.29***
Deg of Free	9	9	9	9
# of Obs	15144	15144	15144	15144

Standard errors in parentheses
* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

C. Negative Binomial Regression and *AttRec*

The second group of models looks at the impact of cyber insurance on the magnitude of cyber-attacks as measured in records compromised per attack (***AttRec***). As shown in the descriptive statistics, ***AttRec*** is extremely dispersed with some extreme outliers for the Anthem attack in 2015 (79 million records) and the AMCA breach in 2019 (24.4 million). Like the first set of models, we begin simple and then add variables looking

eventually at the impact on individual healthcare sub-entities. Robust standard errors are not allowed in xtnbreg.

The first model looks only at the interaction of *AttRec* and the primary independent variable for number of insurance policies (INSPOL10K) using FE and RE. As shown in Model #6, all coefficients for INSPOL10K are significant and negative indicating the correlation of insurance in reducing the log likelihood magnitude of attacks holding other variables constant. The Hausman test rejects the null indicating that the FE model is best. These results support Hypothesis #1.

Table 6.23 (Model #6): Regression of AttRec & INSPOL10K

	(1)		(2)	
AttRec	xtnbreg_FE1	Std. Error	xtnbreg_RE1	Std. Error
INSPOL10K	-0.0962745***	(0.0139400)	-0.0095881**	(0.0039634)
_cons	-5.5401232***	(0.0680318)	-4.0539940***	(0.0257737)
ln_r			0.2477516**	(0.1028075)
ln_s			12.4440442***	(0.1882828)
Wald chi2	47.70***		5.85**	
Deg of Free	1		1	
# of Obs	15,144		15,144	

Standard errors in parentheses
* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

The second model includes the PUBorPRIV and NPFP indicator variables. Once again it is analyzed using FE and RE. As shown in Model #7, like Model #6, the coefficient for INSPOL10K is small, significant and negative. The PUBorPRIV and NPFP variables are also both significant and negative. The Hausman test rejects the null and indicates the FE model is best. This result supports Hypothesis #1 and the private, for-profit aspects if Hypothesis #2.

Table 6.24 (Model #7): Regression of AttRec, INSPOL10K, PUBorPRIV & NPFP

	(1)		(2)	
AttRec	xtnbreg_FE2		xtnbreg_RE2	
INSPOL10K	-0.0662806***	(0.0152981)	-0.0056194	(0.0044408)
PUBorPRIV	-0.2940175*	(0.1540715)	-0.0487711	(0.0629069)
NPFP	-0.5999279***	(0.1384333)	-0.0690262	(0.0454817)
_cons	-5.1039204***	(0.1268050)	-3.9867015***	(0.0542835)
/				
ln_r			0.2476588**	(0.1027854)
ln_s			12.4436648***	(0.1882310)
Wald chi2	79.65***		10.12**	
Deg of Free	3		3	
# of Obs	15,144		15,144	

Standard errors in parentheses
* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

The next model takes the variables from Model #7 using INSPOL10K with SUBCODE factor. Also the time invariant dummy variable FTE500 has been added with "0" indicating small firms of less than 500 employees, and "1" indicating large firms with more than 500 employees. A series of xtnbreg regressions was then conducted to determine the best mix of significant sub-entity coefficients using FE and RE. The results in Model #8 show that INSPOL10K has turned slightly significantly positive but with many sub-entities having significant negative coefficients. The FTE500 is also significant and positive, indicating that larger firms may not benefit from the insurance safety effect. The results also show significant negative coefficients for small healthcare entities Group Practices and Administrative business associates for the FE and RE models. Conversely, in the FE and RE models large organizations, including health systems, health insurers, and state government health agencies have significant positive coefficients. The Hausman test again rejects the null indicating that the FE model is most appropriate. This result supports Hypothesis #1 and Hypothesis #2.

Table 6.25 (Model #8): xtnbreg of AttRec, INSPOL10K, FTE500 & Key SUBCODEs

	(1)		(2)	
AttRec	xtnbreg_FE4	Std. Error	xtnbreg_RE4	Std. Error
INSPOL10K	0.0855002***	(0.0216227)	0.0188771*	(0.0098754)
FTE500	1.6434251***	(0.1730088)	0.1681443***	(0.0447698)
Admin	-2.1651535***	(0.7376662)	-0.2177803*	(0.1278938)
GroupPrac	-1.4332480***	(0.3763178)	-0.1697997	(0.1082599)
HealthSys	0.6821811***	(0.1628501)	0.1419433**	(0.0661939)
Insurer	0.9867796***	(0.1677125)	0.1862354***	(0.0662166)
StateGov	0.9516269***	(0.2589632)	0.2494283*	(0.1311285)
_cons	-7.2657141***	(0.1714492)	-4.2367068***	(0.0404066)
ln_r			0.2543000**	(0.1029887)
ln_s			12.4555124***	(0.1880871)
Wald chi2	213.39***		44.35***	
Deg of Free	7		7	
# of Obs	15,144		15,144	

Standard errors in parentheses
* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

The results of these eight models all support the three hypotheses. In addition, like the other case studies, they also support the overall dissertation hypothesis that "Insurance can improve the safety posture of firms engaged in emerging technologies".

VIII. Lessons Learned & Recommendations

So, what does the HCAD and NAIC data and these experiences teach us about the role insurance plays in helping to manage healthcare cyber safety, and what lessons learned can be applied to managing cyber risks associated with other sectors and other emerging technologies?

Lesson #1: Value of Mandatory Breach Reporting is Applicable to Other Sectors

The ability to create the HCAD database came as a result of passage of HIPAA and HITECH regulations and the subsequent requirements that covered entities report privacy breaches to DHHS. Over the past decade, Congress has repeatedly debated but failed to pass mandatory breach reporting for most other sectors. Even though cyber-attacks are

constantly evolving, there is value in having historical data that can be analyzed by policy makers, technologists and scholars to better understand cyber-attack trends and consequences.

Recommendation: *Congress should pass a mandatory breach reporting laws that apply to other sectors and, like DHHS and the OCR breach portal, make these reports publicly available.*

Lesson #2: Size & Type of Healthcare Insured Matters in Insurance Safety Benefits

As discussed in Section VI.A and shown in Table 6.6, Healthcare is a sector predominately composed of SMEs, with greater than 98.5% of private healthcare firms having less than 500 employees. Conversely, per Table 6.9, nearly half of HCAD cyber-attacks (2015 to 2020) struck large firms including health systems, health plans and hospitals. SMEs generally have less exposure to cyber-attacks than large businesses but have greater vulnerability due to less advanced cybersecurity investments. Despite this vulnerability, based on NAIC evidence SMEs, including individual practitioners and ambulance services suffer far fewer breaches per capita and likely benefit more from cyber insurance risk management services than larger firms.

Recommendation: *Cyber insurance can incentivize SMEs to implement basic cybersecurity tools such as antivirus, firewalls, and encryption, necessary to prevent most cyber breaches.*

Lesson #3: Insurance Coverage and Risk Management Tailored to Healthcare Firm Needs

Evidence from the NAIC data suggests that cyber insurers that tailor their coverage and risk management services to their healthcare client needs may benefit with lower loss

ratios and higher profitability. Insurers with existing policies with healthcare clients through malpractice insurance, like TDC, may better understand healthcare-sector risks. Betterley Group insurers like Tokio Marine, with a healthcare-specific product and incentives for implementing pre-breach security controls kept their group profitable where other groups like were not. Munich RE and HSB maintain client safety and their own profitability by focusing on SMEs, tweaking coverage and premiums to meet the current risk environment, and investing in firms, products and partnerships to allow them to constantly assess a client's risk posture in real time.

Recommendation: *Understanding healthcare risks, providing healthcare-specific products, and investing in pre-breach scrutiny may increase health firm cyber safety and insurer profitability.*

Lesson #4: Insurers Can Underestimate Cyber Risk Exposing Themselves to Losses

The NAIC data shows that over the period 2016 to 2020, cyber insurance, in general was a highly profitable business. The number of insurers offering coverage grew tremendously, and for much of the period the market was described as "soft" with insurers often competing on price without a clear understanding of the risk. Even during the good years, 2016 to 2019, between 5.3 and 8.5% of all cyber insurance companies lost money, with between 2 and 10 insurers each year experiencing catastrophic losses of over 500 percent. During 2020, the market hardened considerably, as profit margins shrunk and nearly 13% of cyber insurers lost money. In June 2021, insurance rating company A.M. Best described the U.S. cyber insurance market as "grim," stating some insurers "may have bitten off more than they can chew" (Ayers 2021)

Recommendation: *The 2016 to 2019 cyber market resembled the "Gold rush" market for environmental liability insurance (ELI) prior to Love Canal. Insurers need to evaluate how they manage cyber risk from pricing to modeling to risk selection. Otherwise, they may face a collapse similar to what happened to ELI during the 1980s.*

Lesson #5: Insurers Must Help Healthcare Clients Adapt to Evolving Cyber Risk

Evidence from the NAIC data and the regression analysis indicates that insurers may have helped smaller healthcare firms adapt to internal non-ransomware attacks with the frequency and magnitude of these attacks diminishing over time. However, the recent wave of ransomware attacks with associated business interruption, extortion payments, privacy data leaks, and double extortion caught both insurers and their clients off guard. Many cyber insurers lost money in 2020, and a few were forced to withdraw from the market.

Recommendation: *In order to remain profitable, insurers need to help clients adapt to evolving cyber risks via education in pre-breach prevention and post-breach mitigation best practices.*

IX. Conclusions

This case study examined the role that insurance plays in promoting cyber safety and managing cyber risks for firms involved in healthcare services in the United States.

The primary contribution of this case study is the creation of a new Healthcare Cyber Attack Database (HCAD) that documents over 5600 cyber-attacks against U.S. healthcare entities covering the period 2005 to 2021 (Appendix A). Much of the HCAD data came

from the OCR and state breach reporting sites resulting from the passage of mandatory breach reporting laws.

HCAD documents the frequency, type, and magnitude of healthcare-sector cyber-attacks. An econometric analysis of the HCAD data over the period 2015 to 2020 revealed several key findings. First, cyber insurance can have a small but significant impact on healthcare-sector cyber safety as measured in both frequency and magnitude of cyber-attacks. This correlation is more pronounced in smaller, for-profit private healthcare firms such as individual and group practices than in larger, not-for-profit public entities such as government-operated facilities and health plans. HCAD quantitative evidence also indicated that cyber insurance currently may be more effective in helping firms manage non-ransomware, internal attacks than external hacks.

HCAD also contains additional data on ransomware attacks (Appendix B), cyber-attack litigation (Appendix C), and cyber insurance policy performance (Appendix F), coverage (Appendix D), and risk management capabilities (Appendix E). This data provided additional evidence of the evolution of cyber-attacks, and the frequency and magnitude of cyber-attacks against 27 healthcare entities from both the demand- and supply-side of the cyber insurance marketplace. What it shows is that many political economic factors play a major role in motivating healthcare entities to buy cyber insurance and implement cyber safety best practices.

Future plans are to enhance the HCAD to include complete 2021 cyber-attack data. In addition, a series of FOIA requests have been submitted to DHHS requesting access to breach reports involving less than 500 records, audit and breach investigation reports, and

other actions taken by DHHS in response to HIPAA consumer complaints. Ultimately, the goal is in to identify linkages between the NAIC policy performance data and specific HCAD healthcare cyber-attacks. Another future research goal is to use this enhanced data to explore the interaction of cyber insurance with regulation and litigation in managing cyber and other emerging risks.

Chapter 7: Cross-Case Study Analysis & Conclusions

I. Introduction

This dissertation explored the role that public and private insurance mechanism played in helping to regulate, promote safety and manage risks for firms involved in the use of emerging technologies. It utilized a mixed-methods multiple comparative case study approach to explore the key research question: ***"How can insurance promote better safety in emerging technological regimes?"*** This research employed both qualitative and quantitative methods, to explore how insurance promotes better safety in three emerging technologies: 1) nuclear risk at U.S. commercial nuclear power plants, 2) environmental risk at U.S. chemical and waste disposal facilities, and 3) cyber risk in the U.S. health care sector. This final chapter summarizes and compares the three case studies, provides key findings and recommendations, discusses the policy implications and recommendations, and suggests areas for future research.

II. Cross-Case Study Comparative Analysis

The case studies in Chapters Four, Five, and Six explored how public and private insurance mechanisms can promote better safety in three emerging technologies. American social scientist Robert Yin in his book *Case Study Research Design and Methods 4th Edition* (2009) recommends that researchers develop a strategy for analyzing

case studies (Yin 2009, pp.127-130). Four general strategies he recommends include organizing a case description, relying on theoretical propositions, examining rival explanations, and using both qualitative and quantitative data (when available) (Yin 2009, pp. 130-136). As part of this strategy, he suggests that the researcher put the data into different arrays, making a matrix of categories and placing evidence within each category (p. 129). He also suggests that for cross-case synthesis, the researcher should create tables using key coding words following a uniform framework (p. 156) and also consider chronologies (p. 148) and time-series analysis (pp. 144-149) when appropriate. Use of cross-case analysis strengthens external validity, making the results more generalizable to other emerging technology domains.

The comparative analysis below uses all four strategies. NVivo and Microsoft Excel spreadsheets were used to code the qualitative and quantitative data from multiple sources, establishing a chain of evidence that provides construct validity, and reliability that the results can be replicated. Following a descriptive analysis that includes a chronology of key events that impacted the development of insurance in each regime, the analysis proceeds relying on the primary theoretical proposition developed in the literature review and used in each case study - the Insurance Framework. A matrix is developed for the theoretical proposition. The insurance framework is then used to examine and compare the insurance development and coverage in each case study regime. Next, a matrix allows cross-case comparison of the key word dependent variable "safety" and its correlation with key independent variable "insurance" and two rival explanatory variables: "regulation" and "litigation." Other key words including

information gathering, audit, risk assessment, event, and safety measures are also explored within each matrix. Finally, the analysis concludes with a comparative examination of the quantitative data from each case study.

A. Cross-Case Study Comparative Description and Chronology

Table 7.1 provides a descriptive comparison of the three case studies, and a chronology of key events that shaped each regime's insurance development. The unit of analysis for each case study is the operational locations of case study firms. Commercial nuclear power plant sites with one or more reactors; treatment, storage, and disposal facilities (TSDFs) for waste companies; and the offices of healthcare providers and their business associates. As previously noted, the population of entities for each case study varies considerably from around a hundred reactors on about 50 sites, to a couple of thousand TSDFs, to over 750,000 healthcare entity offices.

Table 7.1: Descriptive Comparison & Chronology of Three Case Studies

Description & Chronology	Commercial Nuclear Power	Hazardous Waste Disposal	Healthcare Cyber
Unit of Analysis	Commercial Nuclear Power Plant Reactor Sites	Treatment, Storage & Disposal Facilities (TSDFs)	Healthcare Sector Firms
Population of Units	98 Reactors on 58 sites (2019)	1808 TSDFs (2020)	784,626 Firms (2018)
Period of Study	1954 to present	1970 to present	1997 to present
Initializing Legislation	Atomic Energy Act of 1954	National Environmental Protection Act (1970)	Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Insurance Legislation Trigger	Price Anderson Act (1957)	Resource Conservation and Recovery Act (RCRA) (1976/1982)	Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Primary Regulator	Atomic Energy Commission (AEC) (1946-1975) Nuclear Regulatory Commission (NRC) (1975 to present)	Environmental Protection Agency (EPA) (1970 to present) State EPAs	Department of Health & Human Service (DHHS) Office of Civil Rights (OCR) State Regulators
First Insurance Policy	Yankee Rowe (1960) NELIA/NEPIA	Environmental Impairment Liability (EIL) Howden-Snow Group (1974)	International Computer Security Association (ICSA) @1997
Most significant US Event	Three Mile Island (1979)	Love Canal (1978)	Anthem (2015)
Other significant events	SL-1 “Prompt Critical” (1961)	Donoro Smog (1948)	Popp AIDS Ransomware (1989)
	Fermi I (1967)	The Great Smog in London (1952)	Love Bug (2000)
	Brown's Ferry Fire (1975)	Rachel Carson's Silent Spring (1962)	California Database Breach Notification Security Act (2003)
	Institute of Nuclear Power Operations (INPO) founded (1979)	SS Torrey Canyon (1967)	Health Information Technology for Economic and Clinical Health Act (HITECH) (2009)
	Mandatory Property Coverage (1980)	Santa Barbara Oil Spill (1969)	Hollywood Presbyterian Medical Center Ransomware (2016)
	Chernobyl (1986)	SuperFund Act (1980)	WannaCry Ransomware (2017)
	9/11 Terrorist Attacks (2001)	Exxon Valdez (1989)	NotPetya Ransomware (2017)
	Fukushima (2011)	Deepwater Horizon Oil Spill (2010)	Universal Health System (2020)

Notably, each regime’s period of study started with a significant piece of federal legislation. The passage of the Atomic Energy Act of 1954 created the opportunity for commercial nuclear power, immediately triggered debate on the need for insurance and the subsequent passage of the Price-Anderson Act of 1957. Likewise, the National Environmental Protection Act of 1970 created the EPA, and subsequently led to the

passage of the RCRA in 1976, requiring all TSDFs have financial protection by 1982. The enactment of HIPAA in 1996 led to the immediate recognition of the need for cyber insurance by healthcare entities, and a demand for policies soon after. All three regimes had federal and state regulatory agencies gathering data, publishing standards and safety policies, and in varying degrees issuing monetary penalties for violations.

All three regimes also experienced multiple major events that impacted insurance coverage and altered the regime's definition of safety. For example, the commercial nuclear power regime experienced the Three Mile Island (TMI) event that led to many changes. These changes included hundreds of lawsuits, new NRC regulations, the creation of a new nuclear safety standards body (INPO), and the realignment of the nuclear insurance coverage with new mandatory property insurance and the phasing out of the government liability backstop, replacing it with retrospective coverage where all reactor owners pay for a major accident. Likewise, Love Canal (1979), the passage of the Superfund Act (1980), enforcement of required financial protection under RCRA (1982), and the discovery of hundreds of other environmental disaster sites ignited both litigation and intense demand for environmental insurance. The Anthem cyber-attack in 2015 with over 79 million records compromised and other massive attacks during healthcare's "Year of the Breach," and the emergence of ransomware attacks in 2016 and beyond, drove increased demand for cyber insurance by healthcare-sector companies.

Each case study also identified other significant national and international events from Chernobyl and Fukushima, to Exxon Valdez and Deepwater Horizon, to WannaCry and NotPetya. These events triggered regulator reassessments of safety, firm demand for

insurance, and insurer concerns about insurability and the need for adequate risk appropriate underwriting.

B. Insurance Framework and Emerging Technologies

As outlined in the literature review, one way that emerging technologies deal with these risks is to transfer a portion of it to private insurers and other insurance entities such as captives, risk retention groups and retrospective risk pools. These insurance entities, in turn, often spread the risk further by giving a portion to private reinsurers, retrocession firms, sidecar reinsurance companies, or by creating alterative financial mechanism such as insurance-linked securities and catastrophe bonds. Under extreme risk conditions where the insurance markets fail, governments may intervene to provide backstop reinsurance to cover potentially catastrophic losses, such as occurred with the passage of TRIA following 9/11.

As outlined in Table 7.2 below, many of these insurance framework mechanisms were used by the three emerging technologies in their quest to acquire adequate coverage, and by insurers to obtain sufficient capital to cover potentially catastrophic losses.

Commercial nuclear power has made the most extensive use of this framework. Initially under the Price-Anderson Act of 1957, the insurance industry and federal government established an arrangement where insurers formed large pools involving hundreds of insurance companies to provide $60 million in liability and $65 million in property coverage, and the federal government provided $500 million in backstop liability reinsurance. All licensees operating facilities with a rated capacity of 100 Mw or more were required to have the maximum amount of liability protection available ($560

million). The government's goal was to eventually phase out the reinsurance and have it replaced with coverage provided by private insurers and the licensees. The problem was that commercial nuclear power grew very slowly, while the risk of a catastrophic loss grew substantially. Estimates from the Brookhaven Report and other studies indicated that a maximum possible loss would far exceed available coverage.

Eventually, with Congressional approval, the operators came up with a retrospective plan for both liability and property indemnity, where all operators would contribute to a pool in the event of a major event that exceeds available primary coverage. So far, no event has required the use of the retrospective, and there have been few claims against primary coverage as well. The problem, as demonstrate by Fukushima, is that the nearly $15 billion in coverage currently available in the U.S. is far less than what would likely be needed to cover a similar event.

Table 7.2: Insurance Framework & Emerging Technologies

Insurance	Commercial Nuclear Power	Hazardous Waste Disposal	Healthcare Cyber
Trigger Legislation	Price Anderson Act (1957)	Resource Conservation and Recovery Act (RCRA) (1976/1982)	Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Mandatory Liability/ Property Protection	Yes (1957)/Yes(1980)	Yes (1982)/Yes(1982)	No
Initial Mandatory Liability/ Property Coverage	$560 million(1957)/ $1.06 billion(1980)	$1 million/$2 million (sudden) $3 million/$6 million (gradual)	None
Initial Primary Liability Providers	NELIA (135 insurers) MAELU/MAERP (105 insurers)	Howden-Snow Group (1974) & around 50 other insurers (1976-1989)	AIG & around 10 others
Initial Primary Liability/ Property Coverage	$60 million (1957)/ $1.06 billion (1980)	Up to $50 million	Up to $25 million
Government Backstop (reinsurance)	Yes (1957)	None	None
Initial Government Backstop	$500 million	None	None
Current Mandatory Liability/ Property Coverage	$14 billion/$3.25 billion	$1 million/$2 million (sudden) $3 million/$6 million (gradual)	None
Current Primary Liability/ Property Provider(s)	American Nuclear Insurers (ANI) Nuclear Electric Insurers Limited (NEIL)	Aounnd 50 specialty insurers	Over 600 domiciled insurers
Coverage	$450 million (ANI)	Up to $100 million	Up to $100 million
Current Government Backstop	$0	None	None
Current Retrospective Coverage	$13.48 billion	None	None
Business Interruption Coverage	Yes (Up to $490 million)	None	Yes (Sublimit)
Typical Term of Policy	Lifetime	Claims-Made (1 year)	Claims-Made (1 year)
Types of Insurers	Stock/Mutual/Pools/RRGs/Federal	Stock/Mutual/Pools/RRGs	Stock/Mutual/RRGs

Insurance covering environmental hazards developed in a far different way. Initially, until the mid-1960s, such hazards were covered under standard occurrence-based CGL and P&L policies. However, insurance eventually realized they were over exposed to covering sudden events like oil spills, and gradual pollution events that occur over long periods of time, and began to exclude such events from standard policies. In its place, some insurers created specialty claims-based environmental liability insurance (EIL) that would cover such events only for claims filed during the policy period. Following the passage of RCRA in 1976 and the discovery of the Love Canal disaster in 1978, demand for EIL intensified, and many insurers issued policies without adequately understanding the risk. Many insurers also had to deal with adverse court decisions that, despite

pollution exclusions, made them liable to pay huge tort claims under past CGL and P&L policies. Compounding this problem, with the passage of Superfund in 1981 and the discovery of thousands of new toxic sites, the number of liability suits exploded. In response, most insurers withdrew from the market, and a few filed for bankruptcy. Operators attempted to form risk pools and risk retention groups to cover members insurance, but most of these failed. By the end of the 1980s, many operators of TSDFs could not obtain financial protection required under RCRA, and a substantial number had to cease operations. What emerged out of this market failure were groups of insurance carriers that specialized in specific "niche" environmental hazard policies. These carriers developed expertise in evaluating these hazards, monitoring insureds behavior, and encouraging clients to implement state of the art technology and adopt best safety practices in order to minimize losses.

The final domain, healthcare cyber, is newer than the other domains, and seems to have, so far, taken a more conventional insurance development path. Following the passage of HIPAA in 1996, cyber coverage became available, with some carriers developing products specifically targeted at healthcare-sector firms. Over time, most insurers excluded cyber from standard CGL and P&L policies, though quite a few allowed clients to add cyber coverage through endorsement to existing policies. Many insurers also introduced standalone policies typically with higher levels of coverage, but also with greater scrutiny of client operations and assessment of their cyber maturity. For most of the history of healthcare cyber insurance the product remained highly profitable. Demand increased following the Anthem breach and other high profile healthcare attacks

in 2015's "Year of the Breach," and cyber insurers were able to meet this demand and remain mostly profitable. This began to change in 2018-2019 when ransomware became a new emerging threat particularly targeting healthcare-sector firms. This risk has accelerated during the COVID-19 pandemic, and many carriers have experienced losses. In reaction, most insurers have increased premiums and some carriers have also adjusted their expense ratios by cutting administrative costs, including underwriting. Those carriers that have done the best, like TDC Specialty and Tokio Marine, have increased underwriting scrutiny, and developed products and services specifically targeted at healthcare clients. However, this market is still in a fairly early stage of development, and has not truly experienced a TMI-, Love Canal- or 9/11-like event that might impact future cyber insurance evolution. Thus, some of the insurance experiences from the other two case studies may be applicable to the healthcare cyber domain in the future.

C. Safety and Emerging Technologies

This section looks at the primary dependent variable, safety, and its correlation with three explanatory variables: 1) regulation, 2) litigation, and 3) insurance. The first two variables are rival explanatory variables to the key independent variable explored in this dissertation. In reality, there appears to be a close synergistic relationship among regulation, litigation and insurance in helping to promote firm safety. This synergistic relationship will be explored in more detail below.

1. *Regulation as an Explanatory Variable for Safety*

The first explanatory variable explored in Table 7.3 below is federal and state regulation. Each of the regimes is regulated by a different federal agency, and each

agency has varying amounts of human and monetary capacity to carry out their mission. The NRC regulates about a hundred commercial nuclear reactors with a staff of around 3000 full time employees and an annual budget of $921million. Hazardous waste facilities including around 1800 TSDFs are federally regulated by EPA with a staff of 14,172 employees and an annual budget of a little over $9 billion. In addition to TSDFs, EPA regulates over a million other smaller hazardous waste handlers including gas stations and dry cleaners. However, their oversight functions are heavily supported by state EPAs who handle the bulk of audits and inspections. The DHHS Office of Civil Rights has regulatory authority over approximately 750,000 HIPAA covered entities including healthcare providers and their business associates. They do this with a staff of 157 full time employees and a budget of around $30 million. While some states do investigate cyber breaches, they are not specifically focused on healthcare breaches. Thus, indisputably, OCR oversees the most entities with far less staff and resources than the other two regimes.

Table 7.3: Regulation & Safety in Emerging Technologies

Regulation & Safety	Commercial Nuclear Power	Hazardous Waste Disposal	Healthcare Cyber
Federal Regulatory Agency	Nuclear Regulatory Commission (NRC)	Environmental Protection Agency (EPA)	Dept. of Health & Human Services Office of Civil Rights (OCR)
Full Time Employees	3062 (2020)	14,172 (2020)	157
Budget	$921 million	$9.05 Billion	$30 million
State Regulatory Agency	State EPA	State EPA	State Attorney General Offices
Regulatory Safety Actions	Ex Ante Information Gathering (Licensing , Audits & Inspections)	Ex Ante Information Gathering (Licensing , Audits & Inspections)	Ex Ante Information Gathering (HIPAA Audits & Patient Complaints)
	Nuclear Rules & Standards	Environmental Rules & Standards	HIPAA Safety & Privacy Rules
	Self-Reporting	Self-Reporting	Self-Reporting
	Probabilitic Risk Assessment (PRA)	Environmental Assessment (EA) Environmental Impact Statement (EIS)	HIPAA Risk Assessment
	Ex Post Information Gathering (Accident Investigation)	Ex Post Information Gathering (Accident Investigation)	Ex Post Information Gathering (Breach Investigation)
	Ex Poste Standards Evaluation	Ex Poste Standards Evaluation	Ex Poste StandardsEvaluation
	Civil Monetary Penalties & Compensation for Victims	Civil Monetary Penalties & Compensation for Victims	Civil Monetary Penalties & Compensation for Victims
	Revoke Permit	Revoke Permit	Post Breach on "Wall of Shame"
Regulatory Measures of Safety	Licensee Event Reports (LERs)	# of Financial Audits	HIPAA Complaints
	NRC Plant Availability	# of Non-Financial Audits	HIPAA Audit Results
	NRC Assessment Ratings	# of Safety Inspections	HIPAA Investigations
	NRC Notice of Violations (NOVs) & Significant Events (Ses)	# of Violations	HIPAA Fines

In varying degrees, regulation drives safety at all three regimes. It collects information “ex ante” before an accident or breach occurs. It does this through the licensing or permitting process for nuclear reactors and TSDFs. It also gathers ex ante data through offsite audits and onsite inspections. This happens frequently at nuclear plants, less frequently at hazardous waste facilities, and rarely at healthcare covered entities. All three also depend on entities to self-report adverse events, and on other external entities including members of the public and vendors (including insurers) to report issues when they occur.

All three regulators also conduct risk assessments including probability risk assessments (PRAs) by NRC, environmental impact statements by EPA, and HIPAA Risk Assessments by OCR. These assessments are resource intensive, and rarely are

conducted, especially by OCR. All three also gather ex poste information following an accident or breach including investigations. In some cases standards and regulations are reevaluated in light of investigation findings. Also, each regulator has the authority to issue fines for violations, and provide compensation to third parties who have been harmed. Both the NRC and EPA have the power to revoke licenses, effectively shutting the facility down. OCR cannot shut violators down, but can deny federal funding and shame the entity by posting the breach on the OCR portal.

Thus, federal regulators have significant power to manage safety in all three regimes. However, this power is limited by the resources at their disposal. Also, as noted earlier, regulation has a synergistic relationship with the other two explanatory variables. Regulations for nuclear reactors and hazardous waste facilities specify mandatory insurance as a condition of licensure. Compliance with regulations can be required by insurers as a condition of coverage, and non-compliance can be evidence of negligence in litigation cases. Regulatory violations can also trigger civil litigation by state and local governments, other companies, and individuals.

2. *Litigation as an Explanatory Variable for Safety*

The second variable and rival explanation explored is litigation's role in managing emerging technology safety. As shown in Table 7.4, litigation's risk management tools are powerful but limited. The primary institutions involved in litigation are state and federal courts, and the primary drivers of litigation are tort laws that redress a wrong done to people or other legal entities, and provide relief from the wrongful acts of others,

usually by awarding monetary damages to victims as compensation. Court decisions in one case can also encourage lawsuits by other parties in the same or other jurisdictions.

Much of the ex ante safety impact of litigation is as a deterrent, encouraging firms to enact safety precautions to avoid huge lawsuit costs and harm to their business reputations. The fear of litigation however is a double edged sword. It can encourage safety precautions to avoid accidents and subsequent lawsuits, or it can cause firms to hide accidents in the hopes of not being discovered. This can make the consequences of an adverse event far worse.

Table 7.4: Litigation & Safety in Emerging Technologies

Litigation & Safety	Commercial Nuclear Power	Hazardous Waste Disposal	Healthcare Cyber
Institutions	State & Federal Courts	State & Federal Courts	State & Federal Courts
Drivers	Tort Laws & Court Decisions	Tort Laws & Court Decisions	Tort Laws & Court Decisions
Litigation Safety Actions	Ex Ante Fear of Litigation	Ex Ante Fear of Litigation	Ex Ante Fear of Litigation
	Ex Post Information Gathering (Discovery & Trial Testimony)	Ex Post Information Gathering (Discovery & Trial Testimony)	Ex Post Information Gathering (Discovery & Trial Testimony)
	Ex Poste Standards Evaluation	Ex Poste Standards Evaluation	Ex Poste StandardsEvaluation
	Civil Monetary Penalties & Compensation for Victims	Civil Monetary Penalties & Compensation for Victims	Civil Monetary Penalties & Compensation for Victims
Litigation Measures of Safety	Number & Type of Lawsuits	Number & Type of Lawsuits	Number & Type of Lawsuits
	Settlements & Verdict Awards	Settlements & Verdict Awards	Settlements & Verdict Awards

Most of the safety actions of litigation occur after an adverse event occurs. Through the litigation, ex poste information on safety actions or inactions of the defendant prior to the event is collected through the investigation, discovery and trial process. Ex poste information includes subpoenaed records, oral and written testimony, and other evidence collected by the plaintiffs and their legal teams. Litigation also buttresses safety ex post by providing a mechanism for victim compensation and optimizes cost internalization by potentially making firms pay the full amount for the harm their technology causes.

Litigation can also motivate firms and industries to reexamine safety standards, and make necessary changes if needed. The only real measures of litigation's impact on safety are the number and type of tort cases filed, and their outcomes. Some verdicts can order guilty parties to make safety changes, while others can compel firms or industries to improve safety in order to avoid future legal action. However, given the lengthy time it takes to litigate and re-litigate cases, the safety impact can be delayed or even made moot as technology evolves or the mechanisms for safety changes.

3. *Insurance as an Explanatory Variable for Safety*

This dissertation's third and principle explanatory variable for safety in emerging technologies is insurance. As outlined earlier and in the literature review, the insurance framework provides many private mechanisms for emerging technologies to obtain insurance including primary stock or mutual insurers, captives, reinsurance, risk retention groups, retrospective pools, insurance-linked securities, and catastrophe bonds. All of these private mechanisms rely on the basic business principle that the risk is insurable for a risk-appropriate fee or premium. If the risk is uninsurable, the only real recourse is public insurance through local, state or federal governments.

In Table 7.5 below, the focus primarily is on the private insurance mechanisms for impacting emerging technology safety. Many of these mechanisms are similar to those observed in the other two variables of interest. These include gathering both ex ante and ex poste information, driving development and adoption of standards, providing for compensation of victims, and finding ways to measure firm safety that is then used to

decide future actions. Further, insurance actually incorporates the other two variables into its risk calculation models.

There are basically two types of private sector insurance – first-party that covers the insureds own assets, and third-party that handles liability arising from harm to others. Each of the three regimes handles first-party and third-party coverage in different ways.

Table 3: Insurance & Safety in Emerging Technologies

Insurance & Safety	Commercial Nuclear Power	Hazardous Waste Disposal	Healthcare Cyber
Primary Liability Insurer	American Nuclear Insurance (ANI)	Around 50 specialty insures & 150 Enviromental Products	Over 600 providers of 1st & 3rd Party Cyber Insurance Coverage
Primary Property Insurer	Nuclear Electric Insurance Limited (NEIL)	Around 50 specialty insures & 150 Enviromental Products	Over 600 providers of 1st & 3rd Party Cyber Insurance Coverage
Insurance Safety Actions	Ex Ante Information Gathering (Underwriting Process, Inspections)	Ex Ante Information Gathering (Underwriting Process, Inspections)	Ex Ante Information Gathering (Underwriting Process, HIPAA Compliance Audits)
	Adhere to NRC Regulations & State EPA Regulations	Adhere to Federal & State EPA Regulations	Adhere to HIPAA/HITECH Privacy & Security Rules
	Require INPO Membership & Adoption of INPO Safety Standards (NEIL)	Drive development and adoption of new safety standards	Drive development and adoption of healthcare-specific cyber standards
	Boiler & Fire Inspections (NEIL), Radiation Inspections (ANI)	Site-Specific Inspections	Penetration Testing
	Peer-Review INPO Inspections & Pool Monitoring	Continuous Monitoring	Monitoring through Partnerships with Cybersecurity Companies
	Nuclear Safety Training (ANI & NEIL)	Environmental Safety Training	Cyber Safety Training
	Ex Post Information Gathering (Claims Filing & Accident Investigation)	Ex Post Information Gathering (Claims Filing & Accident Investigation)	Ex Post Information Gathering (Claims Filing & Accident Investigation)
	Compensation for Victims	Compensation for Victims	Compensation for Victims
Insurance Measures of Safety	INPO Rating	RCRA "Cradle to Grave" Manifest	HIPAA Security & Privacy Rule Compliance
	ANI Engineering Rating Factor (ERF)	Site-Specific Criteria	Cyber Maturity Level - NIST
	Claims Frequency & Magnitude	Claims Frequency & Magnitude	Claims Frequency & Magnitude
Policy Safety Measures	Risk-Based Premium Differentiation Premium Credits & Penalties	Risk-Based Premium Differentiation Premium Credits & Penalties	Risk-Based Premium Differentiation Premium Credits & Penalties
	Deductibles, CoPays, Quota Shares, & Waiting Period (NEIL)	Deductibles, CoPays, Quota Shares, & Waiting Period	Deductibles, CoPays, Quota Shares, & Waiting Period
	Exclusions	Exclusions	Exclusions
	Coverage Limits & Retrospective Obligations	Coverage Limits	Coverage Limits
	Right to Stop Operations	Policy-Specific Customized Coverage & Safety Criteria	Partnerships with Managed Security Providers (MSP)
	Right to Suspend Coverage	Right to Suspend Coverage	Right to Suspend Coverage

Commercial nuclear power has only two primary insurers – NEIL for first-party property and ANI for third-party liability. ANI also administers the third-party

retrospective liability pool by collecting annual premiums and, if needed, retrospective payments for victim settlements. Each of these insurers also provides reinsurance to the other. Foreign nuclear insurers also reinsure a portion of both NEIL's and ANI's nuclear risk.

There are about fifty specialty insurers that offer first- or third-party environmental insurance coverage, or both coverages in a comprehensive package. Most of these insurers are non-admitted carriers whose coverage is not regulated by any U.S. state. This means that these insurers can develop highly specialized or niche products, and charge unregulated premiums based on specific client risks, and what the market will support.

Most cyber insurance is domestic and sold by admitted carriers who must register their policies, coverage, and premiums with state regulators, who in turn share this data with NAIC. As of 2020, there were over 600 insurers offering property, liability or combined coverage through either standalone policies or packaged endorsements to other existing policies.

All three regimes gather ex ante information. This is done principally through the underwriting process including policy questionnaires, pre-coverage audits, and in some cases onsite inspections. In the case of nuclear and environmental insurance, the insurer may be involved in the facilities construction, and may have a say in what safety mechanisms are implemented. Part of the underwriting process is to check and see if the applicate is in compliance with applicable federal and state regulations, and to examine their litigation and insurance claims history. Since most policies are claims-made or annually renewable, this process is repeated on a regular basis.

Insurers in all three regimes are also involved in the development of regime safety standards, and these insurers have various mechanisms to encourage their adoption by clients. NEIL requires all of its commercial nuclear power customers to be members of INPO, adopt INPO standards, and submit to INPO inspections. They then use the INPO inspection ratings as a major factor in annual premium calculations. Likewise, environmental and cyber insurers often reward clients who adopt standards and other best practices with premium discounts, and punish non-adopters through premium penalties or denial of coverage.

Insurers in all the regimes offer loss prevention services that are unique to the specific risk. NEIL conducts nuclear plant boiler and fire inspections, and based on their observations make recommendations on how to improve safety. Likewise, ANI conducts radiologic inspections. Both entities share their inspection results with INPO and, if warranted with the NRC. INPO also has NEIL members review their inspection findings. Thus there is a high degree of internal industry visibility which creates peer pressure to fix safety problems. Because of the specialty nature of environmental insurance, insurers may require TSDF clients to undergo special testing for certain hazardous chemicals, or implement continuous monitoring of storage tanks or ground water conditions. Insurers of healthcare cyber may require clients to undergo regular penetration testing to identify vulnerabilities. They may also reward clients who partner with managed security providers who conduct regular HIPAA audits, and monitor and respond to cyber threats.

All regime insurers also provide loss prevention education and incident response training. This includes relevant employee education on fire prevention, hazardous

chemical handling, or identification of phishing scams. Insurers often help clients develop emergency plans to react to radiation leakages, chemical spills, or ransomware attacks that compromise business operations.

Unlike regulation and litigation, most insurance safety mechanisms are proactive and often positively incentivize clients to adopt best safety policies and practices. Insurance also gathers information ex poste following adverse event. This information is gathered through the filing of claims and through claims investigations. Where needed, insurance is also a primary provider of victim compensation including third-party litigation defense and settlement, first-party property damage and business interruption expenses, and payment of regulatory fines.

Emerging technology insurers have also developed or adopted mechanisms for measuring regime safety. Nuclear insurers often use INPO safety ratings to determine premium credits or debits. ANI also uses its Engineering Rating Factor (ERF) to estimate premiums. Environmental insurers review client RCRA "cradle-to-grave" manifests to identify the types and amounts of hazardous chemicals, and healthcare cyber insurers use results of HIPAA audits and NIST cyber maturity levels to determine insurability and premiums.

The final mechanism employed by insurers in all three regimes is the insurance policy itself. All policies contain terms and conditions that are meant to encourage client safety and prevent insurer losses from risks not covered by the collected premium. Terms and conditions include exclusions, coverage limits and sub-limit meant to prevent adverse selection and control for moral hazard. Policies define when, why and how claims are

covered, and what the client must do to assure the terms and conditions are met. Most important the policy states the premiums due, as well as the deductibles, copays, waiting periods and other client obligations designed to internalized some of their risk and promote safe client behavior. Ultimately, if a client fails to fulfill its safety obligations, the insurer has the right to suspend or cancel coverage.

Thus insurance arguably has more tools at its disposal to manage private-sector risk behavior than either regulation or litigations. Further, many of these tools are proactive and use positive incentives to motivate clients to adopt risk reduction and safety best practices.

D. Quantitative Evidence of Insurance & Safety in Emerging Technologies

This final section compares the quantitative evidence from each case study to further demonstrate the role that insurance plays in recording, assessing, and managing safety in the three targeted domains.

1. *Commercial Nuclear Power Quantitative Evidence - Safety & Insurance*

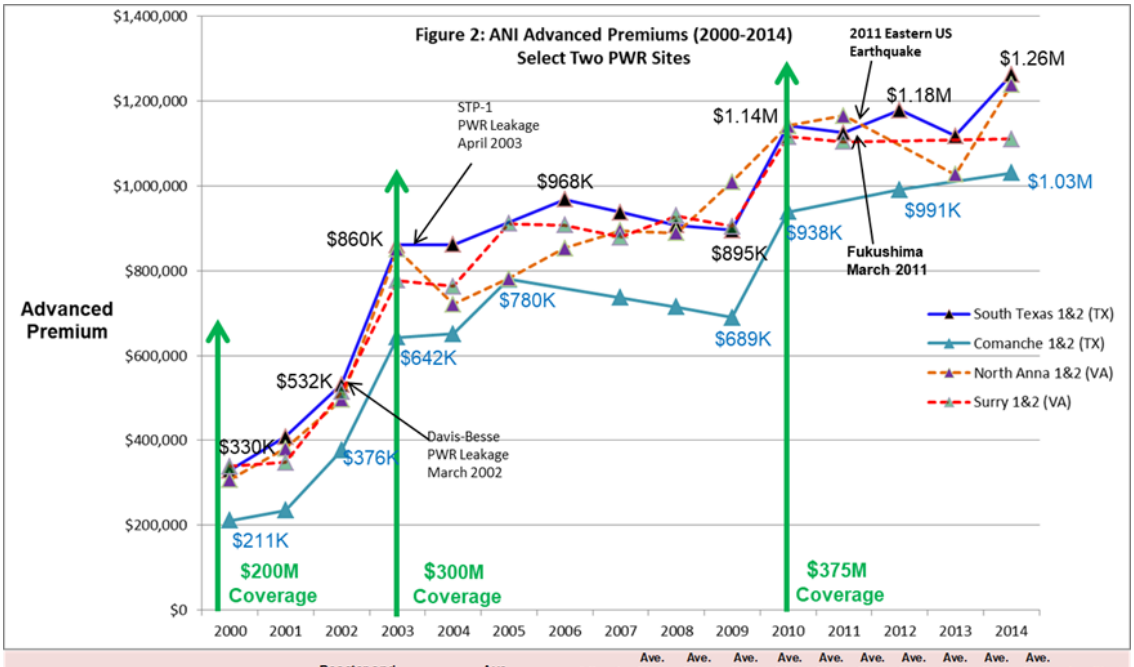
For the commercial nuclear power regime, a key challenge was the availability and structure of available safety data. Much data on commercial nuclear power safety is highly sensitive, and purposefully hidden from public view. To protect the reputations of its members, INPO safety ratings are almost never publically released. Likewise, ANI considers its Engineering Rating Factors a proprietary trade secret, and only shares data with nuclear clients and with the NRC. Data on NRC safety violations and measures are buried in websites beneath layers of background materials and is difficult to scrape, structure, and analyze. Data on NEIL property and ANI liability insurance and premiums

is only available in unstructured annual documents for each individual reactor and plant. Consequently, it was extremely time consuming to search, download, and extract this data for analysis. There is also a great deal of missing data, with no data for some reactor sites and years. Thus one of the major contributions of this dissertation is bringing this safety data to light.

The first set of data looked at the premium data covering the period 2000 to 2014 for two sets of reactor sites – one set in Texas and the other in Virginia (Figure 7.1). Each of the sites had two Westinghouse reactors of similar type. The Texas sites had newer reactors, with higher power, located in less populated areas than the Virginia sites. Key data including changes in coverage levels, reactor availability levels, reactor events, and events at other plants are also noted. What it shows is that the Comanche plant in Texas appears to be the lowest risk or "safest" from liability insurance premium perspective in all fifteen years of coverage. Conversely, the other Texas plant, South Texas had the highest premiums during most years and could be consider a higher risk or "less safe" than Comanche. Comparing these two sites, The South Texas reactors slightly older and higher powered, but are located in a less populated area. Two key factors that might account for the difference in premiums is that South Texas had a reactor leakage in 2003, and had lower average plant capacity over the period possibly indicating non-public operational issues.

This can be compared with the premium data for the two Virginia sites which are distinctly similar to one another. Thus, from a premium perspective, these plants have similar risk profiles, and are more or less equally "safe." The main factors affecting their

premiums appears to be coverage changes, events at other plants, and an earthquake that occurred in Virginia in 2011.



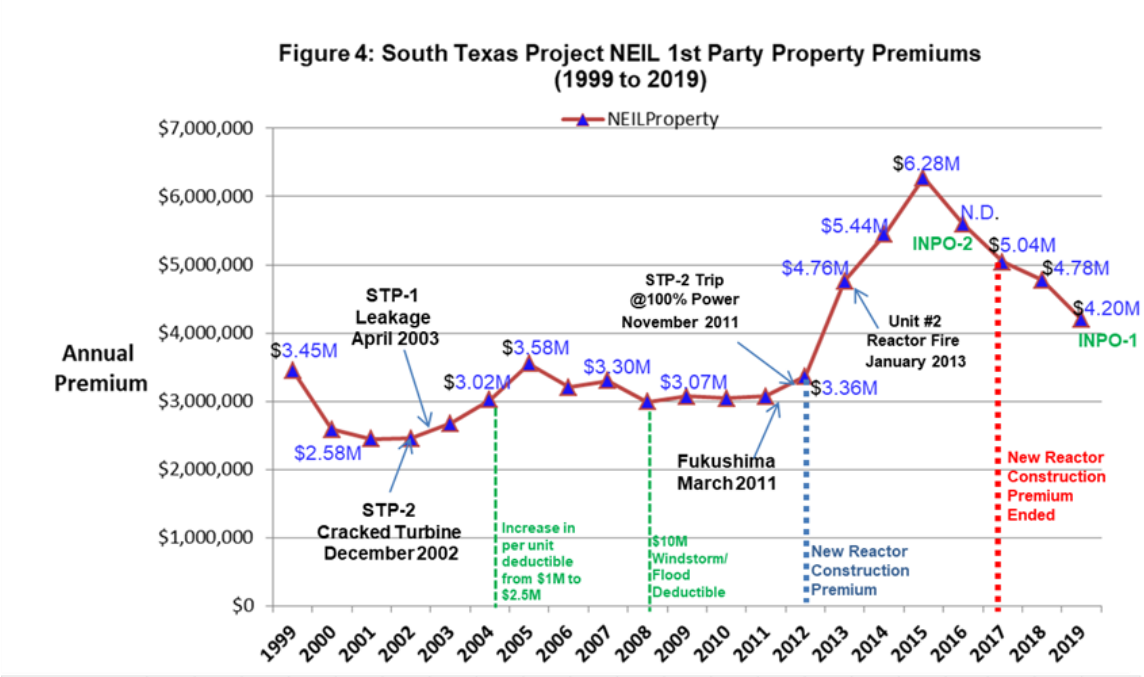
Plant Name, Unit Number	City, State	# PWR	Reactor and Containment Type	Supplier	Ave Age 2000	Ave. MWt	# People w/in 10 miles	Ave. Plant Cap. 2005	Ave. Plant Cap. 2006	Ave. Plant Cap. 2007	Ave. Plant Cap. 2008	Ave. Plant Cap. 2009	Ave. Plant Cap. 2010	Ave. Plant Cap. 2011	Ave. Plant Cap. 2012	Ave. Plant Cap. 2013	Ave. Plant Cap. 2014	Ave. Plant Capacity 2005-2014
South Texas Project	Palacios TX	2	PWR-DRYAMB	WEST 4LP	11.5	3853.0	8,703	88.6%	94.8%	95.9%	95.2%	95.5%	94.5%	91.0%	82.5%	75.2%	92.0%	90.51%
Comanche Peak	Glen Rose TX	2	PWR-DRYAMB	WEST 4LP	8.5	3612.0	21,620	90.4%	96.7%	92.1%	95.2%	97.0%	97.5%	91.5%	94.5%	96.2%	89.0%	94.01%
North Ana Power Station	Mineral VA	2	PWR-DRYSUB	WEST 3LP	21.0	2940.0	34,081	95.3%	93.9%	87.0%	91.3%	96.0%	93.0%	77.0%	94.0%	87.4%	96.0%	91.09%
Surry Power Station	Gravel Neck VA	2	PWR-DRYSUB	WEST 3LP	27.5	2587.0	141,209	93.4%	88.3%	93.6%	93.3%	95.8%	93.8%	84.0%	88.3%	81.3%	94.0%	90.56%

Figure 7.1: Premium Data for Four Plant Sites & Safety (Source NRC)

The second set of data examines NEIL property insurance premiums for the South Texas Plant (STP) covering the period 1999 to 2019. Included in this data are changes to premium deductibles, additional key plant events, NRC significant event and Licensee Event Report (LER), and fire violation counts, NRC plant availability and assessment ratings, and NEIL base and effective credits used in premium determination. Most important are two precious years of INPO safety ratings in 2016 and 2019. What the data shows is a somewhat murky picture of plant safety. Initially, facility property premiums

declined. Then in 2002-2003, the plant experienced a series of problems, with its LERs and fire violations increasing to their highest levels during the twenty year period. Premiums increased during this time, offset somewhat by a decision to increase their deductible. Premiums reach a time period peak in 2005, and then leveled out for six years (2006 to 2011).

Figure 7.2: NEIL South Texas Property Insurance Premiums & Safety



Year	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Significant Events	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	NOV5LER	0	0
Licensee Event Reports	16	11	7	7	10	7	5	8	3	4	4	7	4	2	7	1	2	2	2	2	4
Fire Violations	0	0	0	0	1	3	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0
Ave. Plant Availability	ND	ND	ND	ND	ND	ND	88.60%	94.77%	95.87%	95.23%	95.50%	94.50%	91.00%	82.50%	75.15%	92.00%	81.78%	91.45%	90.98%	89.90%	95.55%
NRC Annual Assessment	GTG	Green	Green	Green	Green	Green	Green	GTG	Green	Green	Green	Green	Green	Green	Green	Green	Green	GTG	GTG	Green	Green
Base NEIL Plant Credit	ND	ND	ND	ND	ND	ND	ND	ND	ND	ND	20.0%	18.0%	18.0%	18.0%	ND	ND	ND	13.0%	11.0%	13.0%	20.0%
Effect. NEIL Plant Credit	ND	ND	ND	ND	ND	ND	ND	ND	ND	ND	30.0%	27.0%	27.0%	27.0%	ND	ND	ND	19.5%	16.5%	19.5%	30.0%
Maximum Retrospective ($M)	$17.26	$12.92	$12.23	$24.51	$26.75	$30.16	$35.49	$32.04	$33.02	$29.90	$30.70	$30.44	$30.74	$33.64	$47.60	$54.43	$62.76	$6.60	$50.40	$47.78	$42.00

Then in 2011, a series of events occurred that increased premiums significantly. The most important event that likely had the biggest impact on premiums was the decision to construct two new reactors. However, coinciding with this decision, the Fukushima

accident occurred, and reactor #2 experienced several issues including a power trip in 2011 and a reactor fire in 2013. During this time NEIL records show that STP's base and effective credits decreased slightly. Premiums reached their all-time peak in 2015 and then declined. In 2016 the first INPO rating shows a good rating of "2" but not the highest achievable. In 2017 the decision was made to end construction of the new reactors, subsequently ending additional construction premiums. In 2019 the second INPO safety rating shows that STP returned to optimum rated safety performance. The NEIL premiums also reached their lowest levels since 2013 with plant base and effective credits also reaching a maximum. Given the hodgepodge of events occurring at STP between 2013 and 2019, it is hard to determine what factors most influenced safety. However, it does appear that STP reached a high level of perceived safety in 2019 based on the NEIL premium, the NEIL credits, and especially the INPO safety rating.

2. *Hazardous Waste Quantitative Evidence – Safety & Insurance*

The quantitative data for hazardous waste facilities is more robust and structured than the data for commercial nuclear power plants. It comes from the EPA's Enforcement and Compliance History Online (ECHO) Database which includes the Resource Conservation and Recovery Act Information System (RCRAInfo) data subset Specifically this analysis looks at data for 1808 TSDFs in 49 U.S. states , the District of Columbia, and Puerto Rico. The data, covering the period 1980 to 2020, includes counts by TSDF by year of the number of financial audits and non-financial evaluations, and the number of financial and non-financial violations.

Several assumptions are made. First, that financial audits check for financial protection, and that a financial violation indicates no insurance. Second it is assumed that non-financial evaluations check for safety, and that a non-financial violation indicates a safety problem. Thus TSDFs with more non-financial violations are less safe. It was also assumed that state and federal TSDFs self-insure, and therefore are not covered by private insurance.

First, a number of interesting trends were observed. As shown in Figure 7.3, over the entire period, the number of financial audits increased, and the number of financial violations decreased. This indicates that TSDFs were increasingly being covered by environmental insurance. Simultaneously, as shown in Figure 7.4, the number of non-financial safety evaluations increased, and then leveled off, but the number of safety violations decreased. Thus while insurance coverage was increasing, safety violations were decreasing, and TSDFs were becoming "safer."

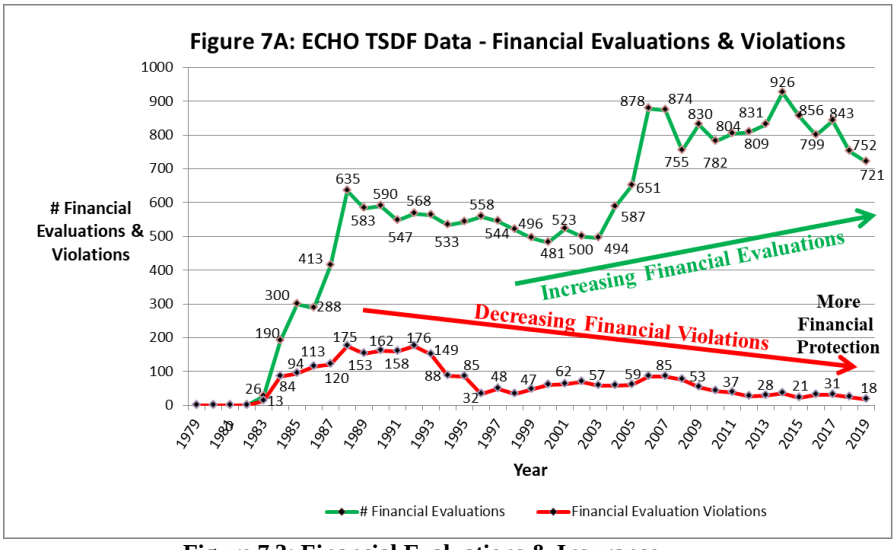


Figure 7.3: Financial Evaluations & Insurance

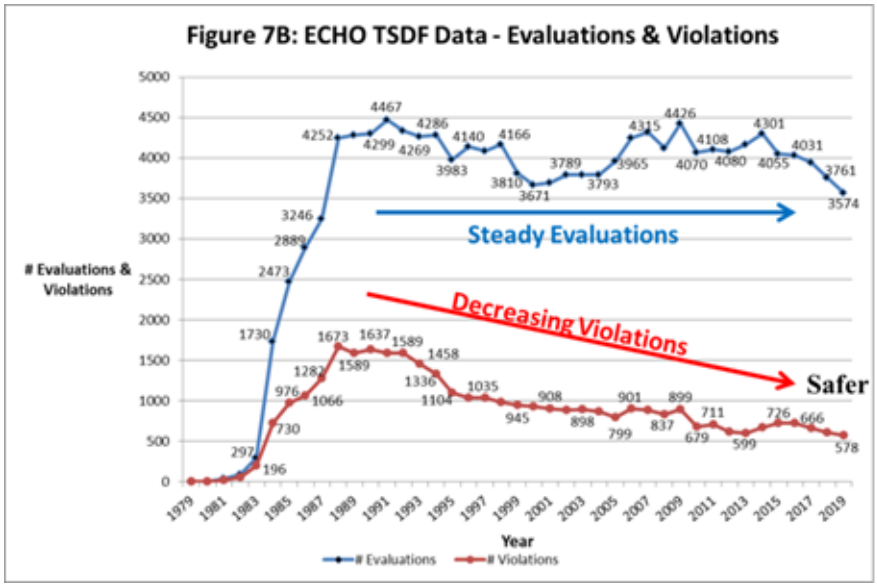


Figure 7.4: Safety Inspections & Safety

Another way to visualize the role of insurance in managing environmental safety is through the creation of indices to allow comparison among individual TSDFs. In the hazardous waste case study, two indices were created. The first index is the ratio of non-financial evaluations (NFE) to non-financial violations (NFV). The logic of this index is that TSDFs with high indices that have many evaluations and few violations are safer than TSDFs with low indices that have few evaluations and many violations. The NFE/NFV index is then calculated individually for all 1808 TSDFs. Likewise, a second index looks at the ratio of financial evaluations (FE) to financial violations (FV). This index only applies to 1608 private TSDFs, since government TSDFs are not subject to RCRA financial protection regulations. The logic of this index is that private TSDFs with high indices that have many financial evaluations and few financial violations are more

likely to have insurance than private TSDFs with low indices. The FE/FV index is then calculated for the 1608 private TSDFs.

In the case study, the indices for 1784 TSDFs in the continental United States were mapped (Figure 7. 4) including 1592 private TSDFs (flags), 154 federal government owned TSDFs (stars) and 38 state owned TSDFs (diamonds).The size and color of the marker for each type of TSDF indicates the magnitude of the NFE/NFV index for the site, with larger black markers depicting the safest facilities with the highest NFE/NFV indices. The FE/FV index is shown using a heat map with deep red and intense yellow indicating areas where the index is high, and light blue and white showing areas where the index is low.

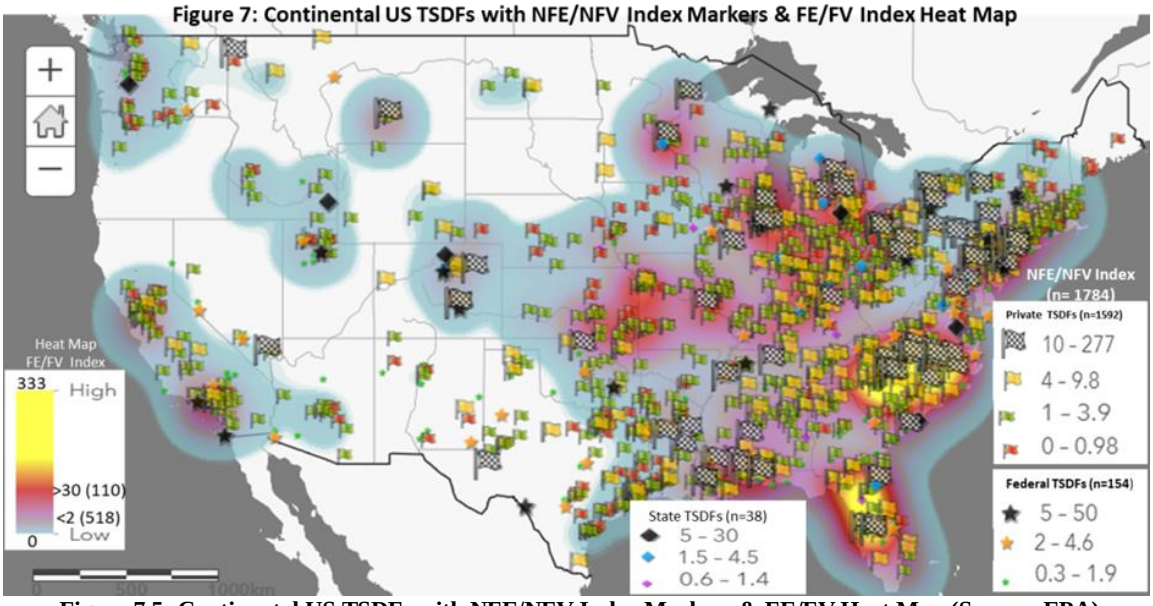


Figure 7.5: Continental US TSDFs with NFE/NFV Index Markers & FE/FV Heat Map (Source: EPA)

Several observations can be made from this data. First, black high NFE/NFV index TSDFs often cluster together in the Carolinas, New Jersey, upper mid-west, lower Mississippi Valley, Florida, and Colorado. Second, these high NFE/NFV index clusters are often located in intense yellow and red areas of the heat map where the FE/FV indices are high. This provides evidence that environmental safety as indicated by high NFE/NFV index could be influenced by financial protection as indicated by high FE/FV index. Further, white and light blue areas with low FE/FV indices seldom contain black flag "safe" TSDFs

3. *Healthcare Cyber Quantitative Evidence – Safety & Insurance*

The quantitative data for the healthcare-sector cyber risk case study is by the far the most robust and structured of the three case studies. The data includes the Healthcare Cyber Attack Database (HCAD) consisting of over 5600 healthcare cyberattack incidents covering the period 2005 to 2021. In the case study, econometric modeling was used to examine the relationship between the take up of cyber insurance by U.S. healthcare sector entities and their management of cyber safety during the period 2015 to 2020. The panel consisted of 15,144 observations from 2,524 healthcare entities over the six-year period. The entities were subdivided into 27 sub-entities (SUBCODE) representing all of the key healthcare provider types (e.g. Doctor, Hospital, etc.) and healthcare support companies (e.g. Admin, Medical Equipment etc.).

There are two key dependent variables representing cyber safety. The first is ***Attack****s* denoting the number (frequency) of cyber-attacks experienced by each entity, each year. The second is ***AttRec*** representing the number of records impacted (magnitude) by each

attack, each year. Each attack in the dataset is rated as either being internal or external (EXTHACK), and if external, whether it involved ransomware (RANSOM). The key independent variable is INSPOL10K which is the estimated number of insurance policies issued each year by sub-entity divided by 10,000. The estimate is based on the population of each sub-entity as derived from the 2018 U.S. Census Statistics of U.S. Businesses (SUSB 2018) times the take-up rates for policies by sector as determined by Marsh Analytics each year and used by the GAO in a May 2021 report (GAO 2021). The dataset also includes indicator variables denoting if the firm is large with more than 500 full time employees (FTE500), public or private (PUBorPRIV), and whether it is non-profit or for profit (NPFP).

The econometric models tested three hypotheses:

H1: Cyber insurance will have a small but significant impact on reducing the frequency & magnitude of cyber-attacks against healthcare sector entities

H2: Cyber insurance will have a more significant impact on reducing the frequency & magnitude of cyber-attacks against small private healthcare firms vs. large and/or public sector entities

H3: Cyber insurance will have a more significant impact on reducing the frequency of non-ransomware and internal cyber-attacks than on ransomware and external hacks.

The econometric models below test these three hypotheses. The first set of models uses ***xtpoisson*** to test Hypothesis #1 and Hypothesis #3 using dependent variable *Attacks* , key explanatory variable INSPOL10K, and time invariant variables including RANSOM, EXTHACK, PUBorPRIV, and NPFP. In interpreting the results of each model, the key item to look at is the sign of each coefficient. **A significant negative**

coefficient indicates the possible positive influence of insurance on cyber safety by reducing the frequency of cyber-attacks.

The first model looks at the interaction of *Attacks* with the primary independent variable INSPOL10K and the time-invariant variable NPFP with "0" equaling nonprofit and "1" indicating for profit. The introduction of a time-invariant dummy makes fixed effects modeling inappropriate. So all the models below use random effects (RE) and pooled xi: Poisson modeling with normal and robust SE. As shown in Model #1, all coefficients for INSPOL10K are small, significant; with negative coefficients for all RE and xi: Poisson models. This supports Hypothesis #1. The NPFP coefficients are also all negative and significant indicating that insurance seems to improve the safety of for profit firms, further supporting Hypothesis #1. Tests were run indicating the model's goodness of fit, with no collinearity or serial correlation.

Table 7.6 (Model #1): xtpoisson/xi: Poisson Regression of Attacks, INSPOL10K and NPFP

Attacks	(1) xtpois_RE2	(2) xtpois_RE2 Robust	(3) xipois2	(4) xipois2 Robust
INSPOL10K	-0.0106572**	-0.0106572***	-0.0106571**	-0.0106571**
	(0.0043185)	(0.0025620)	(0.0043184)	(0.0041991)
NPFP	-0.0852221**	-0.0852221***	-0.0852263**	-0.0852263**
	(0.0412532)	(0.0287743)	(0.0412529)	(0.0402187)
_cons	-1.5357025***	-1.5357025***	-1.5356862***	-1.5356862***
	(0.0285186)	(0.0178159)	(0.0285184)	(0.0281255)
/				
lnsig2u	-1.537e+01	-1.537e+01		
	(10.4566065)	(.)		
Wald chi2	18.49***	83.20***	18.69***	19.77***
Deg of Free	2	2	2	2
# of Obs	15,144	15,144	15,144	15,144

Standard errors in parentheses
* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

The second model introduces the PUBorPRIV time invariant dummy variable where "0" equals public and "1" equals private, along with dropping ransomware attacks (RANSOM==0). The results in Model #2 show better insurance performance vs. non-ransomware attacks with an increasing negative coefficient for INSPOL10K , and negative coefficient for PUBorPRIV. These results support both Hypothesis #1, and also Hypothesis #3 regarding non-ransomware attacks. The Pearson Goodness of Fit soundly fails to reject the null of a good fitting model – indicating a good fit. The mean VIF of 1.84 indicates no collinearity between the INSPOL10K and PUBorPRIV variables.

Table 7.7 (Model #2): xtpoisson Regression of Attacks, INSPOL10K and PUBorPRIV (RANSOM==0)

Attacks	(1) xtpois_RE3	(2) xtpois_RE3 Robust	(3) xipois3	(4) xipois3 Robust
INSPOL10K	-0.0196940***	-0.0196940***	-0.0196941***	-0.0196941***
	(0.0044837)	(0.0025125)	(0.0044837)	(0.0044671)
PUBorPRIV	-0.1057702*	-0.1057702**	-0.1057726*	-0.1057726*
	(0.0611004)	(0.0440730)	(0.0610999)	(0.0603633)
_cons	-1.6143537***	-1.6143537***	-1.6143398***	-1.6143398***
	(0.0551466)	(0.2615386)	(0.0551463)	(0.0542561)
lnsig2u	-1.401e+01	-1.401e+01		
	(8.7745868)	(6.046e+05)		
Wald chi2	27.83***	84.21***	28.42***	28.58***
Deg of Free	2	2	2	2
# of Obs	14,643	14,643	14,643	14,643

Standard errors in parentheses
* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

The third model includes both the PUBorPRIV and NPFP time invariant dummy variables along with the removal of external attacks (EXTHACK==0) – thus for internal breaches only . The results in Model #4 show better insurance performance for. internal attacks with an increasing negative significant coefficient for INSPOL10K , and

significant negative coefficient for PUBorPRIV in all but the xi: Poisson robust model. These results support Hypothesis #1, and also Hypothesis #3 regarding internal cyber-attacks.

Table 7.8 (Model #3): xtpoisson/xi: Poisson Regression of Attacks, INSPOL10K, PUBorPRIV & NPFP (EXTHACK==0)

Attacks	(1) xtpois_RE4	(2) xtpois_RE4 Robust	(3) xipois4	(4) xipois4 Robust
INSPOL10K	-0.0382912***	-0.0382912***	-0.0382912***	-0.0382912***
	(0.0076277)	(0.0074127)	(0.0076277)	(0.0076013)
PUBorPRIV	-0.1619426*	-0.1619426*	-0.1619425*	-0.1619425
	(0.0973649)	(0.0866145)	(0.0973651)	(0.0991927)
NPFP	0.0606222	0.0606222	0.0606221	0.0606221
	(0.0730072)	(0.0745438)	(0.0730074)	(0.0746592)
_cons	-2.2798263***	-2.2798263***	-2.2798303***	-2.2798303***
	(0.0815520)	(0.1308330)	(0.0815521)	(0.0834665)
lnsig2u	-1.120e+01	-1.120e+01		
	(11.6050949)	(1.470e+04)		
Wald chi2	33.89***	44.21***	35.70***	34.22***
Deg of Free	3	3	3	3
# of Obs	13,314	13,314	13,314	13,314

Standard errors in parentheses
* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

The final model testing frequency of attacks takes the variables from Model #1 with SUBCODE factors. Also the time invariant dummy variable FTE500 has been added with "0" indicating small firms of less than 500 employees, and "1" indicating large firms with more than 500 employees. The Federal Government (SUBCODE=1) was used as the control since it is the only sub-entity with no cyber insurance. This allowed a comparison of sub-entities with insurance to be compared to ones without. A series of regressions was then conducted to determine the best mix of significant sub-entity coefficients using RE and xi: Poisson with both normal and robust standard errors. The results, shown in Model #4., show significant negative coefficients for many small healthcare entities

including doctors, dentists, group practices, as well as administrative business associates and small community support organizations. Conversely, large organizations, including health systems, health insurers, and state government health agencies have significant positive coefficients. This supports Hypothesis #2 that cyber insurance will have a more significant favorable impact on the frequency of cyber-attacks against small private healthcare firms vs. large and/or public entities.

Table 7.9 (Model #4): xtpoisson Regression with Attacks, INSPOL10K & other Subcode Variables

Attacks	(1) xtpois_RE6	(2) xtpois_RE6Rob	(3) xipois6	(4) xipois6Rob
INSPOL10K	0.0780954***	0.0780954***	0.0780643***	0.0780643***
	(0.0154693)	(0.0099031)	(0.0154701)	(0.0129064)
Admin	-0.8526935***	-0.8526935***	-0.8523808***	-0.8523808***
	(0.1779414)	(0.1057389)	(0.1779476)	(0.1517559)
Community	-0.7437407***	-0.7437407***	-0.7435210***	-0.7435210***
	(0.1767545)	(0.0900840)	(0.1767592)	(0.1591608)
Dentist	-0.2700887**	-0.2700887***	-0.2700370**	-0.2700370**
	(0.1139428)	(0.0273816)	(0.1139432)	(0.1050755)
Doctor	-0.5278895***	-0.5278895***	-0.5277390***	-0.5277390***
	(0.1361763)	(0.0530006)	(0.1361785)	(0.1225008)
GroupPrac	-0.9331135***	-0.9331135***	-0.9328012***	-0.9328012***
	(0.1714554)	(0.1060371)	(0.1714620)	(0.1467063)
HealthSys	0.2925423***	0.2925423***	0.2925031***	0.2925031***
	(0.0604199)	(0.0422440)	(0.0604202)	(0.0589472)
Insurer	0.2866264***	0.2866264***	0.2865875***	0.2865875***
	(0.0632353)	(0.0571954)	(0.0632355)	(0.0632248)
StateGov	0.3494125***	0.3494125***	0.3493770***	0.3493770***
	(0.1235508)	(0.0883768)	(0.1235509)	(0.1178908)
_cons	-1.7429185***	-1.7429185***	-1.7428773***	-1.7428773***
	(0.0359279)	(0.0190010)	(0.0359284)	(0.0325040)
lnalpha	-1.614e+01	-1.614e+01***		
	(79.4234999)	(0.2900843)		
Wald chi2	68.63***	42126***	68.46**	81.29***
Deg of Free	9	9	9	9
# of Obs	15144	15144	15144	15144

Standard errors in parentheses
* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

The second group of models looked at the impact of cyber insurance on the magnitude of cyber-attacks as measured in records compromised per attack (***AttRec***). ***AttRec*** is extremely dispersed with some extreme outliers. For this reasons, the decision was made to use xtnbreg to model the regressions.

The first econometric model in this set includes the AttRec, INSPOL10K, PUBorPRIV and NPFP variables using fixed effects (FE) and random effects (RE). As shown in Model #5, the coefficient for INSPOL10K is small, significant and negative. The PUBorPRIV and NPFP variables are also both significant and negative. The Hausman test rejects the null and indicates the FE model is best. These results support Hypothesis #1 regarding insurance's significant impact on the magnitude of cyber-attacks. Further, private for-profit firms seem to benefit from this correlation.

Table 7.10 (Model #5): Regression of AttRec, INSPOL10K, PUBorPRIV & NPFP

	(1)		(2)	
AttRec	xtnbreg_FE2		xtnbreg_RE2	
INSPOL10K	-0.0662806***	(0.0152981)	-0.0056194	(0.0044408)
PUBorPRIV	-0.2940175*	(0.1540715)	-0.0487711	(0.0629069)
NPFP	-0.5999279***	(0.1384333)	-0.0690262	(0.0454817)
_cons	-5.1039204***	(0.1268050)	-3.9867015***	(0.0542835)
/				
ln_r			0.2476588**	(0.1027854)
ln_s			12.4436648***	(0.1882310)
Wald chi2	79.65***		10.12**	
Deg of Free	3		3	
# of Obs	15,144		15,144	

Standard errors in parentheses
* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

The final model takes the variables from Model #5 using INSPOL10K with SUBCODE factors. Also the time invariant dummy variable FTE500 has been added with "0" indicating small firms of less than 500 employees, and "1" indicating large firms

with more than 500 employees. The Federal Government (SUBCODE=1) was again used as the control. A series of xtnbreg regressions was then conducted to determine the best mix of significant sub-entity coefficients using FE and RE. The results in Model #6 show that INSPOL10K has turned slightly significantly positive but with many sub-entities having significant negative coefficients. The FTE500 is also significant and positive, indicating that larger firms may not benefit from the insurance safety effect. The results also show significant negative coefficients for small healthcare entities Group Practices and Administrative business associates for the FE and RE models. Conversely, in the FE and RE models large organizations, including health systems, health insurers, and state government health agencies have significant positive coefficients. The Hausman test again rejects the null indicating that the FE model is most appropriate. These results support Hypothesis #2 that cyber insurance will have a more significant impact on the magnitude of cyber-attacks against small private healthcare firms vs. large and/or public entities.

Table 7.11 (Model #6): xtnbreg of AttRec, INSPOL10K, FTE500 & Key SUBCODEs

	(1)		(2)	
AttRec	xtnbreg_FE4	Std. Error	xtnbreg_RE4	Std. Error
INSPOL10K	0.0855002***	(0.0216227)	0.0188771*	(0.0098754)
FTE500	1.6434251***	(0.1730088)	0.1681443***	(0.0447698)
Admin	-2.1651535***	(0.7376662)	-0.2177803*	(0.1278938)
GroupPrac	-1.4332480***	(0.3763178)	-0.1697997	(0.1082599)
HealthSys	0.6821811***	(0.1628501)	0.1419433**	(0.0661939)
Insurer	0.9867796***	(0.1677125)	0.1862354***	(0.0662166)
StateGov	0.9516269***	(0.2589632)	0.2494283*	(0.1311285)
_cons	-7.2657141***	(0.1714492)	-4.2367068***	(0.0404066)
ln_r			0.2543000**	(0.1029887)
ln_s			12.4555124***	(0.1880871)
Wald chi2	213.39***		44.35***	
Deg of Free	7		7	
# of Obs	15,144		15,144	

Standard errors in parentheses
* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Thus, all the results above from the healthcare cyber quantitative analyses seem to support the three hypotheses. Cyber insurance seems to have a small but significant impact on the frequency and magnitude of cyber-attacks against healthcare sector entities. This impact is more significant for small private healthcare firms vs. large and/or public sector entities. It also has a more significant impact on the frequency of non-ransomware and internal cyber-attacks than on ransomware and external cyber-attacks.

III. Key Findings & Contributions

The evidence in the three case studies summarized above tests the research question ***"How can insurance promote better safety in emerging technological regimes?"*** The key finding derived from this evidence supports the main hypothesis that ***"Insurance can improve the safety posture of firms engaged in emerging technologies"***

This dissertation's key contribution is the creation of the Healthcare Cyber Attacks Database (HCAD) documenting over 5600 breaches against healthcare entities and sub-entities over the period 2005 to 2021. It includes over 600 ransomware attacks (HCAD-R), and over 250 cyber litigation cases (HCAD-L). The breadth and depth of this cyber data alone provides rich paths of opportunity for future research.

Within each case study, there are also key findings, contributions, and lessons learned.

Both the nuclear power and hazardous waste case studies demonstrate the utility of mandatory financial protection as a condition of permitting or licensure. Without insurance, firms in these realms cannot legally operate. They also legally must file annual confirmation of coverage and, on request, submit to financial audits by their regulatory

authority. Mandatory insurance is not unique to these two domains. Insurance is a requirement of driver licenses in most states, and a condition of most banks in extending loans for the purchase of a house. Thus, it is a tool that lawmakers can consider when looking for ways to manage private-sector risk.

As shown in all three case studies, insurance provides firms access to many proactive loss management services that can incentivize their investment in safety capabilities. Through premium credits and debits, insurance rewards firms for implementing good safety practices and punishes them for bad. It also forces firms to take responsibility for their safety, by internalizing a portion of the risk through deductibles, copays, coverage limits and exclusions.

Each case study to a greater or lesser extent demonstrates the effect of catastrophic events in shaping both the insurance structure and emerging technology which its supports. Both the commercial nuclear power and hazardous waste regimes experienced one or more seminal events that threaten the availability of insurance and the continued existence of many regime firms. The hazardous waste example, in particular, highlights the jeopardy to insurers who fail to adequately assess client risk. This is a cautionary tale to cyber insurers and providers of insurance to other emerging technologies who are rushing to take advantage of new product opportunities while not truly experiencing a catastrophic event that could disrupt the market and cause existential losses,

Each case study also has snippets of insurance safety actions that may or may not be applicable to other emerging technology domains. In the commercial nuclear power realm, insurance helped to establish and maintain a powerful standards body and peer-

review safety inspection mechanism, INPO, by requiring membership as a condition of coverage. Commercial nuclear power also introduced the government backstop, massive insurance pools, and retrospective coverage as a way to spread and internalize emerging risk. For the hazardous waste sphere, insurers developed specialized niche environmental products that focused on the unique risks posed by different operators. For healthcare cyber firms, cyber insurance appears to be more effective in helping smaller companies improve their safety posture. There is also evidence that insurance is vulnerable to new threats, such as ransomware, and can help clients to adapt to these challenges through education and loss mitigation measures.

Finally, this dissertation research has highlighted the need for more empirical studies on the synergistic interactive roles that insurance, regulation, and litigation play in optimizing safety at emerging technology firms. In each case study, these three variables influenced safety in different ways. Understanding how to balance these variables may be key to the development of public and private policies governing management of emerging technological risks in the future.

IV. Public Policy Implications & Recommendations

The policy recommendations in this section relate primarily to cybersecurity, but could be applied to future emerging technological risks. They build on the lessons learned in all three case studies, along with recent recommendations from the Cyberspace Solarium Commission a congressionally-authorized effort to develop cybersecurity policies.

The CSC produced an initial report with recommendations in March 2020 (CSC 2020) and a follow up report in 2021 (CSC 2021). Some of the CSC recommendation revived efforts by the Department of Homeland Security (DHS) Cyber Incident Data and Analysis Working Group (CIDAWG) to examine the current state of the cybersecurity insurance market and determine how to best advance its capacity to incentivize better cyber risk management. The DHS effort was discontinued in 2016, with the records on the Cybersecurity & Infrastructure Security Agency (CISA) website archived (CISA 2022).

The first recommendation is for a Federal Data Breach Notification Law, first proposed in Congress in 2003 and, despite bipartisan support, still not enacted. The CSC also supports passage of such a law (CSC 2020, p. 94). The most recent proposed bill, the *Cyber Incident Notification Act of 2021* (U.S. Senate 2021) includes a provision that shields entities that submit a report from liability due to the submission of a cybersecurity notification, and would prevent cyber incident notifications from being used as evidence in criminal or civil actions. Given evidence in this dissertation, it is important that this breach notification data be made public, so that it can studied by scholars. Further, given the synergistic relationship between insurance and liability, it is recommended that liability protection not be absolute. Rather, to free up the courts, hacked companies should be required to pay for effected client credit monitoring and identity protection. This is almost inevitably happens in most cyber class action lawsuit settlements, and would speed compensation of victims.

The second recommendation, also recommended by the CSC, is for the creation of a charged with collecting and providing statistical data on cybersecurity and the cyber ecosystem to inform policymaking and government programs. The data from the OCR Breach Portal was invaluable in helping to create the HCAD database. However, data on healthcare breaches of encrypted files or involving less than 500 records is not readily available. A repository of cyber data on all sectors would facilitate studies similar to this dissertation, but broader and more robust, allowing for comparison between different industries or demographic groups. Such data could also provide clarity about what safety measures are most effective in reducing risk, and provide a better understanding of evolving trends in cybersecurity and cyberspace.

The CSC also recommends that the DHS create a Federally Funded Research and Development Center (FFRDC) to work with the state regulators in developing certifications for cybersecurity insurance products (CSC 2020, pp. 79-80). They also recommend establishment of a public-private partnership for modeling cyber risk (CSC 2020, pp. 80-81), and the exploration of a government reinsurance program to cover catastrophic cyber events, similar to TRIA (CSC 2020, pp. 81-82). This dissertation supports these recommendations with some additional suggestions and caveats. The first suggestion is that the FFRDC work with NAIC and other insurance industry associations on the development of underwriting standards to assure consistency in product certification. Also training program should be established for underwriters to guarantee that cyber underwriting standards are adhered to. The public-private partnership on modeling cyber risk is a good idea, but possibly should be expanded to include new

emerging risks as they arise. Finally, a cyber reinsurance program to cover catastrophic cyber events is needed, but the government should work with the private insurers and not undercut the normal development of a private cyber reinsurance market with a non-competitive government solution.

In the current polarized political environment, cybersecurity is one of the few areas with some level of bipartisan consensus. Nearly all lawmakers seem to agree that cybersecurity threats are a national security issue that needs to be dealt with. Regulation may be one solution through the creation of a cyber equivalent to the Nuclear Regulatory Commission or Environmental Protection Agency. However, given growing dislike for government oversight, as demonstrated in the current COVID-19 pandemic, private sector solutions, like insurance, may be more palatable to lawmakers and their constituents. For this reason, policymakers should continue to explore ways that insurance and other private-sector mechanisms can be developed to enhance the safety of new technologies as they emerge in the future.

V. Future Research

The breadth and depth of the data collected for each case study provides wide avenues of opportunity for future research.

Beginning with the HCAD data, a logical first step would be to update the dataset with data for the remainder of 2021. This would include not only data from the OCR Beach Portal, but also additional information from state breach portals, and data on ransomware attacks scraped from key media sources. In addition, a Freedom of Information Act (FOIA) request was submitted to DHHS in March 2021 requesting

access to all breach reports, including reports for breaches of less than 500 records for the period 2015 to 2021. DHHS has approved this request, and this data will be made available in March 2022. This will create a substantial expansion of the HCAD database and allow for a more robust regression analysis of all healthcare breaches between 2015 and 2021. There are also additional fields in HCAD including entities owned by the same company (Group #), HIPAA and State violations and fines by year, lawsuits and settlement amounts by year, and HIPAA violations and settlements prior to 2015 that could be incorporated into new regression analyses. More detailed regression analysis could also focus on specific sub-entities like hospitals, incorporating additional data from the American Hospital Association dataset on all U.S. hospital including number of full time employees, beds, budgets, and other information.

HCAD-R has additional data on ransomware attacks including (if known) ransomware gang, malware used, whether data was leaked (double extortion), number of days of downtime, and whether ransom was paid and the amount. The HCAD-L has additional data on the type of lawsuits, parties involved, and the current status of the lawsuit including whether dismissed, settled or continued. All of this data could be incorporated into a broader study

In addition to HCAD, cyber insurance data was also acquired from the National Association of Insurance Commissioners (NAIC) containing policy, premiums, and claims data from over 600 insurers for the period 2016 to 2020. This data was analyzed using tables, but could be used in future regression analysis looking at loss and combined ratios, claims frequency, and magnitude of claims losses by insurer.

Both the commercial nuclear power and hazardous waste case studies also have future research potential. Both studies in and of themselves would make for interesting journal articles. A data set exists for most reactor liability insurance and could potentially be used in a more robust quantitative analysis. The RCRA data from EPA ECHO database has over a million records for not only TSDFs but also all other facilities under RCRA regulation. The only limitation is finding tools capable of handling such a huge data set. The data could be used for a panel data regression or some type of spatial analysis.

Finally, one future research goal would be to look quantitatively at the interrelationship among insurance, regulation and litigation in optimizing safety. Theoretical papers have been written on this topic but, to date, there have been no identified research done providing empirical evidence of this synergistic connection.

VI. Final Thoughts

Insurance is not a panacea. Insurance is primarily a private sector business, and stakeholders expect the business to be profitable. New emerging technologies represent a business opportunity that many insurers want to exploit. However, this means that insurance companies sometimes make unreasonable and risky business decisions. As most people have experienced, insurers often delay or reject legitimate claims that should be paid. Like other businesses, they sometimes cut corners and under invest in areas necessary to sustain their operations. This includes underwriting and risk assessment. As a result, they may fail to fully understand the risk they insuring. Such was the case in the 1980s when many environmental insurers misestimated the risks associated with

pollution liability, and may be the case in the future with cyber insurance or some other type of emerging technology.

Insurance is also a vital part of the global economy. Over thousands of years, insurance has been an effective business mechanism for managing emerging risks. It allows businesses to separate operating capital from risk capital, freeing up funds to conduct research, develop new innovations, and expand into new markets. Insurance also acts as a private-sector regulator by determining what risks are acceptable and what risks are not. Thus, while insurance can spur development it can also encourage a more cautious approach. Without insurance, many projects would not get off the ground.

Finally, as this dissertation research has documented, insurance plays a role in establishing standards and educating clients on effective risk management practices It also provides tangible incentives for private-sector firms in diverse sectors to invest in safety measures, to not only protect their own assets, but also enhance the collective safety of the public as a whole.

Appendix A: HCAD Healthcare Cyber-Attack Database Spreadsheet (Excel)

Appendix B: HCAD-RW Healthcare Ransomware Attack Worksheet (Excel)

Appendix C: HCAD-L Healthcare Cyber Litigation Worksheet (Excel)

Appendix D: First & Third Party Coverage Key Groups (Excel)

Appendix E: Pre-Breach & Post-Breach Value-Added Services Key Group (Excel)

Appendix F: Performance of Key Groups (Excel)

Appendix G: Regression Descriptive Statistics (Excel)

References

Acton, J. and Dixon, L., "Superfund and Transactional Costs," RAND, R-4132-ICJ, Santa Monica, CA, 1992.

Adler, J. "The fable of the burning river, 45 years later," The Washington Post, June 22, 2014

Adler, J. "Fables of the Cuyahoga: Reconstructing a History of Environmental Protection," Fordham Environmental Law Journal, v. XIV, 2002.

Agency for Healthcare Research & Quality (AHRQ), "Compendium of U.S. Health Systems, 2018," at: here.

Allison, G. et. al., "Governance of nuclear power: A Report to the President's Nuclear Safety Oversight Committee, Washington DC. September 1981.

American Bar Association, "Report of the Commission on Mass Tort," 1989..

American Hospital Association, "Fast Facts on U.S. Hospitals, 2021," 2021 at: here.

American International Companies (AIG), "Cyber-Risk Management for Healthcare Companies," AIG eBusiness Risk Solutions Brochure, 2003.

American Mutual Reinsurance Company (AMRC), Mutual Atomic Energy Reinsurance Participating Agreement, 1956.

American Nuclear Insurers website, "Facility Form," at: here.

American Nuclear Insurers (ANI), "Seabrook Station Nuclear Energy Liability Insurance: ANI Engineering Rating Factor Dollar Cost Analysis Seabrook Nuclear Station," NF-296, 2003.

American Nuclear Society and Institute of Electrical and Electronics Engineers, "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," NUREG/CR-2300, January 1983,

American Physical Society (APS) Panel on Public Affairs, "Renewing Licenses for the Nation's Nuclear Power Plants," 2013.

American Society of Mechanical Engineers (ASME) Boiler and Pressure Vessel Code, Section III(A) "Rules for Construction of Nuclear Vessels:" Codes and Standards at: here.

Anderson-Kill LLP, "A Guide to Insurance Coverage for Environmental Liability Claims," 2019.

Anderson, R. “Why Information Security is Hard (An Economic Perspective),” *Proceeding ACSAC '01 Proceedings of the 17th Annual Computer Security Applications Conference,* IEEE Computer Society, Washington, DC, January 30, 2001.

Asbestos Litigation Crisis in Federal and State Courts: Hearings before the Subcommittee on Intellectual Property and Judicial Administration of the House Judiciary Committee, 102nd Congress (1992).

ASTM International, “Designation: E1903 – 11 Standard Practice for Environmental Site Assessments: Phase II Environmental Site Assessment Process,” October 18, 2011

At-Bay, “Insurance for the Digital Age,” 2021 at: here.

Atomic Archives, “The Manhattan Project: Making the Atomic Bomb Part IV: The Manhattan Engineer District in Operation,” at: here.

Ayers, E. “U.S. healthcare systems face 'increased and imminent' cyber threats: officials,” Advisen FPN, October 30, 2020 at: here.

Ayers, E. “Grim' prospects for the cyber insurance market, Best says,” Advisen,, 2021 at: here.

Baer, W. “Rewarding IT security in the marketplace. Contemporary Security Policy, April 2003.

Baer, W. S., & Parkinson, A. “Cyberinsurance in it security management,” *IEEE Security & Privacy* (2007), (3), 50-56.

Böhme, R.”Cyber-insurance revisited,” In Proceedings of the 4th workshop on the Economics of Information Security, June 2005.

Bohme, R. and Kataria, G. “Models and Measures for Correlation in Cyber-Insurance,” Working Paper: Workshop on the Economics of Information Security (WEIS) , June 2006.

Böhme, R. and Schwartz, G. "Modeling Cyber-Insurance: Towards a Unifying Framework." WEIS, 2010.

Bolot, J. and Lelarge, M. "Cyber Insurance as an Incentive for Internet Security," *Managing information risk and the economics of security*, Springer US, 2009, 269-290.

Braunberg, A. “Multiple drivers for cyber security insurance,” Tech. rep., NSS Labs Nov. 2013

Brown, J., Kroszner, R. and Jenn, B. “Federal Terrorism Risk Insurance,“ NBER Working Paper No. 9271, October 2002..

Bailey, P, Blake, K., Brown, M., Duback, P., Krill, S., Laurenson, J. and Saltzman, J. “The Price-Anderson Act - Crossing the Bridge to the Next Century: A Report to Congress,” NUREG/CR-6617, October 1998.

Bajak, F. "How bad is ransomware? One insurer has dropped coverage for extortion payments," Chicago Tribune, May 7, 2021 at: here.

Bandyopadhyay, T. Mookerjee, V. and Rao, R. "Why IT Managers Don't Go for Cyber-Insurance Products," Communications of the ACM, 52:11, November 2009.

Banham, R. "Hacking It (Cyberinsurance)," CFO Magazine, 16:9, August 1, 2000.

Barrish, R, Antoff, R. and Brabson, J. "Third Party Audit Pilot Project in the State of Delaware Final Report," June 6, 2000.

Bartel, R. "WASH-1400 The Reactor Safety Study: The Introduction of Risk Assessment to the Regulation of Nuclear Reactors," U.S. Nuclear Regulatory Commission, NUREG/KM-0010, Washington DC, August 2016.

Basak, S. and Chiglinsky, K. "Buffett Not Eager for Berkshire to Be Cyber Insurance Leader," May 7, 2018 at: here.

Beauchamp, T. "Hooker Chemical and Love Canal," at: here.

Beaver, W. "Duquesne Light and Shippingport: Nuclear Power Is Born in Western Pennsylvania," Western Pennsylvania Historical Magazine, Vol. 70, No.4 (October 1987).

Belarus Foreign Ministry, "Chernobyl disaster: Why are the consequences still observed? And Why is the international assistance still critical?" April 2009 at: here.

Bell, M. and Davis, D. "Reassessment of the Lethal London Fog of 1952: Novel Indicators of Acute and Chronic Consequences of Acute Exposure to Air Pollution," *Environmental Health Perspectives,* Volume109, Supplement 3, June 2001.

Berger Montague, "Universal Health Services Ransomware Attack Class Action," 2021 at: here.

Berliner, B. "Large Risks and Limits of Insurability," *Geneva Papers on Risk & Insurance* (October 1985): 10(4), 313-329.

Bestsennyy, C. Gilbert, G. & Harris, A. "Telehealth: A quarter-trillion-dollar post-COVID-19 reality?" McKinsey & Company, 2021.

Betterley, R. "The Betterley Report, Cyberrisk Market Survey 2009," June 2009.

Betterley, R. "The Betterley Report: Cyber Insurance for Healthcare Market Survey," October 2020.

Bischoff, P. "Ransomware attacks on US healthcare organizations cost $20.8bn in 2020," Compartech, March 10, 2021 at: here

Boissoneault, L. "The Deadly Donora Smog of 1948 Spurred Environmental Protection—But Have We Forgotten the Lesson?" *Smithsonian,* October 26, 2018.

Brokaw, T. (Reporter), & Ellis, R. (Anchor). 1998, March 17. Former Residents of Love Canal Receive Settlement 20 Years Later. [Television series episode]. NBC Nightly News. at: here,

Bryan, K. and Lamoureux, C. "Data Breach Litigations: 2020 Year in Review," National Law Review, December 28, 2020 at: here.

Buntin, M, Burke, M. Hoaglin, M. and Blumenthal, D. "The Benefits Of Health Information Technology: A Review Of The Recent Literature," Health Affairs; 30:3, March 2011.

Carlson, J. Star Tribune (Minneapolis), "750,000 Medtronic defibrillators vulnerable to Hacking," March 22, 2019.

Carroll, S., Hensler, D. et al. "Asbestos Litigation Costs, Compensation, and Alternatives," Santa Monica, CA: RAND Corporation, 2005.

Carson, R., *Silent Spring*, Boston: Houghton Mifflin, 1962.

Castellano, G. "Governing Ignorance: Emerging Catastrophic Risks— Industry Responses and Policy Frictions," The Geneva Papers, 2010, 35.

Center for Medicare & Medicaid Services (CMS), "Security Standards: Physical Safeguards," 2007, Volume 2 / Paper 3 at: here.

Center for Medicare & Medicaid Services (CMS), "Security Standards: Technical Safeguards 2007A, Volume 2 / Paper 3 at: here .

Cerulus, L. "EU medicines agency says hackers manipulated leaked coronavirus vaccine data," Politico, July 25, 2021 at: here.

CGI, "The Cyber-Value Connection Revealing the link between cyber vulnerability and company value," 2017 at: here.

Chernobyl Forum, "Chernobyl's Legacy: Health, Environmental and Socio-Economic Impacts and Recommendations" 2006 at: here.

Chubb Insurance, "Broadform Liability & Environmental Protect Insurance Policy Schedule and Wording," May 2019.

Chubb/NetDiligence "Cyber Risk Calculator," at: here.

Ciocco, A and Thompson D."A follow-up of Donora ten years after: methodology and findings," *American Journal of Public Health*, 1961; 51(2):155–164.

Clark, D., Berson, T. and Lin, H. (Eds.) *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues,* National Research Council 2014.

Clark, M. "Big tech companies including Intel, Nvidia, and Cisco were all infected during the SolarWinds hack," December 21, 2020 at: here. Clarke, R. and Knake, R. *Cyber War: The Next Threat to National Security and What to Do About It*, Harper Collins, USA, 2010.

Clements, J. “Case Study Remediation of Three Mile Island Unit 2 in Preparation for Decommissioning,” March 2018.

Clinton, L. “Cyber-insurance metrics and impact on cyber-security,” Internet Security Alliance, 2012

Coalition, “Cyber Insurance Claims Report,” H1 2020 at: here

Collin, R.W. “The Environmental Protection Agency: Cleaning Up America's Act,” Greenwood Press, 2006.

Congressional Budget Office (CBO) Paper, The Effects of Tort Reform: Evidence from the States, June 2004 for a summary of study results and impact on insurance

Contos, B. “Ransomware attacks force hospitals to stitch up networks,” CSO Online, May 19, 2016 at: here.

CPrime Studios, “Hospital cybersecurity checklist, 2020 at: here.

Cronin, A. “How Global Communications Are Changing the Character of War.” *The Whitehead Journal of Diplomacy and International stations*, Winter/Spring 2013.

CrowdStrike, “2021 Global Threat Report,” 2021.

Crowley, R. & Freeman, C. “A History of Aviation Insurance” at: here

Cyber Risk Management (CyRiM) Project, “Bashe attack: Global infection by contagious malware,” 2019 at: here.

Cyberspace Solarium Commission (CSC), “Cyberspace Solarium Commission Report,” March 2020 at: here.

Cyberspace Solarium Commission (CSC), “2021 Annual Report on Implementation,” August 2021 at: here

Cybersecurity & Infrastructure Security Agency (CISA), “Cybersecurity Insurance Industry Readout Reports,” accessed January 24, 2022 at: here

Dabkowski, C. “A history of the Love Canal disaster, 1893 to 1998,” *The Buffalo News*, August 4, 2018 at: here

Dahlstrom, K., Skea, J. and Stahel, W. “Innovation, Insurability and Sustainable Development: Sharing Risk Management between Insurers and the State,” *The Geneva Papers on Risk and Insurance* (July 2003), 28(3), 394–412.

Danzig, R. “Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America’s Cyber Dependencies,” Center for a New American Security, July 2014.

DataBreaches.net, “Leon Medical Center issues statement about ransomware attack,” January 9, 2021 at: https://www.databreaches.net/?s=Leon+Medical

Davis, J. “Another COVID-19 Research Firm Targeted by Ransomware Attack,” HealthITSecurity, April 8. 2020 at: here.

Davis, J. "UCSF Pays $1.14M to NetWalker Hackers After Ransomware Attack," HealthITSecurity, June 29. 2020 at: here.

Davis, J. "US Ransomware Attacks Doubled in Q3; Healthcare Sector Most Targeted," HealthITSecurity, October 7. 2020 at: here.

Davis, J. "OCR Warns of Global Supply-Chain Cyberattacks Via SolarWinds Orion," HealthITSecurity, December 15, 2020 at: here.

Deed between Hooker Chemical and the Niagara Falls Board of Education, April 28, 1953.

Depalma, A. "Love Canal Declared Clean, Ending Toxic Horror," *New York Times*, March 18, 2004 at: here

Dictionary.com, "Mitigation," accessed September 25, 2016 at: here

Drees, J. "150,000 security cameras hacked, exposing footage from Halifax Health, other hospitals," Becker Health IT, March 10, 2021 at: here.

Dudley, R. "The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks," ProPublica, August 27, 2019 at: here

Eisenhower, D. "Address before the General Assembly of the United Nations on Peaceful Uses of Atomic Energy," New York City, December 8, 1953.

EPA (1980), "Hazardous Waste and Consolidated Permit Regulations," May 19, 1980.

EPA (1981), "Announces First 114 Top-Priority Superfund Sites" EPA press release - October 23, 1981 at: here.

EPA (1982A), "Environmental Monitoring at Love Canal," EPA-600/4-82-030a May 1982.

EPA (1982B), "Liability Coverage: Requirements for Owners and Operators of Hazardous Waste Treatment, Storage, and Disposal Facilities. A Guidance Manual," SW-961, November 1982.

EPA (1988), "Times Beach Record of Decision Signed," Press Release, September 30, 1988.

EPA (1993), "Factbook: National Priorities List Under the Original Hazard Ranking System 1981-1991" Publication 9320.7-08, October 1993.

EPA (2019) Office of Enforcement and Compliance Assurance, "Fiscal Year 2018 EPA Enforcement and Compliance Annual Results," February 8, 2019 at: here.

EPA (2020A), "History of the Clean Water Act, accessed April 20, 2020 at: here.

EPA (2020B), "A Brief Summary of the History of NPDES," at: here.

EPA (2020C), "Types of Brownfields Grant Funding," accessed April 20, 2020 at here.

EPA (2020D), "Underground Storage Tanks: State Financial Assurance Funds," accessed April 20, 2020 at: here.

Ericson, R., Doyle, A. and Barry, D. *Insurance as Governance*, Toronto University Press, 2003, 1-414.

Evans, M. and McMillan, R. "Cyberattacks Cost Hospitals Millions During Covid-19," The Wall Street Journal, February 26, 2021 at: here.

Faure, M. "The complementary roles of liability, regulation and insurance in safety management: theory and practice," Journal of Risk Research, 2014, 17:6, 689-707.

Faure, M and Fiore, K. "The Coverage of the Nuclear Risk in Europe: Which Alternative?" The Geneva Papers (2008), 33, 288–322.

Federal Register Vol. 43, No. 243-Monday, December 18, 1978, EPA, Hazardous Waste Guidelines, Proposed Rules p. 58987; and EPA Hazardous Waste and Consolidated Permit Regulations, May 19, 1980.

Federal Register Vol. 47, No. 134, Tuesday, July 13, 1982, " EPA "Standards Applicable To Owners and Operators of Hazardous Waste Treatment, Storage, and Disposal Facilities; Liability Coverage Requirements."

FEMA.gov "What is Mitigation," accessed September 25, 2016 at: here

FireEye, "Beyond Compliance: Cyber Threats and Healthcare," 2019 at: here

Frankoff, S. and Hartley, B. "Big Game Hunting: The Evolution of INDRIK SPIDER From Dridex Wire Fraud to BitPaymer Targeted Ransomware," CrowdStrike, 2018 at: here.

Fuller, J. "We Almost Lost Detroit," Reader's Digest Press, New York, 1975. *Geneva Papers* (2008), 33, 288–322.

Gallagher Healthcare Practice, "Medical Device Cybersecurity Regulatory Oversight & Insurance Considerations, September 2017.

Geers, K. "The challenge of cyberattack deterrence." *Computer Law & Security Rev,* 2010, 26: 298–303.

Georgia Court of Appeals, Institute of Nuclear Power Operations (INPO) v. Cobb County Board of Tax Assessors," #A98A2077-A98A2084, decided January 05, 1999.

General Accounting Office (GAO 1987), "Hazardous Waste: Issues Surrounding Insurance Availability," Report to Congress, October 1987.

General Accounting Office (GAO 1988), "Hazardous waste: the cost and availability of pollution insurance: report to the chairman, Subcommittee on Environment, Energy, and Natural Resources, Committee on Government Operations, U.S. House of Representatives." Washington DC, October 1988.

Goldzweig, C. Towfigh, A. Maglione, M. and Shekelle, P. "Costs And Benefits Of Health Information Technology," Health Affairs, 28, 2009.

Gordon, L. A., Loeb, M. P., & Sohail, T. "A framework for using insurance for cyber-risk management," *Communications of the ACM* (2003), 46(3), 81-85.

Grand River Lime Company v. Ohio Casualty Insurance Company, 32 Ohio App. 2d 178, 289, N.E.2d 360 (1972).

Gruson, L. "Ex-Love Canal Families Get Payments: Ex-Love Canal Residents Pick Up Their Shares," *New York Times,* February 20, 1985

Hale, M.; Bailey, P. E. (1988). The RCRA Financial Responsibility Program for Hazardous Waste Facilities: Program Fundamentals and Current Developments. Environmental Claims Journal, 1(2).

Hardin, G. "The Tragedy of the Commons". *Science (AAAS)* (December 13, 1968), 162 (3859): 1243–1248.

Hartford Steam Boiler Inspection and Insurance Company HSB Total Cyber™ Rate and Rule Explanatory Memorandum, 2016.

Hartford Steam Boiler (HSB) Inspection and Insurance Company HSB Total Cyber™ Rate and Rule Manual, 2020.

Hartford Steam Boiler (HSB) Inspection and Insurance Company HSB Total Cyber™ Rate and Rule Manual, 2021.

Hatch M., Beyea, J, Nieves JW, and Susser M. "Cancer near the Three Mile Island nuclear plant: radiation emissions," American Journal of Epidemiology, September 1990, 132(3).

Healey, J. (ed.), *A Fierce Domain: Conflict in Cyberspace 1986 to 2012,* Cyber Conflict Studies Association, 2013.

Healey, J. "Risk Nexus Beyond data breaches: global interconnections of cyber risk," Atlantic Council, April 2014.

Health Care Cybersecurity Task Force (HCIC), "Report on Improving Cybersecurity in the Health Care Industry," June 2017.

HealthIT.gov, "Office-based Physician Electronic Health Record Adoption," 2017, at: here.

HealthIT.gov, "Security Risk Assessment Tool," 2021, at: here.

Herbeck, D. "Insurance to Cover Occidental's Cleanup Costs," *The Buffalo News,* June 25, 1996 at: here..

Herath, H., & Herath, T. "Copula-based actuarial model for pricing cyber-insurance policies," *Insurance Markets and Companies: Analyses and Actuarial Computations* (2011), 2(1), 7-20

Hickman, H. L. "Activities of the Office of Solid Waste Management Programs Fiscal Year 1975 Annual Report," EPA, October 1975.

Hicks, J. "Atoms for Peace: The Mixed Legacy of Eisenhower's Nuclear Gambit," Science History Institute, summer 2014.

Higgins, K. "Medical Industry Under Attack By Chinese Hackers," Dark Reading, March 14, 2013, at: here.

Hines, N.W., "Nor Any Drop to Drink: Public Regulation of Water Quality Part I: State Pollution Control Programs, 52 *Iowa Law Review,* 186 (1966).

HIPAA Journal, "Shareholder Sues LabCorp to Recover Losses Caused by Data Breaches," May 1, 2020 at: here.

HIPAA Journal, "Voicemail Phishing Scam Identified Targeting Remote Healthcare Workers," June 8, 2020 at: here.

HIPAA Journal, "Sen. Warner Seeks Answers about Suspected Universal Health Services Ransomware Attack, October 14, 2020 at: here.

HIPAA Journal, "Largest Healthcare Data Breaches in 2020," January 1, 2021 at: here.

Hoffmann, A. "Internalizing externalities of loss prevention through insurance monopoly," *Proc. Annual Meeting of American Risk and Insurance Association*, Washington DC, Aug 2006.

Hourihan, J. "Insurance Coverage for Environmental Damage Claims," *The Forum* (American Bar Association Section of Insurance, Negligence and Compensation Law), 15:4, Spring 1980.

Humpstone, C. "Pollution Insurance Comes of Age," *Risk Management Magazine*, August 1977

Hutter, B. "The Role of Non-State Actors in Regulation," Economic and Social Research Council, Discussion Paper No. 37, April 2006.

IBM Global Services, "IBM Security Services 2014 Cyber Security Intelligence Index," June 2014.

Ikeda, S. "Phishing Attack Targets Vaccine Supply Chain; Linked to Charitable Gavi Project, Attempts Recorded Throughout Europe and Asia," CPO Magazine, 2020 at: here.

Institute of Nuclear Power Operations (INPO) SOER 02-4, "Reactor Pressure Vessel Head Degradation at Davis-Besse Nuclear Power Station," November 2002.

Institute of Nuclear Power Operations (INPO), 2020 at: here.

Insurance Information Institute (IIIA), "Insurance Information Fact Book 2015..

International Atomic Energy Agency (IAEA), "IAEA, Statute as Amended, 1989 at: here.

International Atomic Energy Agency (IAEA), "IAEA Safety Standards: Functions and Processes of the Regulatory Body for Safety General Safety Guide," GSG-13, Vienna, Austria, 2018.

International Atomic Energy Agency (IAEA), "International Nuclear and Radiological Event Scale (INES)," 2020 at: here.

International Atomic Energy Agency (IAEA), "Safety Standards," at: here.

International Research and Technology Corporation (IR&TC), "Hazardous Waste Management Issues Pertinent to Section 3004 of the Resource Conservation and Recovery Act of 1976," EPA Report SW-183c, 1979.

International Organizations of Standards (2020), "ISO 14000 family –Environmental Management," accessed April 20, 2020 at: here.

IRMI, "A Big Picture on Environmental Insurance," accessed April 20, 2020 at: here.

Ives, A, "Chapter 2 Love Canal" in *The Market Meets the Environment: Economic Analysis of Environmental Policy*, 1999.

Jaffee, D. and Russell, T. "Should Governments Provide Catastrophe Insurance?" Fisher Center for Real Estate and Urban Economics, UC Berkeley, September 1, 2005.

Jackson Township Municipal Utilities Authority v. Hartford Accident and Indemnity Company N.J. Super. L. 451 A.2d 990 (1982).

Jedicke, P. "The NRX Incident," 1989 at: here.

Jenkins v. Raymark Industries, Inc., 109 F.R.D. 269 (E.D.Tex. 1985)

Jercich, K. "Telehealth poses big cybersecurity dangers, Harvard researchers warn," 2020 at: here.

Johnson, A. "WannaCry: Ransomware attacks show strong links to Lazarus group," 2017 at: here.

Johnson, K. "EPA Formally Recognizes ASTM E1527-13 as Compliant with CERCLA's All Appropriate Inquiry Rule," 2014 at: here

Joint Committee on Atomic Energy (JCAE), "Hearings on S.3323 and H.R.8862 to Amend the Atomic Energy Act of 1946" 83rd Congress, 2nd Session, 1954.

Joint Committee on Atomic Energy (JCAE), "Hearings on Atomic Energy Development, Growth, and State of the Atomic Energy Industry" 84th Congress, 1st Session, 1955.

Joint Committee on Atomic Energy (JCAE), "Hearings on Governmental Indemnity for Private Licensees and AEC Contractors against Reactor Hazards," 84th Congress, 2nd Session on May15 to 21 and June 14, 1956.

Joint Committee on Atomic Energy (JCAE),"Hearings on Government Indemnity and Reactor Safety" 85th Congress, 1st Session March 25-27, 1957.

Joint Committee on Atomic Energy (JCAE), "Hearing on Nuclear Energy Liability Policy," 85th Congress, 1st Session, March 1957.

Joint Committee on Atomic Energy (JCAE), "Hearings on the Development, Growth, and State of the Atomic Energy Industry," 86th Congress, 2nd Session, January 1960.

Joint Committee on Atomic Energy (JCAE), "SL-1 Accident: Atomic Energy Commission Investigation Board Report," 87th Congress, 1st Session, June 1961.

Joint Committee on Atomic Energy (JCAE), "Hearings on Proposed Extension of AEC Indemnity Legislation" 89th Congress, 1st Session, Washington, DC, June 22-24, 1965.

Joint Committee on Atomic Energy (JCAE), "Extending and Amending the Price-Anderson Indemnity Provisions of the Atomic Energy Act of 1954, as amended," 89th Congress, 1st Session, Report 883, August 26, 1965.

Joint Committee on Atomic Energy (JCAE), "Proposed Amendments to Price-Anderson Act Relating to Waiver of Defenses" 89th Congress, 2nd Session, July 19-21, 1966.

Joint Committee on Atomic Energy (JCAE-A), "Hearings on Browns Ferry Nuclear Plant Fire," 94th Congress, 1st Session, September 16, 1975.

Joint Committee on Atomic Energy (JCAE-B), U.S. Congress, "Hearing on H.R. 8631 to Amend and extend the Price-Anderson Act" 94th Congress, 1st Session, September 23-24, 1975.

Kammer, R. (1982) "Letter from National Bureau of Standards, sent to Senators Daniel Moynihan and Alfonse D'Amato and Congressman John LaFalce." August. 30, 1982,

Kaufman, G. & Scott, K. "What is Systemic Risk, and Do Bank Regulators Retard or Contribute to It?" *The Independent Review* (2003), 7(3).

Keller, W. and Modarres, M. "A historical overview of probabilistic risk assessment development and its use in the nuclear power industry," Reliability Engineering & System Safety, 89, 2005.

Kemeny, J. et al. "The President's Commission on the Accident at Three Mile," Washington, DC October 1979.

Kesan, J., Majuca, R., & Yurcik, W. "Cyberinsurance as a market-based solution to the problem of cybersecurity: a case study," In Proc. WEIS, June 2005.

Kimball, K. "Chapter 2 Insurance for Replacement Power Costs " Staff Studies Nuclear Accident at Three Mile Island Special Report. January 1, 1982.

Kleindorfer, P. and Kunreuther, H. "Challenges Facing the Insurance Industry in Managing Catastrophic Risks," *The Financing of Catastrophe Risk*, Chapter 4, University of Chicago Press, 1999.

Krepinevich, A. "Cyber Warfare: A "Nuclear Option?" Cen. for Strategic and Budgetary Assess., 2012

Kronenberg, W. "The Environmental Insurance Markets in the U.S. and Western Europe: A U.S. Underwriter's Observations," The Geneva Papers on Risk and Insurance, 20 (No. 76, July 1995).

Kshetri, N. “Pattern of global cyber war and crime: A conceptual framework” J. of International Management 11 2005.

Kunreuther, H. “The Role of Insurance in Managing Extreme Events: Implications for Terrorism Coverage,” *Risk Analysis* Vol. 22 No. 3, June 2002.

Kunreuther, H. and Heal, G. “Interdependent Security.” *J. of Risk and Uncertainty,* 2003, 26:2/3, 231-49.

Lahnstein, C. “The Insurability of New Liability Risks,” *The Geneva Papers on Risk and Insurance* (July 2004), 29(3), 512–517.

Landow-Esser, J. and Spears, K.C. “Insurance coverage for environmental claims,” *Journal of Property Management*, 57(3), 1992.

Lansco, Inc. A New Jersey Corporation, Plaintiff, v. The Department of Environmental Protection of the State of New Jersey, et al. Decided December 4, 1975. at: here.

Lear, L. “Rachel Carson's "Silent Spring" *Environmental History Review,* 17:2 (Summer 1993).

Lee, B. “Ransomware: Unlocking the Lucrative Criminal Business Model,” Palo Alto Networks, Unit 42, 2018.

LeLarge, M & Bolot, J. “Economic Incentives to Increase Security in the Internet: The Case for Insurance,” IEEE INFOCOM 2009.

Lemos, R. “'Act of War' Clause Could Nix Cyber Insurance Payouts,” Dark Reading, October 29, 2020 at: here.

Libicki, M. “The Specter of Non-Obvious Warfare,” *Strategic Studies Quarterly* (Fall 2012), 88-101.

Liu, A. “AstraZeneca staffers targeted in suspected hacking scheme amid work on COVID-19 vaccine: report,” November 30, 2020 at: here.

Liu, A. “Hackers breach Pfizer/BioNTech COVID-19 vaccine data in cyberattack targeting EMA,” FiercePharma, December 10, 2020 at: here.

Lloyd’s, “Glossary,” 2017 accessed at: https://www.lloyds.com/common/help/glossary?Letter=I

Lochbaum, D. “Reactor Core Damage: Power Excursion,” at: here.

Majuca, R., Yurcik, W., and Kesan, J. “The Evolution of Cyberinsurance,” in *Securing Privacy in the Internet Age* (2005) at: here.

Marotta, A., Martinelli, F., Nanni, S., & Yautsiukhin, A. “A Survey on Cyber-Insurance,” IIT TR-17/2015, Technical Report, November 2015.

Marsh & Microsoft, “2019 Global Cyber Risk Perception Survey,” September 2019: here

Masonite Corporation. v. Great American Surplus Lines Insurance Co. (224 Cal. App. 3rd, 912, 1990).

Mazur, A. *Hazardous Inquiry: The Rashomon Effect at Love Canal*, Harvard University Press, Cambridge, MA, 1998

Mazuzan, G. and Walker, J. "Controlling the Atom: The Beginnings of Nuclear Regulation, 1946-1962," 1984.

McClure, R., "A Review of Nuclear Energy Insurance," 1968 at: here.

McClure, R. "An Actuarial Note on Experience Rating Nuclear Property Insurance," Proceedings of the Casualty Actuarial Society (PCAS), 49:112, November 1972.

McGee, K. "$115 Million Settlement in Massive Anthem Breach Case," BankInfoSec, June 23, 2017 at: here.

Meixler, E. "Japan Acknowledges the First Radiation-Linked Death From the Fukushima Nuclear Disaster," Time Magazine, September 6, 2018 at: here.

Morrison Foerster, "Privacy Litigation 2020 Year in Review: Data Breach Litigation," January 4, 2021 at: here.

Morse, S. "Healthcare's number one financial issue is cybersecurity, Healthcare Finance, July 30, 2019 at: here.

Mukhopadhyay, A., Chatterjee, S., Roy, R., Saha, D., Mahanti, A., & Sadhukhan, S. "Insuring big losses due to security breaches through Insurance: A business model," in Proceedings of 40th Annual Hawaii International Conference on System Sciences (HICSS 2007).

Mulligan, D. and Schneider, F. "Doctrine for Cybersecurity," *Daedalus* (September 2011), 140(4):70–92.

MunichRE Website (2016). HSB "The history of Hartford Steam Boiler," at: here.

Munich Re, "Pioneering cyber insurance: Munich Re partners with Google Cloud and Allianz," March 2, 2021 at: here.

Murphy, A. "Financial Protection Against Atomic Hazards," Report for the Atomic Industrial Forum by the Legislative Drafting Research Fund of Columbia University, January 1957.

Murphy, K. "Have the EHR Incentive Programs Reached a Stagnation Point?" HER Intelligence, January 5, 2016 at: here. .

NAIC System for Electronic Rates & Forms Filings (SERFF) at: here.

National Association of Insurance Commissioners (NAIC), "Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement," December 4, 2020 at: here.

National Conference of State Legislatures (NCSL), "Security Breach Notification Laws," accessed August 25, 2021 at: here.

National Cyber Security Centre (NCSC), "Advisory: APT29 targets COVID-19 vaccine development," 2020 at: here.

National Institute of Standards and Technology (NIST*), Framework for Improving Critical Infrastructure Cybersecurity Version 1.0*, February 12, 2014.

National Institute of Standards & Technology (NIST), "Cybersecurity Framework, 2021 at: here.

Navigant Consulting, "Assessment of the Nuclear Power Industry – Final Report," June 2013.

NetDiligence, "Cyber Claims Study 2020 Report," 2020, Version 1.1.

New York Department of Health, "Love Canal: Public Health Time Bomb, a special report to the governor and legislature," September 1978.

New York State Department of Health (NYSDH), "Love Canal: A Special Report to the Governor & Legislature: April 1981," at: here.

Niagara County v. Utica Mutual Insurance, Supreme Court, Niagara County, April 14, 1980, 103 Misc. 2d 814 (N.Y. Misc. 1980).

NJCCIC, "Ransomware," 2021 at: here.

Nuclear Energy Liability Insurance Association (NELIA), "Constitution of the Nuclear Energy Liability Insurance Association," adopted May 9, 1956.

Nuclear Electric Insurance Limited (NEIL), "Policy Holder Disclosure and Payment for Acts of Terrorism Endorsement," 2002.

Nuclear Electric Insurance Limited (NEIL), "2001 Annual Report," Wilmington, DE 2002.

Nuclear Electric Insurance Limited (NEIL), "2012 Annual Report," Wilmington, DE, 2013

Nuclear Electric Insurance Limited (NEIL 1999-2019), "Primary Property and Decontamination Liability Insurance Policy," #P99-075 to #P15-075 October 1, 1999 to April 1, 2020.

NUCO FC&S Expert Coverage Interpretation, "CY 00 01 01 18 Commercial Cyber Insurance Policy," April 10, 2019 at: here.

Nye Jr, Joseph, "Nuclear lessons for cyber security," Air University Press, 2011.

OECD, "Enhancing the Role of Insurance in Cyber Risk Management," Dec. 8, 2017 at: here.

Office of Technology Assessment, U.S. Congress, "Coming Clean, Superfund Problems Can Be Solved," U.S. Government Printing Office, Washington, D.C., October 1989.

Oliveira, R. “American Nuclear Insurers: Industry Radio Active Waste Experiences,” Proceedings of the Symposium on Waste Management at Tucson, Arizona February 28-March 3, 1988, Vol. 1 Low Level Waste.

Omang, J. “EPA Names 115 Worst Toxic Waste Dump Sites in U.S.,” *The Washington Post*, October 24, 1981.

Onge, K. “First Auto Policy Sold 110 Years Ago Today,” *Insurance J*, February 27, 2008 at: here

O’Tool, T. “Soviet Approach to Nuclear Safety Is 'Different,” WA Post, October 1978 at: here.

Owens, W., Dam, K. and Lin, H. (eds.) *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*,” National Research Council, 2009.

Paignen, B. “Health Hazards at Love Canal,” Roswell Park Memorial Institute, January 1979.

Pate, Z. “INPO's impact in the USA,“ IAEA Bulletin, Autumn 1986.

Peltier, R. “Dominion’s North Anna Station Sets New Standard for Earthquake Response,” Power Magazine, October 31, 2012.

Percival, R. “Environmental Federalism,” Maryland Law Review, 54(4), 1995.

Philadelphia Indemnity Insurance Co. “Environmental Liability and Remediation Expense Coverage,” Policy PI-EVP-002 (2009).

PolicyAdvise website accessed August 20, 2021 at: here.

Ponemon Institute/IBM, “Cost of a Data Breach Report 2020,” July 2020.

Poulsen, K., McMillan, R. & Volz, D. “SolarWinds Hack Victims: From Tech Companies to a Hospital and University,” The Wall Street Journal, December 21, 2020 at: here.

President’s Commission on Critical Infrastructure Protection (PCCIP), *The Report of the President’s Commission on Critical Infrastructure Protection*, Washington, DC, October 1997.

PropertyandCasualty.com “ICSA Offers Hacker Insurance to Companies Certified Through Its TruSecure Program,” June 15, 1998 at: here.

PropertyandCasualty.com “AIG Unit Creates E-Business Security Panel for Insureds,” January 18, 2000 at: here.

Public Law 55-425 (P.L. 55-425), “The Refuse Act of 1899,” 55th Congress, 1st Session, March 3, 1899.

Public Law 79-585 (P.L. 79-585), “The Atomic Energy Act of 1946,” 79th Congress, 1st Session, August 1, 1946.

Public Law 83-703 (P.L. 83-703), "The Atomic Energy Act of 1954: An Act to amend the Atomic Energy Act of 1946, as amended, and for other purposes," 83rd Congress, 2nd Session, August 30, 1954.

Public Law 85-256 (P.L. 85-256), "An Act to Amend the Atomic Energy Act of 1954 - Price–Anderson Nuclear Industries Indemnity Act," 85th Congress, 1st Session, Sept. 2, 1957.

Public Law 89-210 (P.L. 89-210), "An Act to Amend the Atomic Energy Act of 1954 (as amended)" 89th Congress, 1st Session, September 29, 1965.

Public Law 89-645 (P.L. 89-645), "An Act to amend to Atomic Energy Act of 1954, as amended," U.S. Congress passed October 13, 1966.

Public Law No. 91-190 (P.L. 91-190), "National Environmental Policy Act of 1969," 91st Congress, 1st Session, January 1, 1970.

Public Law No. 91-604 (P.L. 91-604), "Clean Air Amendments Act of 1970," 91st Congress, 2nd Session, December 31, 1970.

Public Law 93-438 (P.L. 93-438), "Energy Reorganization Act of 1974," 93rd Congress, 2nd Session, October 11, 1974.

Public Law 94-197 (P.L. 94-197), "An Act to amend the Atomic Energy Act of 1954, as amended," 94th Congress, 2nd Session, December 31, 1975.

Public Law 94-580 (P.L. 94-580), "Resource Conservation and Recovery Act of 1976," 94th Congress, 2nd Session, October 21, 1976.

Public Law 95-510 (P.L. 95-510), "Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA) of 1980,' 42 USC 9601, December 11, 1980.

Public Law 99–499 (P.L. 99-499), "Superfund Amendments and Reauthorization Act (SARA) of 1986," 99th Congress, 2nd Session, October 17, 1986.

Public Law 100-408 (P.L. 100-408), "Price-Anderson Amendment Act of 1988," 100th Congress, 2nd Session, August 20, 1988.

Public Law 104-191, "Health Insurance Portability and Accountability Act," 1996, text at: here.

Public Law 107-297 (P.L. 107-297), `Terrorism Risk Insurance Act of 2002," 107th Congress, 2nd Session, enacted November 26, 2002.

Public Law 108-117 (P.L. 108-117), "2003 Consolidated Appropriations Resolution," 108th Congress, 1st Session, February 20, 2003.

Public Law 109-58 (P.L. 109-58), "Energy Policy Act, Title VI, Nuclear Matters, Subtitle A—Price-Anderson Act Amendments," 109th Congress, 1st Session, August 8, 2005.

Pal, R. “Cyber-Insurance for Cyber-Security: A Solution to the Information Asymmetry Problem,” Preprint submitted to SIAM Annual Meeting May 22, 2012.

Pal, R., & Hui, P. (2013, May) “On differentiating cyber-insurance contracts a topological perspective,” in proceeding of 2013 IFIP/IEEE International Symposium, May 2013, 836-839.

Radetzki, M. and Radetzki, M. “Private Arrangements to Cover Large-scale Liabilities Caused by Nuclear and Other Industrial Catastrophes,” *The Geneva Papers on Risk and Insurance* (April 2000), 25(2), 180-195.

RANDMark40 “A Brief History of Insurance,” accessed September 26, 2016 at: here

Reed, T. “Cyberattack on Universal Health Services in September cost health system $67M last year,” Fierce healthcare, February 26, 2021 at: here

Rees, J. “Hostages of Each Other: The Transformation of Nuclear Safety since Three Mile Island,” The University of Chicago Press, Chicago. 1994.

RegisteredNursing.org, “What is Meaningful Use?” 2021 at: here.

Riehl v. Travelers Insurance Company, Civil Action No. 83-0085, Western District Court, Pennsylvania, 1984.

Reindl, J.C. “Did we really 'almost lose Detroit' in Fermi 1 mishap 50 years ago?” Detroit Free Press, October 9, 2016.

Reisch, M. “A legislative history of the Comprehensive Environmental Response, Compensation, and Liability Act of 1980 (Superfund), Public Law 96-510 prepared by the Environment and Natural Resources Policy Division of the Congressional Research Service of the Library of Congress, for the Committee on Environment and Public Works, U.S. Senate, Washington : U.S. G.P.O., 1983.

Reuters, “South Texas 2 nuclear unit enters final repair stage,” April 5, 2012.at here.

Romanosky, S., Ablon, L. Kuehn, A. Jones, T. “Content Analysis of Cyber Insurance Policies How Do Carriers Price Cyber Risk?” April 20, 2019 at: here.

Rosenkranz, E. (1986) “The pollution exclusion clause through the looking glass,“ *Georgetown Law Journal*, 74(4).

Rossi, M. “First-Party E-Commerce Risks,” IRMI June 2000 at: here.

Rowe, W. *An Anatomy of Risk*, New York, John Wiley & Sons, 1977..

Rufford, N. Leppard, D. and Eddy, P. “Nuclear Mystery: Crashed plane's target may have been reactor,” Sunday Times, London, October 21, 2001.

Sack, H., “The Story of the Morris Worm – First Malware hits the Internet,” Sci-Hi Blog, November 2018, accessed August 25, 2021 at: here.

Schmidt, E. (August 2010) Attributed Quote

Schneider, B. “Computer security: It's the economics, stupid,” Paper presented at the 1st Annual Workshop on Economics of Information Security, Berkeley, CA, 2002.

Schwartz, G., Shetty, N., & Walrand, J. “Cyber-Insurance: Missing market driven by user heterogeneity preparation,” 2010 at: www.eecs.berkeley.edu/nikhils/SecTypes.pdf.

Schwartz, G. & Sastry, S. “Cyber-insurance framework for large scale interdependent networks,” Proc. of the 3rd Intl. Conf. on High Confidence Networked Systems, ACM, April 2014, 145-154.

Seals, T. “WHO Targeted in Espionage Attempt, COVID-19 Cyberattacks Spike,” ThreatPost, March 24, 2020, at: here.

Shavell, S. “A model of optimal use of liability and safety regulation.” *RAND Journal of Economics*, 15:2, Summer, 1984, pp. 271-280.

Sherman, C. et al. “The Forrester New Wave: Connected Medical Device Security, Q2 2020 The Eight Providers That Matter Most And How They Stack Up,” June 11, 2020 at: here.

Shetty, Nikhil, Schwartz, G. Felegyhazi, M. and Walrand. J. "Competitive cyber-insurance and internet security," *Economics of Information Security and Privacy*, Springer US, 2010. 229-247.

Sideris, A., Hockenbury, R. Yeater, M. and Vesely, W. “Nuclear Plant Fire Incident Data File" Nuclear Safety, 20:3, May-June 1979

Simon, B. “Environmental Insurance Coverage under the Comprehensive General Liability Policy: Does the Personal Injury Endorsement Cover CERCLA Liability?” *UCLA Journal of Environmental Law and Policy*, 12(2), 1994.

Singer, P. and Friedman, A. *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, 2013

Sinha, S., “State of IoT 2021: Number of connected IoT devices growing 9% to 12.3 billion globally, cellular IoT now surpassing 2 billion,” September 22, 2021 at: here

Smith, B. and Ganning, P. “EPA and OSHA Penalty Increases*,” Environmental Law and Policy Monitor*, January 21, 2020 at: here.

Smith, R. “Deep Panda: PRC Cyber Militia Conducts Shaping Operations?” The Counter Terrorist ~ June/July 2015.

Soderstrom, R. “The Role of Insurance in Environmental Litigation,” *The Forum* (American Bar Association. Section of Insurance, Negligence and Compensation Law), Vol. 11, No. 3 (Spring 1976), p. 765-766.

Songini, M. “Hospital Confirms Hacker Stole 5,000 Patient Files,” Computer World, December 18, 2000 at: here.

Spitzner, l. “This is Why The Human is the Weakest Link,” SANS. January 1, 2021 at: here.

Stubbs, J. “Exclusive: Suspected North Korean hackers targeted COVID vaccine maker AstraZeneca – sources,” Reuters, November 27, 2020 at: here.

Starr, C. and Whipple, C. “Coping with Nuclear Power Risks: The Electric Utility Incentives,” Nuclear Safety, Vol. 23, No. 1, January- February 1982.

Strauss. L. Chairman, United States Atomic Energy Commission, “Remarks Delivered at the Founders’ Day Dinner, National Association of Science Writers, on Thursday, September 16, 1954, New York, New York at: here.

South Texas Project Excellence Plan, Revision 1” September 1, 2016.

State of New York v. Occidental Petroleum Corp., No. 41006, N.Y. Sup. Ct., filed Apr. 28, 1980.

Stern, A, “History of Air Pollution Legislation in the United States,” *Journal of the Air Pollution Control Association*, 1982, 32:1.

Sweeney, E. “CMS increases Healthcare.gov breach total to 93,600,” Fierce Healthcare, 2018 at: here.

SwissRE, “A History of Insurance,” 2013, accessed September 26, 2016 at: here

Team RiskIQ, “RISKIQ I3 Intelligence Brief: Ransomware in Health Sector 2020: A Perfect Storm of New Targets and Methods,” April 9, 2020.

Techalloy Co. v. Reliance Insurance. Company, 338 Pennsylvania Super. 1, 487 A.2d 820 (1984)

TEPCO Press Release, “TEPCO to invest in South Texas Project expansion (STP 3&4) - First Japanese utility to invest in the overseas nuclear power project,” May 10, 2010.

Thatcher. T. “The Truth about the SL-1 Accident — Understanding the Reactor Excursion and Safety Problems at SL-1,” at: here.

ThaiCERT, “Threat Group Cards: A Threat Actor Encyclopedia,” 2021 at: here.

The Guardian, “US hospital systems facing 'imminent' threat of cyber-attacks, FBI warns,” October 29, 2020 at: here.

The White House, “Improving Critical Infrastructure Cybersecurity,” Executive Order 13636: Preliminary Cybersecurity Framework. February 12, 2013.

Tieman, J. “Invasion of the 'love bug'. Modern Healthcare; Chicago Vol. 30, Issue 19, (May 8, 2000): 16.

Tondel, I., Meland, P., Omerovic, A., Gjaere, E. and Solhaug, B. “Using Cyber-Insurance as a Risk Management Strategy: Knowledge Gaps and Recommendations for Further Research,” SINTEF Report, November 2015.

Toregas, C. and Zahn, N. “Insurance for Cyber Attacks: The Issue of Setting Premiums in Context,” George Washington Univ. Cyber Security Policy and Research Inst., January 14, 2014

Townsend, K. at: “Medical Practice Closing Permanently After Ransomware Attack, 2019, at: here.

Trend Micro, “A Constant State of Flux: Trend Micro 2020 Annual Cybersecurity Report,” February 23, 2021 at: here.

Tyson, R. “The Intergovernmental Cleanup at Love Canal: A First Crack at "The Sleeping Giant of the Decade,” *Publius*, Winter 1980.

United Nations Scientific Committee on the Effects of Radiation (UNSCEAR), “Sources and Effects of Ionizing Radiation,” UNSCEAR 2008 Report to the General Assembly.

United States Aviex Co. v. Travelers Ins. Co., 125 Mich. App. 579, 336 N.W.2d 838 (1983).

United States v. Alaska Southern Packing Co. 1936, 84 F. 2nd 444, 445-446 (C.A. 9, 1936).

United States v. Hooker Chemical and Plastics Corp., et al., a civil suit filed by the U.S. Justice Department in U.S. District Court, Buffalo, NY (December 1979).

United States v. Hooker Chemicals Plastics Corporation. “Testimony of Frank Rovers of Conestoga-Rovers Associates of Waterloo, Canada, hired by the City of Niagara Falls in 1979 to evaluate the Love Canal dumpsite,” 680 F. Supp. 546 (W.D.N.Y. 1988).

United States v. Standard Oil Company, 384 U.S. 224 (1966).

University of Buffalo, Niagara Gazette Love Canal Chronology, 1894 - May 1980 at: here.

Urban et al. v. Occidental Chemical Corporation et al., December 20, 1983.

U.S. Atomic Energy Commission (USAEC), “Reports to the U. S. Atomic Energy Commission on nuclear power reactor technology,” Washington: US Government Printing Office, 1953.

U.S. Atomic Energy Commission (USAEC), “Preliminary Report of the Insurance Study Group to the Atomic Energy Commission, AEC Release No. 662, July 1955.

U.S. Atomic Energy Commission (USAEC), “Final Report of the Insurance Study Group to the Atomic Energy Commission, AEC Release No. 794, March 19, 1956.

U.S. Atomic Energy Commission (USAEC), “Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants,” WASH-740, 1957.

U.S. Atomic Energy Commission (USAEC), “Amendments to Regulations Governing Financial Protection Requirements and Indemnity Agreements,” AEC-R 29/9, March 19, 1960

U.S. Atomic Energy Commission (USAEC), "AEC Staff Study of the Price-Anderson Act, Chapter 4 Legislative Resolution: Fundamental Policy Issues and Criteria," January 1974.

U.S. Census Bureau (Census.gov), "All Sectors: Summary Statistics for the U.S., States, and Selected Geographies: 2017.

U.S. Census Bureau (Census.gov), "2018 SUSB Annual Data Tables by Establishment Industry" 2018 at: here .

U.S. Code of Federal Regulation, NRC: 10 CFR 50.54(w) Conditions of Licenses – Requirements for Onsite Property Damage Insurance.

U.S. Code of Federal Regulation (40 CFR § 312.20), "All Appropriate Inquiries," July 1, 2011 at: here.

U.S. Congress, "The Water Quality Act of 1965." 79 Stat. 903, 70 Stat. 498. Washington, D.C.: October 2, 1965.

U.S. Cybersecurity Emergency Response Team (US-CERT), "National Initiative for Cybersecurity Careers and Studies, "Explore Terms: A Glossary of Common Cybersecurity Terminology," accessed October 7, 2015 at: here.

U.S. Department of Commerce Internet Policy Task Force, "Cybersecurity Innovation and the Internet Economy," Washington DC, June 2011..

U.S. Department of Health & Human Services, "DHHS Evaluation of Results of Environmental Chemical Testing By EPA in the Vicinity of Love Canal-Implications for Human Health-Further Considerations Concerning Habitability," Washington, DC, July 13, 1982

U.S. Department of Energy (USDOE), Energy Research Advisory Board, "Review of the Proposed Strategic National Plan, Volume 1," October 1986, pp. D4-5.

U.S. Department of Health and Human Services (DHHS), "Business Associates," 2003 at: here.

U.S. Department of Health and Human Services (DHHS), "HHS Delegates Authority for the HIPAA Security Rule to Office for Civil Rights," August 3, 2009 at here

U.S. Department of Health and Human Services (DHHS), "HIPAA Administrative Simplification Enforcement," 2009 at: here.

U.S. Department of Health and Human Services (DHHS), "Summary of the HIPAA Privacy Rule," at: here.

U.S. Department of Health and Human Services (DHHS), "Breach Notification Rule," 2013 at: here.

U.S. Department of Health and Human Services (DHHS), "HIPAA Privacy, Security, and Breach Notification Audit Program," December 17, 2020 at: here.

U.S. Department of Health and Human Services (DHHS), "Putting America's Health First FY 2021 President's Budget for HHS," 2021 at: here.

U.S. Department of Health and Human Services Office for Civil Rights (OCR) "Annual Report to Congress on HIPAA Compliance For Calendar Years 2011 and 2012" 2013 at: here.

U.S. Department of Health and Human Services Office for Civil Rights (OCR) "HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework" 2016 at: here.

U.S. Department of Health and Human Services Office for Civil Rights (OCR) "Report to Congress on HIPAA Compliance For Calendar Years 2015, 2016, and 2017," 2018 at: here..

U.S. Department of Health and Human Services Office for Civil Rights (OCR) "2016-2017 HIPAA Audits Industry Report" December 2020 at: here.

U.S. Department of Health and Human Services Office for Civil Rights (OCR) Breach Portal accessed August 20, 2021 at: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

U.S. Department of the Interior (USDOI), National Park Service, "Historic American Engineering Record: Shippingport Atomic Power Station," 1983, pp. 3-4

U.S. Department of Justice (USDOJ), "Occidental to pay $129 Million in Love Canal Settlement," News Release, December 21, 1995, at: here.

U.S. Department of Justice (DOJ), "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals Causing Over $30 Million in Losses," November 28, 2018 at: here.

U.S. Food & Drug Administration (FDA), "Cybersecurity," 2021 at: here.

U.S. Government Accountability Office (GAO), "Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market," GAO-21-477, May 2021 at: here

U.S. House Subcommittee on Government Operations, "Hearings on H.R. 11510," 93rd Congress, 1st Session, Washington DC, November 1973.

US House of Representatives, Hazardous waste disposal report together with additional and separate views by the Subcommittee on Oversight and Investigations of the Committee on Interstate and Foreign Commerce, 97th Congress, first session. Washington, DC 1979.

U.S. House of Representatives "Love Canal study and habitability statement: hearing before the Subcommittee on Commerce, Transportation, and Tourism of the Committee on Energy and Commerce, Ninety-seventh Congress, second session, August 9, 1982.

U.S. House of Representatives, "Liability insurance availability: hearings before the Subcommittee on Commerce Transportation, and Tourism of the Committee on Energy and Commerce," 99th Congress, Washington DC, 1985-1986.

U.S. Senate, "Hearings Before the Subcommittee on Reorganization and International Organizations of the Committee on Government Operations: Coordination of Activities Relating to the Use of Pesticides," 88th Congress, 1st Session, May-June. 1963.

U.S. Senate Subcommittee on Energy Research and Development, "Hearings on S.1225, Price-Anderson Act Amendments Act of 1985," 99th Congress, 1st session, June 25, 1985.

U.S. Senate Subcommittee on Transportation, Infrastructure, and Nuclear Safety, "Hearings on Price-Anderson Act reauthorization," 107th Congress, 2nd Session, January 23, 2002.

U.S Senate Committee on Energy and Natural Resources, "Hearings on Nuclear Power," 108th Congress, 2nd session, 2004.

U.S. Nuclear Regulatory Commission, "Reactor Safety Study: An Assessment of Accident Risk in U.S. Commercial Nuclear Power Plants," WASH-1400, Washington, DC, October 1975.

U.S. Nuclear Regulatory Commission, "Safety Evaluation Report: related to operation of the Browns Ferry, Units 1 & 2, following the March 22, 1975 Fire," NUREG-0061, June 1976.

U.S. Nuclear Regulatory Commission, Lessons Learned Task Force, "Final Report," NUREG-0585, October 1979.

U.S. Nuclear Regulatory Commission, "Plan for Developing a Safety Goal" NUREG-0735, October 1980.

U.S. Nuclear Regulatory Commission, "An Approach to Quantitative Safety Goals for Nuclear Power Plants," NUREG-0739, October 1980.

U.S. Nuclear Regulatory Commission, "Nuclear Regulatory Commission Issuances: Opinions and Decisions," July 1, 1980 to December 31, 1980, Volume 12, 1981.

U.S. Nuclear Regulatory Commission (USNRC),"Use of INPO SEE-IN Program (Generic Letter No. 82-04)," March 1982.

U.S. Nuclear Regulatory Commission, Office of Policy Evaluation, "Safety Goals for Nuclear Power Plant Operation," NUREG-0880, May 1983.

U.S. Nuclear Regulatory Commission, "The Price-Anderson Act--The Third Decade Report To Congress," NUREG-0957, October 1983.

U.S. Nuclear Regulatory Commission, "Probabilistic Risk Assessment Reference Document," NUREG 1050. September 1984.

U.S. Nuclear Regulatory Commission, “Policy Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants,”1985.

U.S. Nuclear Regulatory Commission, “Individual Plant Examination for Severe Accident Vulnerabilities,” Generic Letter No. 88-20, November 22, 1988.

U.S. Nuclear Regulatory Commission, “Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Final Policy Statement,” Federal Register, 60:158, August 16, 1995, pp. 42622-42629.

U.S. Nuclear Regulatory Commission, “INES Rating of Davis-Besse Reactor Head Degradation Event,” March 21, 2002 at: here.

U.S. Nuclear Regulatory Commission, "Use of Probabilistic Risk Assessment in Plant-Specific, Risk-Informed Decision-making: General Guidance," NUREG-0800, June 2002.

U.S. Nuclear Regulatory Commission Office of Nuclear Regulatory Research (USNRC ONRR), “Three Mile Island Accident of 1979 Knowledge Management Digest Overview,” NUREG/KM-0001, Revision 1, June 2016.

U.S. Nuclear Regulatory Commission, “The Reactor Safety Study: The Introduction of Risk Assessment to the Regulation of Nuclear Reactors,” WASH-1400, August 2016.

U.S. Nuclear Regulatory Commission, “Backgrounder on the Three Mile Island Accident,” here

U.S. Senate, “Cyber Incident Notification Act of 2021,” 117th Congress, First Session, July 21, 2021 at: here.

USI (2018), “Growing Trend of Costly Environmental Claims Expected to Continue in 2018,” at: here.

VanderLaan, K. “Legal Practice in a HITECH Environment: An Overview of the HITECH Act and its Effect on Lawyers as Business Associates,” accessed August 25, 2021 here.

Verizon, “2018 Data Breach Investigations Report 11th edition,” 2018.

Voreacos, D, Chinlisky, K. and Griffen, R. “Merck Cyberattack’s $1.3 Billion Question: Was It an Act of War?” Bloomberg, December 3, 2019 at: here.

Vuono, M. and Hobbs, R.” Environmental Insurance vs the Pollution Coverage of a Standard GL Policy,” 10 *Environmental Claims Journal*, 83, 1997.

Waste Management v. Peerless Insurance Company, 316 N.C. 386, 346 S.E.2d 134 (1986).

Wald, M., “Out-of-Court Settlement Reached Over Love Canal,” New York Times, June 22, 1994.

Weiss, P. & Burger, L. “Bayer contains cyber-attack it says bore Chinese hallmarks,” Reuters, April 4, 2019 at: here.

Werner et. al., “Basic Ratemaking: Fifth Edition, 2016.

Wendland, W. Letter to Gary Little (Progress Energy), “ANI Nuclear Liability Insurance Inspection Brunswick Steam Electric Plant,” November 4-6, 2008.

White, W., “Certificate of Shop Inspection – May 8, 1957,” in Heffner, R.E. SPERT III Pressurizer Vessel Failure (1962).

White House, “Memorandum regarding "Operation Candor," NSC Papers, July 22, 1953.

White House, "Atoms for Peace" Speech, Press Release, December 8, 1953.

White House, “Use of Pesticides: A Report of the President’s Science Advisory Committee,” Washington DC, May 15, 1963.

White House, “Reorganization Plan No. 3 of 1970: Special Message from the President to the Congress About Reorganization Plans to Establish the Environmental Protection Agency and the National Oceanic and Atmospheric Administration,” July 9, 1970 at: here

Willis Tower, “Insurance Marketplace Realities 2021 – Cyber risk,” Nov. 18, 2020 here.

Wilson, S. “SolarWinds recap: All of the federal agencies caught up in the Orion breach,” FedScopp, December 22, 2020 at: here.

Winder, D. “This 20-Year-Old Virus Infected 50 Million Windows Computers In 10 Days: Why The ILOVEYOU Pandemic Matters In 2020,” Forbes, May 4, 2020, at here.

World Nuclear Association, “Chernobyl Accident,” 2020, at: here.

World Nuclear Association, “Fukushima Daiichi Accident,” 2019 at: here.

World Nuclear Association, “Nuclear Power Reactors,” 2020 at: here.

Worthley, J. and Torkelson, R. “Lessons from the Love Canal,” *Administration and Society*,”13:2, August 1981, pp. 145-160.

Yin, R. *Case Study Research Design and Methods (4th Edition),* SAGE Publications, Inc., Thousand Oaks, CA, 2009.

Young, D., Lopez, J., Rice, M., Ramsey, B., & McTasney, R. “A framework for incorporating insurance in critical infrastructure cyber risk strategies,” *International Journal of Critical Infrastructure Protection* (April 2016).

Zhao, X., Xue, L. and Whinston, A. “Managing Interdependent Information Security Risks: A Study of Cyberinsurance, Managed Security Service and Risk Pooling,” Thirtieth International Conference on Information Systems, Phoenix, Arizona 2009.

Zuesse, E. “Love Canal: The truth seeps out,” *Reason*, February 1981, at: here.

Biography

John Gudgel graduated from the Colorado School of Mines in 1980 with a degree in Geological Engineering. He went on to get a Master of Science degree in Telecommunications from the University of Colorado, Boulder in 1985. He then worked for 25 years for telecommunications and media companies, and received his second Master of Science degree in eCommerce from George Mason University in 2009. He and his wife, Dorothy, currently live in Herndon VA, and are the proud parents of Jackie, and four Border collies: Max, Mollie, Woody, and Winston.

.

.

.