Nebraska Law Review

Volume 97 | Issue 2 Article 7

2018

The Case for a Federal Cyber Insurance Program

David L. Vicevich
University of Nebraska College of Law

Comment*

The Case for a Federal Cyber Insurance Program

TABLE OF CONTENTS

I. Introduction 556
II. Cyber Risk Is Best Addressed by Insurance 558
A. U.S. Policy Contributes to Cyber Insecurity 558
1. The United States Leads in Cyber Offense 558
2. U.S. Domestic Policy Fosters Cyber Insecurity .. 560
B. An Escalating, Dynamic, and Unique Risk 562
C. State and Multinational Actors Increasingly Involved 565
D. Unique Cybersecurity Issues Frustrate Policy 566
III. Responses to Cyber Risk Beyond Insurance Are Failing 571
A. The Public Law Response Is Inadequate 571
B. Private Law Is Ineffective at Addressing Cyber Losses 575
C. Public and Private Law Contradict Limiting Remedies 576
IV. The Private Insurance Market Is Unable to Manage Cyber Risk 576
A. The Market Is Undercapitalized 576
1. Current Market Capitalization 576
2. Losses Outstrip the Market 578
B. Cyber Risk Management Is Uniquely Difficult 579

* David Vicevich, LL.M 2018, University of Nebraska Lincoln College of Law; J.D. 1999, Washington University in St. Louis School of Law; B.A. 1996, Gonzaga University. The author is an attorney in private practice and owns a boutique litigation firm in Butte, Montana.

A prior version of this paper was submitted as a thesis requirement for the Space, Cyber, and Telecommunications LL.M program at UNL. The author wishes to thank Professor Justin (Gus) Hurwitz for his guidance and assistance and for fostering and challenging the concepts related to this paper. Further thanks to the editorial staff at the NEBRASKA LAW REVIEW for their work and patience and to Amara and Gillian Vicevich for their unending support. Any errors that remain are the author's and the author's alone.

1. From the Consumer and Business Perspective .. 579
2. From the Insurance Perspective 580
C. Current Cyber Coverage Is Inadequate 582
1. Coverage Not Widespread 583
2. Coverage Mirrors Regulation Instead of Risk ... 584
3. Coverage Is Difficult to Obtain 585
4. Coverage Is Expensive 587
5. Obtained Coverage Is Illusory 588
6. Adequate Coverage from the Private Market Is Unsustainable 591
V. Cyber Insurance Is Vital for Cyber Risk Management .. 592
VI. Federal Cyber Insurance: A Solution to Cyber Risk Management 593
A. Public/Private Collaboration Is Required 593
B. Defining the Threat Matrix 595
C. Federal Insurance Models 596
1. Federal Backstop Insurance (TRIP and Commercial Space Law) 597
2. FDIC 599
3. NFIP 601
D. General Benefits of National Cyber Insurance 602
E. Counterpoint: Possible Negative Results of National Cyber Insurance 603
VII. Conclusion 604

"Take back your insurance
Baby nothing's guaranteed"

—Tom Petty, Bob Dylan, Mike Campbell, "Jammin' Me" (1987)

I. INTRODUCTION

Perhaps the greatest threat to U.S. national security is the cyber threat. Vast amounts of wealth are lost annually to this threat—a wealth transfer historically akin to the conquest of the New World by Spain. The lack of security in the cyber ecosystem stems from a devil's brew of foreign policy, domestic policy, and a substantial, dynamic threat. In foreign policy, the United States uses cyberattacks to great effect and leads the world as a source of cybercrime.[1] Domestic policy supports deregulated utilities and encourages private development of Internet and telecommunications infrastructure for convenience,

1. James Cook, *The World's 10 Biggest Cybercrime Hotspots in 2016, Ranked*, BUS. INSIDER (May 14, 2017), http://www.businessinsider.com/worlds-10-cybercrime-hotspots-in-2016-ranked-symantec-2017-5 [https://perma.unl.edu/6UJ8-55XS] (describing threat numbers including malware, phishing, and spam, which are sourced from Symantec's Internet security threat report of April 2017).

speed, and utility, but not security. The U.S. economy and the breadth of its industry rely on the Internet and telecommunications infrastructure. As a market economy, most U.S. critical infrastructure is also private.[2] The United States, therefore, is an attractive target unable to respond adequately through its national security institutions because of its own offensive cyber operations.

Domestic cybersecurity measures have failed as well. Public law responses are fragmented and ineffective.[3] The Federal Trade Commission (FTC) has stepped into the void, perhaps beyond its authority, but it simply cannot address the breadth of security problems that continue to scale. Private law also fails in the cyber ecosystem, leaving individuals little recourse when personal information is lost, and businesses and government little recourse for insecure technology. The disjointed approach confuses actors and creates inconsistent incentives and uncomfortable decision-making. Basic security measures increase the possibility of government intrusion, and deterrent measures and research—like bug bounties and friendly hacking—are criminalized.[4]

Cyber insurance serves as an adept regulator in this policy vacuum, but it faces severe challenges that render it ineffective. The private insurance market is undercapitalized compared to large losses. Cyber risk possesses unique qualities, including interdependent security and correlated failure. Thus, cyber risk management is difficult, and the insurance industry is unable to pool risk. Because of these factors, cyber insurance is not widespread. The insurance is reactive to regulation and purchased after breaches as an alternative to security. It is hard to obtain, expensive, and limited by rigid exclusions. Coverage that is purchased will not cover many common cyberattacks. The private market for insurance may be unsustainable.

---

2. James Eastman, *Avoiding Cyber-Pearl Harbor: Evaluating Government Efforts to Encourage Private Sector Critical Infrastructure Cybersecurity Improvements*, 18 COLUM. SCI. & TECH. L. REV. 515, 520, 528–31 (2017). For consideration of "critical infrastructure," see *Critical Infrastructure Sectors*, DEP'T HOMELAND SEC. (July 11, 2017), https://www.dhs.gov/critical-infrastructure-sectors [https://perma.unl.edu/3PL6-DVE4] (listing 16 sectors of critical infrastructure: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear, transportation, and water and wastewater).

3. Elizabeth A. Rowe, *RATs, TRAPs, and Trade Secrets*, 57 B.C. L. REV. 381, 407–08 (2016) (discussing, e.g., how the last federal criminal law effort addressing hacking, the 1986 Computer Fraud and Abuse Act (18 U.S.C. § 1030), criminalizes legitimate security research such as friendly hacking by security firms and academics and the employment of bug bounties by companies offering rewards for hackers identifying vulnerabilities).

4. *Id.*

After considering U.S. policy, the nature of the threat, the failed public and private law responses, and the limitations of the private cyber insurance market, the discussion herein moves to consider a national cyber insurance program. It considers the need for public and private collaboration and examines three existing federal insurance programs. It considers federal backstop insurance, like the Terrorism Risk Insurance Program (TRIP), as a model to expand the risk pool for private insurers; the Federal Deposit Insurance Corporation (FDIC) as a model to restore faith in shaken institutions; and the National Flood Insurance Program (NFIP) as a model to address correlated failure and provide security in future development. Finally, this Comment briefly considers the possible benefits and detriments of a national cyber insurance program generally.

II. CYBER RISK IS BEST ADDRESSED BY INSURANCE

A. U.S. Policy Contributes to Cyber Insecurity

1. The United States Leads in Cyber Offense

In 1970, the Soviet Union established a new section, Directorate T within the KGB, tasked with obtaining badly needed technology from Western research and development.[5] Its operating arm known as "Line X" engaged in cloak and dagger techniques during trips by Soviet delegations, like applying glue to shoes during a Boeing tour to obtain metal samples.[6] French President Francois Mitterrand informed Ronald Reagan in 1981 that the French had employed the services of an engineer working for Directorate T, who supplied thousands of documents on the Soviet program that included the identity of hundreds of Line X officers.[7] The documents revealed the success of Directorate T and that stolen technology was supporting Soviet defense.[8] The trove also included a Soviet technology wish list containing gas pipeline pump, turbine, and valve control software.[9]

The U.S.S.R's gas supply was critical to its internal economy and to its hard currency earnings from the West.[10] Accordingly, the United States engaged in efforts to block Soviet gas sales to Western Europe.[11] The CIA and American industry cooperated in preparing

5. David E. Hoffman, *Reagan Approved Plan to Sabotage Soviets*, WASH. POST (Feb. 27, 2004), https://www.washingtonpost.com/archive/politics/2004/02/27/reagan-approved-plan-to-sabotage-soviets/a9184eff-47fd-402e-beb2-63970851e130 [https://perma.unl.edu/8N4D-4WE3].
6. *Id.*
7. *Id.*
8. *Id.*
9. *Id.*
10. *Id.*
11. *Id.*

flawed software and in publishing the technology to Line X.[12] The software was designed to operate properly for a time before resetting pump speed and valve settings to overstress pipeline joints and welds.[13] The software triggered a huge explosion on a Soviet gas pipeline in Siberia in the summer of 1982.[14] The explosion was the largest non-nuclear explosion and fire ever observed from space.[15] The Soviet trust placed in stolen technology was shaken forever, and internal economic decline ultimately contributed to the Soviet collapse a few years later.[16] Russia, to this day, maintains that it is entitled to respond to a cyberattack with nuclear retaliation.[17]

Similarly, malware targeting industrial control systems caused the failure of thousands of centrifuges at uranium enrichment plants in Natanz, Iran in 2010.[18] Called "Stuxnet," the code targeted logic controllers that ran automated processes in the plant and damaged the operation severely enough to set the plant's capabilities back two years.[19] Atypical of malware and contrary to common motivations behind malware, Stuxnet targeted a specific, limited set of computers.[20] The use of four zero-day hacks in the malware suggests that the target was of great value to the attacker.[21] It was not the work of hackers, but months of work by organized programmers with significant resources.[22] The malware was highly specialized, and its utility intended specifically for the destruction of nuclear centrifuges.[23] These factors and the United States' refusal to deny responsibility strongly evidence the involvement of the United States and Israel in the development and deployment of Stuxnet.[24] It has been suggested that Stuxnet was designed and used intentionally for compliance with the Law of Armed Conflict (LOAC).[25] Beyond physically damaging the centrifuges and requiring the replacement of computer systems, Stuxnet likely inflicted psychological damage similar to that inflicted on the Soviet Union's trust of stolen technology.[26]

12. *Id.*
13. *Id.*
14. *Id.*
15. *Id.*
16. *Id.*
17. Jeremy Richmond, *Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?*, 35 FORDHAM INT'L L.J. 842, 846 (2012).
18. Eastman, *supra* note 2, at 526.
19. *Id.* at 526–27.
20. Richmond, *supra* note 17, at 853.
21. *Id.* at 853–54 (noting the high value of Windows zero-days and that programmers almost never use more than one in a single piece of malware).
22. *Id.* at 854–55.
23. *Id.* at 855.
24. *Id.* at 845, 853–56.
25. *Id.* at 894.
26. *Id.* at 859.

Stuxnet code spread around the world and now serves as a model for attacking industrial facilities.[27] For example, the Duqu virus, which appears to collect information from host computers for future attacks, uses sections of Stuxnet code.[28] Other U.S. code developed for use by the intelligence apparatus have later been used malevolently. For example, the WannaCry ransomware attack that caused $4 billion in losses used EternalBlue technology developed by the National Security Agency (NSA) to exploit vulnerabilities in a Windows platform.[29] In addition to the United States' successful use of cyberattacks against other countries' strategic assets and the resulting proliferation of technology, the United States continues as a world leader in the source of cybercrime with nearly one-quarter of detected global threats originating in the United States in 2016.[30] This figure, up from previous years, exceeds the detected threats from China by more than two-and-one-half times and threats from Russia more than sevenfold.[31]

2. U.S. Domestic Policy Fosters Cyber Insecurity

The Telecommunications Act of 1996 set U.S. policy towards the commercial development of the Internet as one of free market competition and private development with light touch regulation.[32] As a result, the Internet was not designed for security, but the private sector contributed $1.5 trillion to build out fixed and mobile networks in the United States.[33]

> Here is the inconvenient truth about our connected world: the Internet was designed for accessibility and speed—never for security and protection. While it has delivered on its promise of social and economic progress, it has also delivered unparalleled opportunities to those seeking to scale global conflict, terrorism, criminal activity, state and industrial espionage, and vandalism.[34]

The same positive quality of interconnection that the Internet provides also provides ease and the framework for systemic infection, damaging businesses and economies.[35]

U.S. policy provides disincentives to security and incentivizes the use of digital data. For example, the use of Virtual Private Networks

27. *Id.* at 860–61.
28. *Id.* at 861–62.
29. Jonathan Berr, *"WannaCry" Ransomware Attack Losses Could Reach $4 Billion*, MONEYWATCH (May 16, 2017), https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/ [https://perma.unl.edu/TA7A-QSZW].
30. Cook, *supra* note 1.
31. *Id.*
32. In the Matter of Restoring Internet Freedom, 33 FCC Rcd. 311, 317 (2018).
33. Statement of Chairman Ajit Pai at 132, In the Matter of Restoring Internet Freedom, 33 FCC Rcd. 311 (2018) (No. 17-108).
34. David N. Lawrence et al., *It's the Cyber Crime and Its Sponsors (Not My Cyber-Security), Stupid*, 5 J.L. & CYBER WARFARE 1, 24 (2017).
35. Rowe, *supra* note 3, at 399–400.

(VPNs) as a basic security measure to encrypt data and conceal its location is discouraged by measures such as Rule 41 of the *Federal Rules of Criminal Procedure*.[36] Rule 41(b)(6)(a) extends venue for warrants seeking stored electronic media to any district outside the district where activities related to a crime may have occurred, if the location of the information has been concealed through electronic means.[37] It is worth noting, however, that extension of venue applies to warrants seeking evidence of a crime and property used in a crime. A warrant, therefore, could seek to search a criminal victim's computer or an innocent's computer that is hacked and used for illegal purposes.[38] Once an innocent's computer is hacked, Rule 41 allows the issuance of warrant in any federal district to search that computer if a VPN was used as a basic security measure. If a hacker gets in, so can the government from a venue far, far way.

U.S. cybersecurity law is inconsistent. U.S. policy encourages and resulting law requires the transition of information having the highest privacy interest, such as medical records, to electronic form.[39] As a result, policy demands protection and security of this data.[40] The security stakes of health records becoming inaccessible are the highest because loss of use could result in patients' deaths.[41] Strict privacy, security, and breach notification rules, therefore, apply to health records.[42] All states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands now impose data breach notification laws enforcing a duty to protect personal information.[43] The federal government's willingness, however, to respond to security issues has diminished. Shortly after the adoption of the Telecommunications Act of 1996, President Clinton recognized the threat to cybersecurity and telecommunications stating,

> No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from today [May 22, 2003] the United States shall have achieved and shall maintain the ability to protect the nation's critical infrastructures from intentional acts that would signifi-

36. *See* STEVEN M. BELLOVIN, THINKING SECURITY: STOPPING NEXT YEAR'S HACKERS 92–97 (2016) (providing a discussion of use of VPNs for security purposes).
37. FED. R. CRIM. P. 41(b)(6)(a).
38. FED. R. CRIM. P. 41(c)(1)–(4).
39. *See, e.g.*, American Recovery and Reinvestment Act of 2009, 42 U.S.C. § 300jj–11(b) (2012).
40. *See*, *e.g.*, *id.* § 300jj-11(b)(1).
41. MARTIN ELING & WERNER SCHNELL, GENEVA ASS'N, TEN KEY QUESTIONS ON CYBER RISK AND CYBER RISK INSURANCE 24 (Fabian Sommerrock ed., 2016).
42. Paul R. DeMuro, *Keeping Internet Pirates at Bay: Ransomware Negotiation in the Healthcare Industry*, 41 NOVA L. REV. 349, 375–82 (2017) (discussing the HIPAA privacy, security, and breach notice rules).
43. *Security Breach Notification Laws*, NAT'L CONF. OF ST. LEGISLATURES (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.unl.edu/K6TK-DWRU].

> cantly diminish the abilities of: . . . the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.[44]

By 2015, the optimism waned. President Obama stated, "Government has many capabilities, but it's not appropriate or even possible for government to secure the computer networks of private businesses."[45]

Cybersecurity is national security.[46] Private sector vulnerability is a national security issue because 85% of U.S. critical infrastructure is private.[47] Even a threat just to the payment processing industry is recognized as a national security issue.[48] It is on the forefront for companies, financial institutions, law enforcement, and regulators.[49] The insurance industry recognizes cybersecurity as an issue at the national and international level.[50] Despite this, the policy allocating the losses sustained due to the lack of cybersecurity remains undecided.[51] Recognizing the scope of the security problem, the policy of the U.S. government changed course from addressing the security problem to stating that it cannot and should not be responsible to secure private networks. The U.S. government's national security infrastructure, unfortunately, is the only national institution with the experience and resources to address the problem.[52]

B. An Escalating, Dynamic, and Unique Risk

Since 2000, six times more people use the Internet, and they now number more than three billion.[53] Four computer viruses were known in 1990 and more than 5,000 by 2012, with over 100 new viruses appearing each month since.[54] Between 2009 and 2011 alone, attacks on

44. *Public Safety Tech Topic #20 – Cyber Security and Communications*, FED. COMM. COMMISSION, https://www.fcc.gov/help/public-safety-tech-topic-20-cyber-security-and-communications [https://perma.unl.edu/22KV-DZCV] [hereinafter *Public Safety Tech Topic #20*] (quoting Presidential Decision Directive 63 (PDD-63)).
45. Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, 2015 U. ILL. J.L. TECH. & POL'Y 341, 369 (quoting Obama at the Cybersecurity and Consumer Protection Summit held on February 13, 2015 at Stanford University during which he promoted, principally, government and private sector cooperation to address cybersecurity concerns).
46. *See* Lawrence et al., *supra* note 34, at 2, 23–30.
47. Eastman, *supra* note 2, at 520, 528–31; *see also Critical Infrastructure Sectors*, *supra* note 2 (listing examples of critical infrastructure identified by the U.S. Department of Homeland Security).
48. Trautman, *supra* note 45, at 356.
49. *Id.*
50. ELING & SCHNELL, *supra* note 41, at 35.
51. *See* Lawrence et al., *supra* note 34, at 43.
52. Trautman, *supra* note 45, at 358.
53. Jason F. Keen, *Conventional Military Force as a Response to Cyber Capabilities: On Sending Packets and Receiving Missiles*, 73 A.F. L. REV. 111, 112 (2015).
54. *Id.*

key infrastructure increased seventeenfold.[55] Data breaches increased by 40% between 2014 and 2015.[56] Cyberattacks are becoming more frequent, and prevention is difficult.[57] The risk is always changing with the advent of custom malware tailored towards particular targets, and security countermeasures require continuous updating and monitoring.[58] Cyber risk is a unique risk because of the speed with which it changes, and improvements in security can be probed and adapted too easily.[59] The atmosphere has scaled from criminals seeking small gains to sophisticated and organized groups characterized by continuous innovation.[60] While bank customers were targeted in the past, the banks are now the targets.[61]

The nature of the risk is uniquely broad and can be caused not only by crime but also by natural disasters, human failure, war, or terrorism.[62] The risk is characterized by interdependencies.[63] The vulnerability of a network depends not only on its own security, but on the security of other networks connected to it.[64] The risk can also be characterized as systemic, involving correlated failure through which multiple networks fail due to one event, such as when one vulnerability is exploited on a number of networks.[65] Effective computer security is very difficult and expensive to do correctly.[66] It is more complex than security in the physical world and is reliant on code.[67] No system is ever completely secure, and cybersecurity also depends on how victims respond to breaches.[68]

---

55. *Id.* at 112–13.
56. Nelly Rosenberg, *An Uphill Battle: FTC Regulation of Unreasonable Data Security as an Unfair Practice*, 66 DEPAUL L. REV. 1163, 1170 (2016).
57. Minhquang N. Trang, *Compulsory Corporate Cyber-Liability Insurance: Outsourcing Data Privacy Regulation to Prevent and Mitigate Data Breaches*, 18 MINN. J.L. SCI. & TECH. 389, 389 (2017).
58. *See* Ariana L. Johnson, *Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation*, 20 N.C. BANKING INST. 277, 277–78, 309 (2016).
59. Trang, *supra* note 57, at 392–93.
60. Jennifer Gordon, *Like a Bad Neighbor, Hackers Are There: The Need for Data Security Legislation and Cyber Insurance in Light of Increasing FTC Enforcement Actions*, 11 BROOK. J. CORP. FIN. & COM. L. 183, 186 (2016).
61. Johnson, *supra* note 58, at 277–78.
62. ELING & SCHNELL, *supra* note 41, at 12.
63. *Id.*
64. Sasha Romanosky et al., *Content Analysis of Cyber Insurance Policies: How Do Carriers Write Policies and Price Cyber Risk?* 6 (Workshop on the Econ. of Info. Sec., Working Paper No. 28, 2017), http://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/06/WEIS_2017_paper_28.pdf [https://perma.unl.edu/5RAQ-56AQ].
65. *Id.*
66. Justin (Gus) Hurwitz, *Cyberensuring Security*, 49 CONN. L. REV. 1495, 1501–02, 1504 (2017).
67. *Id.* at 1502–03.
68. *Id.* at 1504.

Hacked government entities include the Israeli Defense Force, India's Eastern Naval Command, Royal Bank of Scotland, Defense Research and Development Canada, University of California-Berkeley, the Federal Bureau of Investigation, the U.S. Senate, the Internal Revenue Service, the Office of Policy and Management, and the Central Intelligence Agency.[69] The 2008 financial crisis forced U.S. state governments to decrease their security budgets.[70] They remain vulnerable and have valuable personal information, such as tax, driving, professional, educational, health, and criminal records, at risk.[71]

"FBI Director James Comey stated that 'there are two kinds of big companies in the United States . . . those who've been hacked . . . and those who don't know they've been hacked.'"[72] Hacked companies include JPMorgan Chase, Amazon, Yahoo, Safeway, Kohl's, Esurance, Wendy's, Aon Hewitt, Comcast, Home Depot, Target, Neiman Marcus, T-Mobile, Sony, Hilton, Uber, Trump Hotels, Costco, State Farm, American Airlines, United Airlines, U.S. Steel, and Alcoa.[73] At least 97% of Fortune 500 companies have been hacked.[74] Any corporation in the United States can be penetrated, and self-protection through investment in security can be ineffective.[75] For example, JPMorgan was breached, thus losing account information from 83 million individuals and businesses, despite a $250 million expenditure to improve cybersecurity.[76] Eighty-seven percent of companies consider cyber liability as a top ten business risk and consider the risk to information assets higher than the risk to property, plant, and equipment (PP&E).[77] Seventy-two percent of security experts believe that their organizations will suffer major breaches within a year, 74% are too understaffed to address threats, and 67% are undertrained.[78] Detection times are too slow, taking over 150 days on average to detect breaches and up to another 100 days to mitigate, leaving intruders eight months to search and sort.[79] In excess of 60% of attacks are now on small businesses, and this trend is increasing.[80]

69. *Id.* at 1497; Keen, *supra* note 53, at 113–14; Trautman, *supra* note 45, at 359.
70. Trautman, *supra* note 45, at 359.
71. *Id.*
72. Trang, *supra* note 57, at 389.
73. Rosenberg, *supra* note 56, at 1164, 1170; Rowe, *supra* note 3, at 403.
74. Gordon, *supra* note 60, at 186.
75. ELING & SCHNELL, *supra* note 41, at 31; Trautman, *supra* note 45, at 346.
76. Eastman, *supra* note 2, at 518.
77. PONEMON INST., 2017 GLOBAL CYBER RISK TRANSFER COMPARISON REPORT 4, 6 (2017).
78. Lawrence et al., *supra* note 34, at 27.
79. *Id.* at 43.
80. Lance Bonner, *Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches*, 40 WASH. U. J.L. & POL'Y 257, 274 (2012); Rowe, *supra* note 3, at 422–23.

Losses from security breaches are on the rise and not just in the United States, but worldwide.[81] The average annual cost for cybercrime exceeds $15 million *per U.S. company* and is increasing by 20% a year.[82] Damages from breaches to private entities come from diverse and numerous sources. A breached U.S. company can face damages from class action lawsuits, FTC actions, Securities and Exchange Commission (SEC) enforcement actions, and shareholder derivative lawsuits.[83] It may also suffer reputational damage, contractual damages, response costs, loss of intellectual property, and share value loss over 2% per breach.[84] Not only is network security interdependent, but so are the losses caused by breaches. Stock prices may even fall for Internet-based companies when another Internet-based company is breached.[85]

Managing cyber risk is the defining risk management challenge of this century.[86] The Internet generates $2–3 trillion a year and as much as one-fifth of it is lost to crime.[87] One trillion dollars of intellectual property is lost annually.[88] The losses represent the largest transfer of wealth in human history.[89]

C. State and Multinational Actors Increasingly Involved

The scaling of the attacks and the nature of the attacker are cause for concern. For example, the Carbanak attacks in 2013 consisted of a multinational organization of criminals targeting more than 100 banks with a series of sophisticated attacks.[90] Losses ranged from $2.5 million to $10 million per attack and totaled almost $1 billion.[91]

North Korea had ties to the Guardians of Peace that breached Sony in late 2014.[92] Media reports are rife with reports of attacks from Russia, China, and North Korea.[93] Critical infrastructure is constantly probed by Russian, Chinese, Iranian, and North Korean hackers, in-

81. Andrew Zachery Ryan Smith, *FTC Regulating Cybersecurity Post* Wyndham*: An International Common Law Comparison on the Impact of Regulation of Cybersecurity*, 45 GA. J. INT'L & COMP. L. 377, 378, 391 (2017).
82. *Id.* at 378.
83. Trang, *supra* note 57, at 398–405.
84. ELING & SCHNELL, *supra* note 41, at 16.
85. *Id.*
86. Gregory D. Podolak, *Insurance for Cyber Risks: A Comprehensive Analysis of the Evolving Exposure, Today's Litigation, and Tomorrow's Challenges*, 33 QUINNIPIAC L. REV. 369, 370 (2015).
87. Trautman, *supra* note 45, at 356.
88. Rowe, *supra* note 3, at 384.
89. Gordon, *supra* note 60, at 186.
90. Johnson, *supra* note 58, at 277.
91. *Id.*
92. Scott J. Shackelford, *The Law of Cyber Peace*, 18 CHI. J. INT'L L. 1, 3 (2017).
93. Kevin R. Doherty, *The Art of (Cyber) War*, 29 INTELL. PROP. & TECH. L.J. 16, 17 (2017).

cluding private sector industry, healthcare, transportation, communications, and utility infrastructure.[94] A variety of foreign attackers operate for different reasons.[95] China and Russia hack for commercial and political reasons.[96] Many actively attacking states do not separate military and business interests like the United States.[97] One Chinese espionage unit alone breached over 100 U.S. companies.[98] In addition to the usual suspects, France, Taiwan, Japan, India, and Israel have engaged in cyber espionage against U.S. business interests.[99] Iran and North Korea go further than commercial and political attacks by employing malware to deny service and to sabotage or destroy.[100] Eastern European sources tend to be criminal.[101] Other attacks are more contextual, such as attacks on Western news organizations originating in Syria during its civil war.[102]

Over 120 countries have active information operations.[103] In terms of U.S. national security, security experts rate cyber risk from foreign actors as second only to weapons of mass destruction.[104] While there appears to be consensus that the LOAC applies to cyberattacks, there is doubt that it can effectively regulate.[105] Because of the growing foreign risk, the U.S. Department of the Treasury required standalone cyber insurance policies to comply with the Terrorism Risk Insurance Act (TRIA) of 2002, effective April 2017.[106]

D. Unique Cybersecurity Issues Frustrate Policy

Consideration of the various concerned constituencies in cybersecurity issues demonstrates the complexity of policy. They are also valuable when analyzing policy questions and considering the benefit and detriment of possible measures. They are used throughout this Comment to evaluate the effect of shifting responsibilities. Consumers, investors, businesses (including subgroups within having distinct interests, such as the technology sector), law enforcement, government, and national security entities all share interest in cybersecurity

94. Lawrence et al., *supra* note 34, at 26–27.
95. Trautman, *supra* note 45, at 356–57.
96. *Id.* at 356.
97. *Id.* at 360 (e.g., North Korea, a totalitarian state, attacking Sony rather than a competing business).
98. Rowe, *supra* note 3, at 384.
99. *See id.* at 401.
100. Trautman, *supra* note 45, at 357.
101. *Id.*
102. *Id.*
103. *See* Richmond, *supra* note 17, at 846.
104. *Id.*
105. *Id.* at 847.
106. Virginia N. Roddy, *Expanding Risks, Growing Market: Cyber Insurance Today*, 59 FOR DEF. 80, 84 (2017).

and each face unique threats.[107] Tension arises between these groups as policy is formed.[108] Although this is common for policy considerations in the United States, a unique problem arises in cybersecurity policy development. "Because cybersecurity involves highly complex technological issues (and usually hidden costs), many constituencies will find it difficult to obtain or perceive accurately the information necessary to determine their own best interest."[109] The inability of constituencies to perceive their respective interests in cybersecurity policy is complicated by lack of trust in government and lack of interest by civil groups and academic institutions.[110]

The policy complexities that arise from the constituencies are numerous. A primary tension arises from businesses seeking liability protection to information share with respect to security breaches.[111] Consumer groups oppose this.[112] Government gets caught in the middle trying to balance these concerns. For example, the SEC requires disclosure of breaches and perceived cyber risks.[113] This government disclosure requirement, meant to protect investors and potentially consumers, frustrates law enforcement and national security constituencies' efforts to monitor and map sources and methods of cyberattack.[114] The business constituency opposes the regulation because breaches continue regardless, so the additional cost of regulation brings no perceived benefit.[115] An independent business constituency—the cybersecurity industry—benefits from breaches and sees stock values rise over 1%, or the equivalent of over $1 billion, after the announcement of another company's breach.[116]

Another conflict between constituencies previously discussed is the use of offensive cyberattack to affect what national security entities may view as higher priority security interests—such as limiting the proliferation of nuclear weapons—only to have the code later used against U.S. interests, such as with Stuxnet and EternalBlue. Rules that seek to regulate specific industries or protect consumers do little to address the general issues that make cybersecurity difficult, resulting in inefficiency.[117] A cohesive policy on cybersecurity would need to overcome fundamental geopolitical questions and contentious parti-

107. *See* Trautman, *supra* note 45, at 351.
108. *Id.*
109. *Id.*
110. *Id.*
111. Johnson, *supra* note 58, at 298.
112. *See id.* at 300.
113. Trautman, *supra* note 45, at 354.
114. *Id.* at 354–55.
115. *See id.* at 357.
116. ELING & SCHNELL, *supra* note 41, at 16 n.7.
117. Hurwitz, *supra* note 66, at 1517.

san differences; however, consistent terminology to even discuss these issues has yet to evolve.[118]

One primary barrier to policy and regulation is the attribution problem, the identity of the bad actor in cybersecurity is difficult to ascertain.[119] "Due to the technological nature of data breaches, it is difficult to ascertain the wrongdoer, the severity of damages, and even the fact that identity theft occurred."[120] Stolen information is intangible. When it is copied, the original may remain intact and in place, unlike tangible items.[121] This results in the lengthy delay in detection discussed above, which again reduces the likelihood of identifying the perpetrator.[122] The source of the attack that breached Target in 2013, causing losses into the hundreds of millions, has not been identified.[123] A Russian teen may have created the malware, but it was then placed on the Internet for anyone to use.[124] The same is true of the 2011 Sony PlayStation Network breach.[125] A breach may involve criminals in several countries, raising jurisdictional issues should a source be identified.[126] The same attribution problem arises in determining if a state actor was involved, even if the individual source is determined.[127] The inability to identify online actors serves as a barrier to effective regulation.[128] The problem is not simply that attackers cannot be identified, but is often that they are misidentified.[129] Observers have joked that government officials are often wrong as to the source, scope, and intent of an attack, but never in doubt.[130] The attribution problem means that losses from cyber breaches cannot be transferred to the responsible party. The various constituencies, therefore, are left to struggle with allocating losses.

One business constituency that could be held responsible is the technology sector that produces products containing vulnerabilities—the very vulnerabilities that can affect many entities and result in correlated failure discussed above.[131] Cybersecurity is completely dependent on code.[132] The heart of all cybersecurity is software, regardless

118. *See* Trautman, *supra* note 45, at 376–78.
119. Hurwitz, *supra* note 66, at 1513–14.
120. Daniel Bugni, *Standing Together: An Analysis of the Injury Requirement in Data Breach Class Actions*, 52 GONZ. L. REV. 59, 61 (2017).
121. Rowe, *supra* note 3, at 393.
122. *Id.*
123. Eastman, *supra* note 2, at 517.
124. *Id.* at 517–18.
125. Bonner, *supra* note 80, at 259–60.
126. *See* Johnson, *supra* note 58, at 277.
127. Doherty, *supra* note 93, at 16–17.
128. Trautman, *supra* note 45, at 377.
129. *See* BELLOVIN, *supra* note 36, at 40.
130. *Id.*
131. See Romanosky et al., *supra* note 64, at 6, for a discussion of correlated failure.
132. Hurwitz, *supra* note 66, at 1501–05.

of the complexity of the systems or the size of the entity seeking protection.[133] Code is law, and whoever controls the software makes the rules.[134] Contracts that are routinely upheld by courts immunize the technology sector from their business constituent clients.[135] End-user license agreements (EULAs) are used by developers to pass the cost down the line to the purchasing business.[136] Without any legal regime, insurance, or other mechanism to shift this risk, the risk falls to consumers—or the owners of the information lost—and they are completely reliant on the entity or business to protect the information.[137] They also lack any recourse against the technology sector because a strict liability regime is not in place, and legal requirements of privity stand in the way.[138] Without regulation, businesses may have little incentive to protect consumer information.[139] Businesses, furthermore, are preoccupied with other matters and fail to appreciate the current and future costs of security breaches.[140] Without liability protection, businesses are hesitant to share information that could contribute to better security.[141] If a breach occurs, breach notification statutes do not require the disclosure or information sharing of the vulnerability that led to the breach, again passing the cost and responsibility away from the developers to businesses and ultimately to consumers.[142]

Allocating responsibility in the case of a state actor is a more difficult task still. Little recourse exists in private international law, and exploration of the possibilities of using private international law to enhance cybersecurity are barely explored.[143] The likelihood of an armed response under the existing international regime is unlikely:

> These opinions on the future of use of force concepts aside, the combination of law and politics makes it clear that in any likely scenario an authorization by the UN Security Council to use force against a cyber-only capability is dubious at best. There is also little chance that the ICJ would ever make a finding that a cyber intrusion was an "armed attack" based on its excessively-high thresholds for the "use of force" and "armed attack" as coupled with the unwilling-

133. Marian K. Riedy & Bartlomiej Hanus, *It Is Just Unfair Using Trade Laws to "Out" Security Software Vulnerabilities*, 48 LOY. U. CHI. L.J. 1099, 1114–15 (2016).
134. Trautman, *supra* note 45, at 349 ("In cyberspace, as Lawrence Lessig says, '[c]ode is law.' James Grimmelman observes that '[u]nlike the rule of law, the rule of software is simple and brutal; whoever controls the software makes the rules. . . .'").
135. *See* Hurwitz, *supra* note 66, at 1515.
136. Riedy & Hanus, *supra* note 133, at 1109.
137. Rosenberg, *supra* note 56, at 1164.
138. Hurwitz, *supra* note 66, at 1524.
139. *Id.* at 1511.
140. Trautman, *supra* note 45, at 358.
141. Johnson, *supra* note 58, at 285, 297–98.
142. *See, e.g.*, CAL. CIV. CODE § 1798.82 (West 2018).
143. Shackelford, *supra* note 92, at 3–4.

> ness to attribute any hostile action to a State which does not openly declare ownership of said action.[144]

Although the LOAC may apply to cyberattacks by international consensus, the primary consideration under the existing regime is whether a cyberattack comports with the LOAC.[145] In other words, the LOAC does not serve as a bar to cyberattacks, and governments are generally opposed to new treaties regarding cyberattacks.[146] The sources of the LOAC are worth consideration in the context of cyberattacks. Beyond treaties, custom forms the basis of the LOAC and, as set forth above, the United States has both perpetrated cyberattacks and has not responded to attacks with force as a matter of custom.[147] Contemplation of the use of force to respond to cyberattacks is largely hypothetical because rarely do cyber operations "cross the armed attack threshold."[148] Instead, "[t]he majority of the cyber risk facing the public and private sectors lies in the arena of cybercrime and espionage."[149] Consider, for example, events of February 2013 when a government report detailed the activities of one unit of hackers of the Chinese People's Liberation Army, which was clearly condoned by the Chinese government.[150] The United States response was outlined as follows:

> First, we will increase our diplomatic engagement . . . [and] convey our concerns to countries where there are high incidents of trade secret theft . . . . Second, we will support industry-led efforts to develop best practices to protect trade secrets . . . . Third, [the Department of Justice] will continue to make the investigation and prosecution of trade secret theft by foreign competitors and foreign governments a top priority . . . . Fourth, . . . we will conduct a review of our laws to determine if further changes are needed to enhance enforcement . . . . Lastly, we will increase public awareness of the threats and risks to the U.S. economy posed by trade secret theft.[151]

This soft response to theft clearly attributable to an armed force of another nation contains no mention of the national security apparatus and provides the stark reality facing U.S. businesses, institutions, and consumers. The only institution capable of responding to this risk is the national security apparatus, but the consequence of U.S. conduct is that it cannot respond.

---

144. Keen, *supra* note 53, at 149.
145. Richmond, s*upra* note 17, at 864.
146. *Id.* at 865.
147. *Id.* at 869–71.
148. Shackelford, *supra* note 92, at 4.
149. *Id.*
150. Rowe, *supra* note 3, at 384–85.
151. *Id.* at 385 (quoting Victoria Espinel, *Launch of the Administration's Strategy to Mitigate the Theft of U.S. Trade Secrets*, WHITE HOUSE BLOG (Feb. 20, 2013, 2:59 PM), https://obamawhitehouse.archives.gov/blog/2013/02/20/launch-administration-s-strategy-mitigate-theft-us-trade-secrets [https://perma.unl.edu/28WK-6JYR]).

The purpose of this discussion is not to question the wisdom of the policy decisions to use cyberattack as either an offensive or preemptive national security measure. Nor is it to question the policy of telecommunications deregulation to foster private sector economic and infrastructure development. The purpose is to draw attention to the overwhelming risk these policies create, how they limit the U.S. government's ability to provide security, and to begin a discussion of cyber risk management.

III. RESPONSES TO CYBER RISK BEYOND INSURANCE ARE FAILING

"Public law" refers to a general classification of law concerning the relationship between the state and the people who compose it and the responsibilities of public officers.[152] This section focuses on criminal, administrative, and legislative responses to cyber risk. It is distinct from "private law," discussed in the next section, which concerns the relationships between individuals, corporations, and associations or, more simply put, between citizen and citizen.[153]

A. The Public Law Response Is Inadequate

In general terms, the United States was unprepared for the explosion of cyber risk, and there is a misperception that cybersecurity is a new problem. The reason for this unpreparedness is not entirely clear. Government recognition of the importance of computer security dates back to 1965; the Brooks Act created what is now called the National Institute of Standards and Technology (NIST), which is responsible for promulgating computer security standards.[154] Computer viruses date to the 1990s.[155] By the late 1990s, business losses to security breaches ranged into the hundreds of billions.[156] Cyber insurance policies began to appear by the late 1990s.[157] The Love Bug virus circulated in 2000, causing $15 billion in damage around the world.[158] The Y2k bug, or concern with computers' internal clocks not correctly recognizing two digit year dates for 2000 ('00) as coming after 1999 ('99), cost U.S. government and businesses as much as $225 billion.[159] It

152. *See Public Law*, BLACK'S LAW DICTIONARY (10th ed. 2014).
153. *See Private Law*, BLACK'S LAW DICTIONARY (10th ed. 2014).
154. *Public Safety Tech Topic #20*, *supra* note 44.
155. Keen, *supra* note 53, at 112.
156. Bonner, *supra* note 80, at 262.
157. DANIELLE GILMORE & DAVID ARMILLEI, *The Future Is Now: The First Wave of Cyber Insurance Litigation Commences, and the Groundwork Is Laid for the Coming Storm*, *in* INSURANCE LAW 2016: TOP LAWYERS ON TRENDS AND KEY STRATEGIES FOR THE UPCOMING YEAR 23 (2016) (available at 2016 WL 1089828).
158. Bonner, *supra* note 80, at 262.
159. DeWayne Lehman, *Senate: Y2k Fixes Worth the Billions Spent*, COMPUTERWORLD (Mar. 6, 2000), https://www.computerworld.com/article/2593290/it-management/

also led to significant education regarding cybersecurity: "'Most significantly, the IT infrastructure and mechanisms for more effectively managing it have been modernized,' . . . . 'Also, Y2k has caused a heightened level of knowledge among executive-level managers as to the importance and vulnerabilities of information technology.'"[160]

Public law authorities were not so educated, and the United States suffered from and continues to suffer from its gerontocratic tendencies with respect to cybersecurity. Around the time of Love Bug, the FBI Director did not have a computer in his office, and the Secretary of Defense needed staff to print out his e-mails for him.[161] The person responsible for protecting the United States from cyber threats, the Director of Homeland Security, commented publicly that he did not use e-mail as late as 2012.[162] As of 2013, eight out of nine U.S. Supreme Court justices—responsible for determining cyber legality—did not use e-mail.[163] Prominent Senators such as Lindsey Graham, Orrin Hatch, and Chuck Schumer do not use e-mail.[164] Many business and government leaders continue to be over the age of fifty.[165] As a result of leadership being, as former CIA Director General Michael Hayden coined them, "digital immigrants," no substantive cybersecurity legislation was passed during the big bang of cyber risk between 2002 and 2014.[166] The last effort in criminal law at the federal level pertaining to cybersecurity was the Computer Fraud and Abuse Act (CFAA) adopted in 1986.[167] The measures in place have unintended consequences. For example, employing hackers to retaliate against attackers has been suggested as a potential deterrent in the realm of protecting trade secrets, but this conduct is criminalized by the CFAA.[168] The same is true of legitimate security research activity.[169]

Initiatives to address cyber risk at the federal level are fragmented at best. Over 100 cybersecurity bills were introduced in the last several years, but most were unsuccessful.[170] Congress is generally reluctant to act.[171] The competing interests between business and consumer constituencies vexes the executive and legislative branches

---

senate—y2k-fixes-worth-the-billions-spent.html [https://perma.unl.edu/FL9H-6SPP].

160. *Id.* (quoting from the final report of the U.S. Senate Special Committee on the Year 2000 Technology Problem).
161. Trautman, *supra* note 45, at 350.
162. *Id.*
163. *Id.*
164. *Id.*
165. *Id.*
166. *Id.* at 350, 376.
167. 18 U.S.C. § 1030 (2018).
168. Rowe, *supra* note 3, at 420.
169. *Id.* at 408.
170. Johnson, *supra* note 58, at 298.
171. Eastman, *supra* note 2, at 522.

of government.[172] Lobbying opposes meaningful regulation, and potential regulation is feared too complex and too expensive.[173] No comprehensive data security legislation has passed.[174] What is in place is a disconnected patchwork of federal and state laws.[175] For example, NIST maintains a list of known software vulnerabilities but not of malware and security breaches.[176] Current public law has three glaring deficiencies: it is overly voluntary, it is overly reactive, and it lacks involvement of the national security infrastructure.[177] These deficiencies have rendered the public law structure largely ineffective.[178]

Consider, for example, the Cybersecurity Act of 2015.[179] In short, the Act encourages information sharing with the Department of Homeland Security (DHS), requires consumer personal information be removed from the information shared, and offers limited liability for sharing information.[180] The assumption is that if enough vulnerabilities are shared, blanket defenses can be derived against the finite number of threats.[181] This assumption is flawed because continuously probing, custom malware produces infinite possibilities for breach as hundreds of millions of new malware viruses generate each year.[182] Furthermore, the delay in detection means that information sharing comes too late to be effective.[183] As of late 2016, only one company had shared data with DHS under the Act.[184] Overall, the Act has been called too little, too late, like "driving a car by looking in the rearview mirror."[185] Arguably more effective measures, such as mandatory insurance and requiring basic measures (e.g., patching and updating), are absent in public law.[186]

172. Johnson, *supra* note 58, at 297–98.
173. Eastman, *supra* note 2, at 532–33.
174. Gordon, *supra* note 60, at 186.
175. *Id.* at 185.
176. ELING & SCHNELL, *supra* note 41, at 36.
177. Trautman, *supra* note 45, at 377.
178. Eastman, *supra* note 2, at 547–50.
179. Cyber Security Act of 2015, Pub. L. No. 114-113, 129 Stat. 2242 (changing various sections of the United States Code).
180. Eastman, *supra* note 2, at 546–47.
181. *Id.* at 548.
182. *Id.* at 548–49.
183. *Id.*
184. *Id.* at 549–50.
185. *Cybersecurity Act of 2015 Is Ineffective, Warns DB Networks*, CISION PR NEWSWIRE (Dec. 29, 2015), https://www.prnewswire.com/news-releases/cybersecurity-act-of-2015-is-ineffective-warns-db-networks-300197479.html [https://perma.unl.edu/2BRZ-E8DQ]; *see* Paul Rosenzweig, *The Cybersecurity Act of 2015*, LAWFARE (Dec. 16, 2015), https://www.lawfareblog.com/cybersecurity-act-2015 [https://perma.unl.edu/B5ZQ-UCL3].
186. Bonner, *supra* note 80, at 273 ("The majority of companies in the United States are not buying cyber risk insurance."); *Cybersecurity Act of 2015 Is Ineffective, Warns DB Networks*, *supra* note 185 ("Basic security hygiene includes applying software patches . . . .").

One notable exception to federal inaction is the FTC.[187] Critics have noted that the FTC stepping into this void may exceed jurisdictional limits because of the absence of congressional authorization.[188] The FTC brings enforcement actions under a standard of failure to provide reasonable and appropriate data security for personal information.[189] It has, however, created confusion because it has not produced a Trade Regulation Rule (TRR) or any other meaningful guidance or standards for the meaning of reasonable and appropriate security.[190]

> What many companies in the private sector may find troubling is that, although the . . . cost-benefit balancing test pushes them to evaluate their practices, the FTC has not published clear standards for what exactly constitutes unreasonable cybersecurity and data security measures. This places the FTC in an odd position where it can prosecute businesses for not maintaining reasonable data security practices without telling businesses what exactly they consider reasonable practices.[191]

Although it has been successful and brought fifty cases between 2002 and 2014, it is now facing growing resistance and litigation.[192] The enforcement actions are costly and case-by-case enforcement is inefficient.[193] The FTC will not be able to keep up with the increasing numbers of data breaches.[194] The FTC's enforcement actions are consumer-based, fail to address larger security concerns, and fail to educate about cybersecurity issues.[195]

Of primary concern for the subject matter herein is that public law contains no remedy for losses caused by failed cybersecurity. "[T]here are no public law institutions that generally ensure parties harmed by adverse cyber-incidents can secure recovery for their losses, that alter the perverse incentives faced by the various actors in the cybersecurity ecosystem, or that generally improve the overall quality of that ecosystem."[196] Reliance on the government in the United States is misplaced.[197] More concerning still is that the patchwork, ineffective body of public law in the United States is the world's most ad-

187. Gordon, *supra* note 60, at 190.

188. GILMORE & ARMILLEI, *supra* note 157, at *10–13.

189. Rosenberg, *supra* note 56, at 1179.

190. *Id.* at 1186–87 (discussing the FTC's failure to initiate new Trade Regulation Rules (TRR)).

191. Eastman, *supra* note 2, at 545.

192. Rosenberg, *supra* note 56, at 1178–79; *see also, e.g.*, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015) (challenging the FTC's authority to regulate data security as an unfair practice).

193. Rosenberg, *supra* note 56, at 1184.

194. Smith, *supra* note 81, at 405–06.

195. Hurwitz, *supra* note 66, at 1519–20.

196. *Id.* at 1516.

197. *See* Rowe, *supra* note 3, at 408.

vanced in its efforts to integrate cybersecurity into politics and business.[198]

B. Private Law Is Ineffective at Addressing Cyber Losses

Actions by consumers to redress cyber losses in private law face many challenges. Cases need to survive standing challenges, both facially and factually.[199] Because of the standing requirement of actual harm, losing data is insufficient and concrete damage, such as fraudulent charges, need to be demonstrated for successful litigation.[200] For this reason, plaintiffs have had marginal success in courts.[201] That is, if a consumer can even get to court. Private law remedies are limited by the attribution problem, and finding the responsible party in a technologically complex environment is a difficult hurdle to overcome.[202] The failure of plaintiffs to track insurance policies in their allegations may also risk the loss of insurance coverage.[203]

Furthermore, in actions by business constituents, EULAs prevent private law remedies by breached entities against developers of security software:

> On the face of these license agreements, the commercial user—the company that purchases the security software—bears the risk of loss in the event of a data breach. This contractual allocation of risk may be a perfectly reasonable choice for the licensee, for it can insure against that risk. But to the extent the lack of accountability on the part of security software vendors undermines the goal of data security, this scenario should be unacceptable to the millions of consumers whose sensitive personal information, housed by the purchasers of commercial security systems, is consequently more vulnerable to theft and misuse.[204]

Third, private law has left cyber insurance coverage in a state of chaos. Many insurance terms that could cover cyber loss either in standalone policies or in traditional liability policies remain untested in litigation.[205] Courts have avoided interpreting cyber insurance issues along traditional insurance lines, such as with consideration of intentional acts under liability policies.[206] The lack of judicial information has led to coverage unforeseen by insurers, preventing them from limiting the effect of correlated failure.[207] The reverse is also

198. *Id.* at 425.
199. Roddy, *supra* note 106, at 85.
200. Rosenberg, *supra* note 56, at 1172.
201. *Id.*
202. Hurwitz, *supra* note 66, at 1513–14.
203. Roddy, *supra* note 106, at 85.
204. Riedy & Hanus, *supra* note 133, at 1109.
205. Hurwitz, *supra* note 66, at 1537.
206. Romanosky et al., *supra* note 64, at 34.
207. Daniel Schwarcz, *Coverage Information in Insurance Law*, 101 MINN. L. REV. 1457, 1501 (2017).

true, with unforeseen gaps in coverage rendering policies illusory once considered by a court.[208] Overall, uncertainty has left insurers to reduce their exposure and limits.[209]

C. Public and Private Law Contradict Limiting Remedies

In *Zurich American Insurance Co. v. Sony Corp. of America*, a court held that Sony did not have coverage under policy language regarding publication of personal information after a data breach.[210] The reasoning was that the theft of data was not a publication by Sony and was, therefore, not covered.[211] At the same time, the FTC could bring an action for Sony's failure to make reasonable efforts at data protection. In other words, there is no coverage for actions of third parties in private law, but there is responsibility for third party acts in public law.[212] This can leave a business constituent in a terribly vulnerable position—being liable in regulatory enforcement without coverage.[213]

Furthermore, courts uphold policy exclusions for statutory violations.[214] When the effect of this is considered under the myriad of data protection duties found in state and federal law, the effect is chilling. For example, personal information was released by a video company, and coverage was avoided because the company violated a Michigan video rental privacy statute.[215] Private law rulings like this leave little comfort for consumers, business constituents, or insurers. The overall security environment is affected because businesses are dissuaded from information sharing for fear of public law prosecution or private law results leaving them uninsured.[216]

IV. THE PRIVATE INSURANCE MARKET IS UNABLE TO MANAGE CYBER RISK

A. The Market Is Undercapitalized

1. Current Market Capitalization

Empirical research indicates that the cyber insurance industry has the potential to serve as a highly effective regulator and an engine of risk management, even when compared to other forms of insur-

208. Erica J. Dominitz, *To Err Is Human; To Insure, Divine: Shouldn't Cyber Insurance Cover Data Breach Losses Arising (in Whole or in Part) from Negligence?*, BRIEF, Summer 2017, at 32, 35–36.
209. ELING & SCHNELL, *supra* note 41, at 16.
210. 127 A.D.3d 662 (2015) (discussed in Gordon, *supra* note 60, at 198–99).
211. *Id.*
212. Gordon, *supra* note 60, at 199.
213. *Id.*
214. *Id.* at 201.
215. Nat'l Union Fire Ins. Co. of Pittsburgh v. Coinstar, Inc., 39 F. Supp. 3d 1149, 1156 (W.D. Wash. 2014).
216. Trautman, *supra* note 45, at 379.

ance.[217] This evidence suggests that cyber insurance providers should strengthen organizational compliance and improve their response to data breaches.[218] The current cyber insurance market has reached $2 billion in annual premiums.[219] Boosted by SEC cyber risk disclosure requirements, the cyber insurance market may be worth at least $7.5 billion by 2020.[220] Higher estimates place the market at $20 billion by the end of the decade.[221] By way of comparison, the commercial insurance market in terms of net premiums was $247 billion in 2015.[222] The total value of insurance premiums written in the United States approaches $2 trillion annually.[223] The cybersecurity industry will greatly exceed the insurance market, ballooning to $170 billion by 2020.[224]

Development of the cyber insurance market is hampered by insurability issues related to low limits, policy variation, and hidden or indirect losses.[225] For example, Target, subject to a highly damaging breach in 2013, could not find adequate insurance.[226] "The Target breach demonstrates that demand is no longer the problem in insuring companies against cyber risk—it is now an issue of quality of supply."[227] The numbers referred to in this section for capitalization of the insurance market refer to premiums written, not coverage limits. The total amount of coverage is difficult to calculate.[228] Estimates place the premium to coverage ratio at about 1% with a $100,000 premium buying a policy limit of $10 million.[229] Rough estimates, therefore, place existing coverage in the United States at $200 billion.

---

217. Shauhin A. Talesh, *Insurance Companies as Corporate Regulators: The Good, the Bad, and the Ugly*, 66 DEPAUL L. REV. 463, 474–84 (2017) (comparing cyber insurance regulation of corporate entities with director and officer policies and employment and anti-discrimination (EPLI) coverage).

218. *Id.*

219. Romanosky et al., *supra* note 64, at 3.

220. Shackelford, *supra* note 92, at 14.

221. Romanosky et al., *supra* note 64, at 3.

222. *Id.*

223. Roddy, *supra* note 106, at 81.

224. Hurwitz, *supra* note 66, at 1511.

225. ELING & SCHNELL, *supra* note 41, at 31.

226. Trang, *supra* note 57, at 398, 423.

227. *Id.* at 423.

228. *See, e.g.*, Thomas H. Bentz Jr., *Is Your Cyber Liability Insurance Any Good? A Guide for Banks to Evaluate Their Cyber Liability Insurance Coverage*, 21 N.C. BANKING INST. 39, 40–41 (2017) (detailing some of the barriers to consistent valuation and attempting to synthesize the market data); Romanosky et al., *supra* note 64, at 3.

229. Romanosky et al., *supra* note 64, at 4.

2. Losses Outstrip the Market

As discussed above, the overall cyber loss exceeds $1 trillion per year.[230] Because of correlated failure and inherent interdependencies, cyber events have the potential to inflict natural-disaster-type damages in a single incident.[231] WannaCry ransomware damages in 2017 may total $4 billion.[232] In 2016, other ransomware attacks caused losses of $1.5 billion.[233] The Love Bug caused upwards of $15 billion in damage two decades ago.[234] More significantly, the cost per attack and per breach has risen. One attack cost Target $148 million.[235] One settlement of a class action lawsuit resulting from a breach cost Anthem $115 million.[236] One criminal gang alone caused banks to lose $1 billion.[237] The average cost per data breach is also increasing because of the recent trend towards litigation by consumers, with the current average breach costing $5.58 million.[238]

The losses are so high that they now represent existential risk to breached companies.[239] In the case of insurers, the issues of interdependency and correlated failure discussed above can serve to magnify damages into ranges that would be existential threats to many nations. Insurers fear a "Cybergeddon" event, and the probability of a critical information infrastructure breakdown in the next decade is 10%.[240] Such an event leading to the loss of e-mail, text messaging, cloud service, and online banking could cause $250 billion in losses in a few days alone.[241] Blackouts further concern insurers. The cascading effects of the loss of a power grid serving just fifteen U.S. states could cause damages of up to $1 trillion and insurance claims totaling over $70 billion.[242] These numbers represent the short term only. The estimated cost of a blackout in the United Kingdom in the short term is £49 billion, but with losses of £442 billion in the five years following the blackout.[243] Events like these, perhaps caused by a natural disaster instead of malicious conduct, could place additional pressure on insurers facing both cyber risk and property claims from a single event. The market is not large enough, with approximately $200 bil-

230. ELING & SCHNELL, *supra* note 41, at 10.
231. Trang, *supra* note 57, at 395.
232. Berr, *supra* note 29.
233. *Id.*
234. Bonner, *supra* note 80, at 262.
235. Eastman, *supra* note 2, at 517.
236. Meghan E. Ruesch, *Show Me the Bitcoin! The Costs of Cyber Risks and the Cyber-Insurance Coverage Landscape*, IN-HOUSE DEF. Q., Fall 2017, at 66.
237. Johnson, *supra* note 58, at 277.
238. Gordon, *supra* note 60, at 184–85.
239. Talesh, *supra* note 217, at 474.
240. ELING & SCHNELL, *supra* note 41, at 28, 31.
241. *Id.* at 28.
242. *Id.*
243. *Id.*

lion in coverage addressing $1 trillion in annual losses, and the potential loss is so extreme that the ability of the market to ever address the risk is questionable.

B. Cyber Risk Management Is Uniquely Difficult

1. From the Consumer and Business Perspective

Traditional risk management balances prevention and insurance, with the extent of preventative measures depending on the pricing of insurance:

> [R]isk management is often framed as a trade-off between investing in controls that reduce the average loss of a security event, and insuring against a loss. Indeed, [sources] show that as insurance becomes more affordable, there is less incentive to invest in self-protection (IT security) measures. At an extreme, if the price of insurance were very inexpensive, companies would be very unlikely to protect themselves against any kind of loss. Conversely, as insurance becomes more expensive, companies become more willing to self-protect (the price of insurance becomes much higher relative to any security measures). [Sources] also suggest that the demand for insurance is increasing in the size of the loss, and decreasing in probability of loss. That is, companies are more willing to insure against larger, less frequent loss events.[244]

This risk management framing, however, is questionable in the realm of cyber risk. "The classical risk management process consists of five steps: the definition of goals, risk identification, risk evaluation/analysis, the actual risk management (avoidance, mitigation, transfer, retention), and finally, the monitoring of risk. In each step of the classical risk management process, cyber risks show special characteristics."[245]

Data breaches simply are not always preventable, regardless of the adequacy of security measures.[246] Months before Target's malware breach in 2013, it invested $1.6 million in a malware detection tool, and JPMorgan spent $250 million on prevention before it was breached in 2014.[247] Both events were due to simple human error.[248] The sophistication of the entity can have little to do with the possibility of the breach.[249] The technological aspects of security measures renders them unmanageable and impossible to monitor internally for effectiveness.[250] The defining cyber characteristic of correlated failure is that a vulnerability in a widely used software application could be exploited.[251] Different products share code, so one vulnerability may

244. Romanosky et al., *supra* note 64, at 7.
245. ELING & SCHNELL, *supra* note 41, at 23.
246. Rosenberg, *supra* note 56, at 1184–85.
247. Eastman, *supra* note 2, at 517–18.
248. *Id.*
249. Hurwitz, *supra* note 66, at 1528.
250. *Id.*
251. Romanosky et al., *supra* note 64, at 6.

jeopardize whole lines of products.[252] Another defining cyber characteristic, interdependent security, means that a company's network security is only as good as the other networks to which it is connected.[253] Neither of these characteristics can be addressed by internal preventative measures.

The decision not to insure for cyber risk taken by almost three-quarters of U.S. companies is primarily related to the expense, but it is also related to policy exclusions and the belief that coverage is inadequate due to the overwhelming liability exposure.[254] Moral hazard and national security concerns have resulted in legal prohibitions of insuring against some forms of cyber risk, such as ransomware.[255] The unpreventable risk further extends beyond the business constituency and applies also to the consumers, who have no control over how their information is stored by the government or businesses and are forced to trust these other constituencies.[256] The lack of information regarding highly technical subjects for both business and consumer constituencies serves as a basic impediment to risk management.[257]

2. From the Insurance Perspective

Insurers view cyber insurance as a risk like no other because of limited data and "the quick evolution and proliferation of threats."[258] Insurers have two decades of experience with cyber insurance,

> But cyber insurance as a mass market product is still in its nascent stages; the risks it seeks to cover are difficult to measure, model, and price. As one economist noted, cyber coverage "is like insuring an aircraft in 1915—there's a lot more that we don't know than we do know at this point."[259]

The little amount of reliable data and information shared causes skewed insurance calculations.[260] Cyber risk stems from interdependencies, is subject to rapid change, and is characterized by a great degree of uncertainty with respect to data and modeling.[261] Information is difficult to find, and insurers are left to use hypotheticals to project losses.[262] The information available to insurers is often biased because its source is the cybersecurity industry or software developers

252. Riedy & Hanus, *supra* note 133, at 1103.
253. Romanosky et al., *supra* note 64, at 6.
254. PONEMON INST., *supra* note 77, at 17.
255. DeMuro, *supra* note 42, at 371–72, 392–93 (discussing the Patriot Act's blanket ban on ransomware payments in the United States and the blanket ban in the United Kingdom).
256. Rosenberg, *supra* note 56, at 1164.
257. Trautman, *supra* note 45, at 352–53, 358.
258. Trang, *supra* note 57, at 405.
259. GILMORE & ARMILLEI, *supra* note 157, at *1 (quoting Matthew Sturdevant).
260. Shackelford, *supra* note 92, at 15.
261. ELING & SCHNELL, *supra* note 41, at 10.
262. *Id.*

and is inherently unreliable because of the rapidly changing nature of cyber risk.[263]

Because of the unique management challenge created by cyber risk, insurers price premiums by guessing, outsourcing, basing premiums on competitor pricing, or basing premiums on other types or lines of insurance.[264] These methods result in flat-rate pricing and heavy reliance on asset value or revenue to base rates.[265] Furthermore, policy premium calculation for small businesses ends up being simplistic in its analysis of risk.[266] It also appears that insurers' lack of data has left entities seeking insurance to independently determine the terms and limits of their policies with less guidance from insurers than with other lines of insurance.[267] Despite underwriters having decades of experience with cyber insurance, few carriers are confident in their pricing models.[268]

Correlated failure in cybersecurity is a matter of concern for businesses, and it raises a serious challenge to the effectiveness of insurance as a risk management tool for cyber risk at a fundamental level. Insurance relies on risk pooling to mitigate risk:

> From the insurer's perspective, insurance is a risk-distribution device, that is, a mechanism by which the insurer pools multiple risks of multiple insureds in order to take advantage of "the law of large numbers." This statistical phenomenon is reflected in the financial world by the diversification of investment portfolios. It is embodied in the day-to-day world by the adage, "Don't put all your eggs in one basket."
>
> Many insureds who pay premiums will not incur losses. Insuring many independent risks in return for numerous premiums thus serves to distribute risk, in effect spreading a portion of the insurer's potential liability among his insureds. Distributing risk allows the insurer to reduce the possibility that a single costly claim will exceed the amount taken in as a premium and set aside for the payment of that claim.[269]

Insurance has successfully managed correlated loss, to a lesser extent, in other contexts including automobile insurance.[270] Cyber risk is globally connected, and the variety in production of IT systems is limited by economies of scale, suggesting that the degree of correlated failure in the cyber arena is much higher than what insurance has managed before.[271] This problem is exacerbated by the small pool currently available to manage that correlation and is considered by the

263. *Id.* at 14–15.
264. Romanosky et al., *supra* note 64, at 23–24.
265. *Id.* at 24, 32.
266. *Id.* at 32.
267. *See*, *e.g.*, Eileen Garczynski, *Protecting Firm Assets with Cyber Liability Insurance*, BUS. L. TODAY (2016) (summarizing guidance from a lawyer for law firms on cyber insurance); Bentz, *supra* note 228 (discussing similar guidance for banks).
268. Romanosky et al., *supra* note 64, at 23.
269. R.V.I. Guar. Co. v. Comm'r, 145 T.C. 209, 228 (2015) (internal citations omitted).
270. ELING & SCHNELL, *supra* note 41, at 14.
271. *Id.*

insurance industry to be a barrier to insurability.[272] A simple example demonstrates the problem. An insurance company provides automobile insurance for Bob and several million others; when Bob has an accident, insurance can manage this risk because many more insureds will not have an accident. This is true even when the loss is correlated if, for example, Bob's accident also involves Mary, who is also an insured, or damages a gas station leading to extensive property damage. Contrast this to the cyber context when Target may not suffer a loss, but a Windows vulnerability may be exploited or Internet servers go down, causing loss for significant portions of the insurer's clientele. The analogy of natural-disaster-type damages from a single incident accurately illustrates correlated failure.[273] It remains to be seen if the simple expansion of insurance markets can alleviate this fundamental issue.[274]

Insurance has shown itself to be unusually adept at regulating for cybersecurity in an atmosphere where government has not.[275] It also holds a great deal of promise to serve as a tool for information collection and assessment. The resultant sharing with consumers and businesses is a powerful mechanism for education, in that it allows constituent groups to understand and advocate for their best interests despite the highly technical nature of the risk.[276] In addition to improving security through education, if constituents were educated as to their best interests and could advocate politically, the response of private and public law institutions might improve as well. To date, the current insurance market has failed to reach this potential and a primary reason is the fundamental limitation of risk pooling with such highly correlated risk.[277]

C. Current Cyber Coverage Is Inadequate

Insurance coverage for cyber risk comes both as endorsements to other policies, such as to errors and omissions (E&O) policies, and as standalone policies.[278] The common first party and third party distinction crosses over from other insurance lines to cyber insurance:

> [F]irst party coverage covers losses for costs incurred directly by the insured. For example, it includes costs related to investigating the cause of a data breach or security incident, costs associated with restoring business services, the cost of notifying affected individuals, credit monitoring services, costs incurred from public relations and media services in order to communicate the event, extortion and ransom payments, and losses associated with business

272. *Id.* at 30.
273. Trang, *supra* note 57, at 395.
274. ELING & SCHNELL, *supra* note 41, at 30.
275. Talesh, *supra* note 217, at 474–84.
276. Hurwitz, *supra* note 66, at 1535–36.
277. *Id.* at 1536–39.
278. Romanosky et al., *supra* note 64, at 4.

> interruption . . . . [T]hird party liability covers the cost of defending against public or private litigation, settlements, judgments, or other rulings, as well as fines, fees, and settlements stemming from these lawsuits.[279]

The development of policy language occurs through a long process similar to a legislative process involving testing and market reaction, including judicial information through case law.[280] The result is the use of standardized forms prepared by the Insurance Services Office, Inc. (ISO).[281] The most typical type of commercial insurance is Commercial General Liability (CGL) insurance, and the business constituency views these policies as the first line of recovery in risk management.[282] In 2014, the ISO adopted new standard form exclusions for cyber risk in CGL policies in an effort to encourage the purchase of standalone cyber insurance policies.[283] Insurers have vigorously maintained that CGL policies do not cover cyber risk, even in policies predating the 2014 ISO form exclusions.[284]

1. Coverage Not Widespread

Only 24% of companies have insurance coverage for cyber loss.[285] This is despite the fact that companies value their information assets higher than PP&E assets.[286] Only 15% of information assets are insured as opposed to 59% of PP&E assets.[287] Companies elect to self-insure information assets twice as often as they elect to self-insure PP&E assets.[288] The likelihood of a major loss to information assets, however, is approximately four times that of PP&E.[289] Companies further recognize that probable maximum loss (PML) from a cyber event is higher than PML for PP&E assets.[290] More than half of companies suffered a significant breach in the last two years and acknowledge that risk is increasing, but almost half still have no plan to purchase cyber insurance.[291] Companies are more likely to report losses to PP&E assets than information assets, and almost one-third of companies believe disclosure of data breaches in financial statements is not required.[292] Most coverage is in the United States.[293]

279. *Id.* at 11–12 (internal citations omitted).
280. Podolak, *supra* note 86, at 377–78.
281. *Id.*
282. *Id.* at 382.
283. GILMORE & ARMILLEI, *supra* note 157, at 2.
284. *Id.* at 3–4; Podolak, *supra* note 86, at 382.
285. PONEMON INST., *supra* note 77, at 4.
286. *Id.* at 5.
287. *Id.* at 8.
288. *Id.*
289. *Id.*
290. *Id.* at 6.
291. *Id.* at 11, 13.
292. *Id.* at 3.
293. *See* Romanosky et al., *supra* note 64, at 3.

Many European companies are unaware the coverage exists, and the market in Europe is less than a tenth of that in the United States.[294] Overall coverage rates in the United Kingdom are only around 2%.[295]

Market incentives are inadequate to convince companies of their need for insurance.[296] Market behavior further affects the ability of insurance to serve as a regulator because trends indicate that firms elect not to purchase insurance until after they are breached. This behavior is concerning to insurers and affects premiums because it implies adverse selection, or the choice to purchase insurance rather than improve security.[297] Although lack of education plays a role in this,[298] other factors affect this decision-making, including expense, exclusions, and inadequacy of coverage versus risk.[299]

2. Coverage Mirrors Regulation Instead of Risk

A troubling trend is that coverage is mirroring regulation. The development of the insurance market has been in response to regulation, not to non-regulatory risk.[300] A recent example is the adoption of SEC regulations boosting the cyber insurance market.[301] Similarly, the coverage landscape supports this notion with data regulated industries, such as healthcare, which have higher rates of insurance coverage than other fields.[302] This coverage does not reflect overall risk. Healthcare, retail, and technology sectors have the highest rates of coverage at around 50%,[303] whilst the financial services sector is attacked three times more than any other.[304] Regulation also appears to be determinative of policy limits, with regulation causing limits to rise[305]

Empirical research into insurance serving as an effective regulator provides a warning in the cybersecurity context. Although insurance has been surprisingly adept at regulating in this field, insurance in highly regulated spheres, such as Employment Practice Liability Insurance (EPLI), has led insurance companies to move away from discouragement of illegal conduct into litigation avoidance.[306] For example, rather than teaching an insured's employees not to illegally

294. *See* ELING & SCHNELL, *supra* note 41, at 10, 29.
295. Romanosky et al., *supra* note 64, at 3.
296. Bonner, *supra* note 80, at 275.
297. ELING & SCHNELL, *supra* note 41, at 31.
298. Trautman, *supra* note 45, at 352–53.
299. *See* PONEMON INST., *supra* note 77, at 17.
300. *See* Gordon, *supra* note 60, at 195–96.
301. Shackelford, *supra* note 92, at 14.
302. Romanosky et al., *supra* note 64, at 3.
303. *Id.*
304. Johnson, *supra* note 58, at 283.
305. *See* Romanosky et al., *supra* note 64, at 4.
306. Talesh, *supra* note 217, at 490–91.

discriminate, insurers may instruct employers to insert venue clauses in contracts or insert these clauses into insurance contracts themselves to limit availability of damages (i.e., punitive damages) or applicable coverage.[307]

Corporate Directors' and Officers' Liability Insurance (D&O coverage) provides another example in which insurance could act as a regulator but has elected not to, thus providing little guidance and preventative education.[308] Put more harshly, D&O policies have become mechanisms that allow directors and officers to use shareholder capital to purchase insurance against shareholder lawsuits.[309] Purchase of insurance is not conditioned on any preventative measures, and no effort is made by insurers to influence corporate conduct.[310] This type of negative behavior by insurance companies tends to thrive in an atmosphere characterized by a lack of judicial information and broad, undeveloped legal standards.[311] In this environment, risk is equated with law, and litigation is viewed as inevitable. This perception, in turn, creates incentives for insurance to focus on lobbying and litigation avoidance rather than education and prevention.[312]

Cyber risk is characterized both by broad standards, such as the FTC's reasonable and appropriate data security for personal information standard,[313] and the corresponding failure to define or provide guidance as to what is reasonable.[314] Cyber insurance is plagued by a lack of judicial information.[315] These characteristics of cyber risk suggest that the potential of insurer as regulator in the cyber ecosystem is in jeopardy.

3. Coverage Is Difficult to Obtain

The cyber insurance market for consumers is still far less developed than that for business constituents facing informational and educational difficulties:

> Besides the low coverage of cyber risk in businesses, the market of cyber insurance for individuals is even less well-developed. There exist only very few personal cyber insurance products, and most people are not even aware of their existence. A study conducted by YouGov (2014) estimates that only one per cent of individuals possesses cyber insurance. However, the potential for

307. *See generally id.* at 490–97 (discussing insurance risk management in the employment and anti-discrimination law context).
308. *See id.* at 485–88.
309. *See id.*
310. *Id.*
311. *See id.* at 490–97.
312. *Id.*
313. Rosenberg, *supra* note 56, at 1179.
314. Eastman, *supra* note 2, at 545.
315. Schwarcz, *supra* note 207, at 1500–01.

> such products seems to be huge, as the survey finds that 19 per cent of the participants would be willing to buy such a product.[316]

In addition to the lack of knowledge regarding policy availability, the arguably largest risk facing consumers is the lack of information and resources explaining the risks and methods to protect themselves.[317] As data breaches continue to receive media attention, consumers become more numb to the risk.[318] Again, this evinces that the location of coverage amongst constituencies does not reflect the risk. A most vulnerable constituency has the least insurance, suggesting a failure of the insurance marketplace.

Coverage for business constituents can be difficult to obtain for several reasons. First, companies may struggle to find coverage at all.[319] Second, there is wild variation between policies.[320] Unlike cyber exclusions for CGL policies, cyber policy forms are not yet developed by the ISO, and development of standards is not on the horizon.[321] Policies are highly negotiable.[322] Cyber insurance does not have its own line of insurance for industry classification purposes, but is spread across multiple lines.[323] It is regulated differently in each U.S. state.[324] It requires expert assistance to purchase, and the purchase of unnecessary double coverage is a risk along with under coverage.[325]

"[The] cyber insurance market is referred to as the 'Wild West' of insurance, as new policies are created on a regular basis and as old policies are constantly updated and revised."[326] Consideration of these policies can be a daunting task. Banks, for example, must consider whether and to what degree to insure with the following types of coverage: forensic investigation coverage, crisis management cost coverage, notification or credit monitoring cost coverage, litigation and privacy liability expense coverage, regulatory defense and penalties coverage, online defamation and copyright and trademark infringement coverage, network business interruption coverage, general expense coverage, data loss and restoration coverage, cyber extortion coverage, computer fraud coverage, and improper electronic transfer of funds coverage.[327] Each of these coverages has individual complexi-

316. ELING & SCHNELL, *supra* note 41, at 30.
317. *See* Trautman, *supra* note 45, at 350, 352–53.
318. Hurwitz, *supra* note 66, at 1511.
319. *See* Trang, *supra* note 57, at 423.
320. Dominitz, *supra* note 208, at 33.
321. Jeffrey T. LaRosa & John P. Campbell, *Cyber Insurance Risks for Insurance Brokers and Lessons Learned from Flood Exposures*, N.J. LAW., June 2016, at 59, 62.
322. *See* Dominitz, *supra* note 208, at 33.
323. *See* Romanosky et al., *supra* note 64, at 9.
324. *Id.* at 4–5.
325. *See* Gordon, *supra* note 60, at 200–01.
326. *Id.* at 200.
327. Bentz, *supra* note 228, at 41–44.

ties. For example, business interruption coverage will specify a waiting period or down time before coverage is triggered and different coverages may have sub-limits.[328]

Beyond coverages, key exclusions must also be considered, including: prior acts, laptop and/or mobile device exclusions, bodily injury and property damage exclusions, mechanical or electronic failure exclusions, acts of war, employment practices exclusions, ERISA exclusions, illegal or fraudulent acts exclusions, insured exclusions, exclusion severability, regulatory exclusions, negligence exclusions, preferred vendor requirements, and reasonable security measure exclusions.[329] The interaction of the cyber coverage with the existing insurance coverage must be further explored, and cyber coverage must be reviewed with respect to existing D&O coverage, E&O coverage, CGL coverage, fiduciary liability insurance, EPLI coverage, and crime or fidelity coverage.[330]

On top of considering the various coverages, exclusions, and interaction with other policies, cyber policies are now offered by more than 500 insurance companies, and shopping for policies involves considerable effort and independent negotiation for terms with competing insurers.[331] Insurance brokers traditionally serve to assist in advising on policy provisions and shopping needs for different insureds.[332] Brokers, however, recognize that, like flood insurance, cyber insurance is rife with possible broker malpractice claims. Cyber insurance from the broker's perspective is more dangerous because of the variation in policies.[333]

4. Coverage Is Expensive

When engaged, insurers serve well as regulators of cyber risk,[334] but this engagement and the overwhelming nature of the risk has led cyber insurance to be expensive.[335] The ratio of premiums to coverage limits is three times higher for cyber insurance than other liability policies and is six times higher than property insurance.[336] Increased regulation and the recent success of class action suits will lead to further increases.[337] Target and Anthem faced a tripling of insurance

328. *Id.* at 40–41; Garczynski, *supra* note 267, at 3.
329. Bentz, *supra* note 228, at 48–52; Gordon, *supra* note 60, at 201; Romanosky et al., *supra* note 64, at 16.
330. Bentz, *supra* note 228, at 45–47.
331. Romanosky et al., *supra* note 64, at 3.
332. *See generally* LaRosa & Campbell, *supra* note 321, at 59–63 (discussing cybersecurity risks and the role of insurance brokers in providing coverage).
333. *Id.* at 62.
334. *See* Talesh, *supra* note 217, at 475–85.
335. Roddy, *supra* note 106, at 84.
336. Hurwitz, *supra* note 66, at 1537.
337. GILMORE & ARMILLEI, *supra* note 157, at 13.

premiums after breaches.[338] Anthem agreed to a $25 million deductible in order to obtain $100 million in limits.[339] Typical premiums can range in the hundreds of thousands.[340] The expense of policies is particularly harmful and potentially prohibitive to small businesses that face an increasing majority of attacks.[341] The costs of third party insurance is even higher.[342] Due to uncertainty and high risk, insurers seek lower limits.[343] Deductibles have risen and few companies secure policy limits beyond $15 million regardless of the exploding losses.[344] Limits, in general, are too small when compared to the risk.[345]

5. Obtained Coverage Is Illusory

In addition to lower limits, insurers respond to uncertain cyber risk with strict exclusions.[346] The greatest variation between cyber insurance policies is in their exclusions.[347] Although cyber insurance has value in prevention and as a regulator, serious concern remains about what policies cover. Standalone policies are marketed as "a flexible insurance solution designed by cyber risk experts to address the full breadth of risks associated with doing business in today's technology-dependent world," and as covering "direct loss, legal liability and consequential damages resulting from cyber security breaches."[348] When claims are made for common cybersecurity issues, they are often vigorously denied under policy language and exclusions.[349] For example, in 2014, P.F. Chang's suffered a loss of customer credit card information, and its credit card service, Bank of America Merchant Services (BAMS), was contractually responsible to MasterCard for fees and assessments for the breach.[350] In turn, P.F. Chang's reimbursed BAMS and sought coverage under a standalone cyber policy.[351] Coverage was denied by the insurer because, under policy language, coverage was limited to privacy injuries, which consumers had suffered, but BAMS had not.[352] A court agreed, granting sum-

338. Shackelford, *supra* note 92, at 15–16.
339. *Id.* at 16.
340. *Id.* at 15.
341. Bonner, *supra* note 80, at 274.
342. Romanosky et al., *supra* note 64, at 32.
343. ELING & SCHNELL, *supra* note 41, at 16.
344. PONEMON INST., *supra* note 77, at 13.
345. Smith, *supra* note 81, at 408.
346. ELING & SCHNELL, *supra* note 41, at 16.
347. Romanosky et al., *supra* note 64, at 11.
348. Roddy, *supra* note 106, at 85 (quoting marketing materials noted in P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co., No. CV-15-01322-PHX-SMM, 2016 WL 3055111, at *1 (D. Ariz. May 31, 2016)).
349. GILMORE & ARMILLEI, *supra* note 157, at 6.
350. *P.F. Chang's China Bistro*, 2016 WL 3055111, at *1–2.
351. *Id.* at *2.
352. *Id.*

mary judgment on the coverage issue in favor of the insurer.[353] Observers have commented that half of common data breach scenarios are arguably excluded from common standalone policies and, to date, the insurance industry has been aggressively pursuing exclusions.[354] Several of these exclusions are worth independent discussion.

Fifty-nine percent of all security breaches involve some form of human negligence.[355] This type of breach has been responsible for some of the most damaging security breaches, including breaches of Target and JPMorgan.[356] Many policies exclude coverage of damage from these breaches under policy language that requires, "Insured[s] to continuously implement the procedures and risk controls identified in the Insured's application for . . . insurance."[357] Similarly, policies require reasonable security measures for an insured to have coverage, and industry standard security measures may not be enough.[358] At the time of Anthem's breach in early 2015, for example, it was not industry standard for a health insurance company to encrypt personal information including Social Security numbers.[359] The reasonable security standard is further problematic with respect to regulation because the FTC uses a similar standard for prosecution.[360] Under this type of breach, therefore, FTC prosecution could result in the loss of insurance coverage.

Policies now exclude liability for statutory and regulatory violations.[361] This is problematic because companies may be caught between regulatory schemes and trying, for example, to protect data under one regime, like HIPAA, without violating the Patriot Act in the example of ransomware.[362] Regardless if the company chooses to pay the ransom or not, this exclusion could apply. It is important to note the trend of companies to insure only after breaches and in response to regulation.[363] The concern is that companies may purchase insurance to protect themselves from a risk that is specifically excluded by policies. Furthermore, no insurance market may exist for coverage until and unless regulation is in place.

353. *Id.* at *9.
354. Dominitz, *supra* note 208, at 33–34.
355. Podolak, *supra* note 86, at 372.
356. *See* Eastman, *supra* note 2, at 517–18.
357. Dominitz, *supra* note 208, at 34 (quoting policy language at issue in Columbia Cas. Co. v. Cottage Health Sys., No. CV-15-03432-DDP-AGRX, 2015 WL 4497730, at *1 (C.D. Cal. July 17, 2015) (case settled prior to disposition)).
358. Podolak, *supra* note 86, at 407.
359. *Id.* at 373, 407–08.
360. *See* Rosenberg, *supra* note 56, at 1179.
361. Gordon, *supra* note 60, at 201.
362. DeMuro, *supra* note 42, at 372–73.
363. *See* ELING & SCHNELL, *supra* note 41, at 31; Gordon, *supra* note 60, at 195–96; Shackelford, *supra* note 92, at 14.

Most risk in cybersecurity is cybercrime.[364] "Intentional hacking is by far the most common cause of stolen or compromised data."[365] Regardless, the single most common exclusion in cyber insurance policies is for criminal activity.[366] At least half exclude extortion and ransom.[367] Even determining whether a policy covers hacking is challenging. Some insurers employ an exclusion that "expressly require[s] that a loss be directly caused by, or solely and directly caused by, an insured cause."[368] In 2014, Sony fell victim to this type of policy exclusion when its PlayStation Network was breached.[369] During litigation, the trial court agreed with the insurer, Zurich, and upheld the clause.[370] The language in this type of clause excludes coverage for *all* losses due to hacking.

The vast majority of policies further exclude acts of war or terrorism.[371] It has been suggested that this exclusion might be viable in the cyber context, both with respect to CGL and standalone policies.[372] Although courts traditionally interpret this type of exclusion narrowly, it still poses a risk in the cyber arena with its attribution complexities.[373] The war analogy, frequently used in U.S. politics (i.e., the War on Drugs), has been applied to cyberattacks and this rhetoric is increasing.[374]

The contractor-coverage issue that arose in *P.F. Chang's* may arise under many policies that purport to be third party policies. In that case, coverage was lost because damage was done to an unanticipated third-party claim (at least unanticipated by P.F. Chang's) from a credit card service provider.[375] Yet another type of third-party issue arises and challenges the value or viability of cyber insurance. The inherent nature of the digital world relies on third parties much more than the physical world. Losses of Internet service and power outages are examples of reliance on third-parties. Many cyber insurance policies will exclude coverage for events like these.[376] Exclusions for independent contractors common in policies may lead to many coverage

364. Shackelford, *supra* note 92, at 4.
365. Riedy & Hanus, *supra* note 133, at 1103.
366. Romanosky et al., *supra* note 64, at 14.
367. *Id.* at 16.
368. Gordon, *supra* note 60, at 201 (quoting Podolak, *supra* note 86, at 405).
369. *See* Podolak, *supra* note 86, at 390 (discussing Zurich Am. Ins. v. Sony Corp. of Am., 2014 WL 3253541 at *1 (N.Y. Sup. Ct. Feb. 24, 2014)).
370. *Id.*
371. Romanosky et al., *supra* note 64, at 14.
372. Doherty, *supra* note 93, at 16.
373. *Id.* at 16–17.
374. *See generally* Rowe, *supra* note 3, at 394–403.
375. P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co., CV-15-01322-PHX-SMM, 2016 WL 3055111, at *1–2 (D. Ariz. May 31, 2016).
376. Romanosky et al., *supra* note 64, at 14.

disputes going forward.[377] The 2013 Target breach was accomplished using credentials of an independent contractor.[378]

Cyber policies were intended to fill gaps in coverage following ISO form changes excluding cyber risk issues.[379] Actual policy language is now creating new gaps between policies. For example, a CGL policy might exclude electronic data as property to avoid property damage claims resulting from cyber loss, but the cyber insurance policy meant to fill this gap might also exclude any data loss resulting from a physical cause or loss of tangible property.[380] The result is that if a data loss is caused by property damage, there is neither coverage under the CGL nor the cyber insurance policy.[381]

6. Adequate Coverage from the Private Market Is Unsustainable

The efforts of insurers to exclude coverage is understandable considering ballooning losses, lack of information, correlated failure preventing effective risk pooling, and the great efforts and expense insurers have taken to be positive regulators of their insureds.[382] A primary concern of the insurance industry is simply whether cyber risk is insurable.[383] The financial sector has taken note of the insurability issue facing cyber risk management. Moody's, Standard & Poor's, and Fitch, financial service companies which publish analysis of investments, all have warned that they will consider downgrading insurers for writing aggressive (adequate) standalone cyber policies.[384] Standard & Poor's went as far as instructing insurers to avoid reliance on data in writing policies because of uncertainty—advising insurers instead to set low limits and strict exclusions to avoid scrutiny by rating agencies and potential downgrading.[385]

The efforts of insurers along these lines makes the purchase of these policies questionable.[386] "While lawyers often counsel insured to buy standalone cyber coverage on top of CGL, even the combination of the two may not be enough to protect the insured from costly losses in

377. Nathan L. Colvin & Timothy C. Dougherty, *Trends for Potential Insurance Coverage for Losses Arising from a Data Breach*, 44 N. KY. L. REV. 29, 34 (2017).
378. *Id.*
379. *See* Podolak, *supra* note 86, at 403–04.
380. *Id.*
381. *Id.*
382. ELING & SCHNELL, *supra* note 41, at 16 (discussing why insurers seek to avoid coverage in the cyber context); GILMORE & ARMILLEI, *supra* note 157, at 5–6, 14 (discussing efforts of insurers); Schwarcz, *supra* note 207, at 1500–01 (discussing the lack of judicial information available to insurers); Talesh, *supra* note 217, at 475–85 (discussing positive, proactive efforts of insurers and how this has made them effective regulators).
383. ELING & SCHNELL, *supra* note 41, at 10, 29.
384. *Id.* at 16.
385. *Id.*
386. Smith, *supra* note 81, at 408.

the event of a cyber attack."[387] Moreover, the more insurers seek to limit coverage through exclusions, the less they regulate effectively.[388] Observers have gone as far as to question whether cyber policies will even continue to be underwritten.[389] The current insurance market "create[s] a perfect storm that will likely lead to claims of coverage gaps, misplaced coverage and improper coverage."[390] Traditional elements of the insurance relationship, such as the relationship between insurance broker and client, are ineffective in this context.[391] If Sony, Target, P.F. Chang's, and Anthem, with cadres of in-house and outside counsel and vast resources to obtain consulting on insurance, cannot negotiate this market, it is unreasonable to expect Bob's Bait Shop, which digitalizes personal information for purposes of game and fish licensing and accepts credit cards, to have any success. Unfortunately, the hacker's target de jour is a business like Bob's.

V. CYBER INSURANCE IS VITAL FOR CYBER RISK MANAGEMENT

Without insurance, the risk management outlook is bleak:

> [U]sers are largely helpless, firms are largely unknowledgeable, software is generally insecure, federal agencies are generally impotent to bring about meaningful change in the structure and operation of private markets, and attackers are largely judgement-proof. As an initial matter, it would offer consumers redress when cyber-incidents occur. But, more importantly, insurance and insurers play a regulatory role. They collect and study information about best practices, they train and educate their customers, they engage with other institutional actors in ways that can improve the overall quality of the security ecosystem, and they lobby for legislative and regulatory changes that reduce their exposure to risk—which, in the security context, means lobbying to reduce overall risk.[392]

The use of electronic devices and the Internet is essential to our daily life from the personal uses of e-mail, shopping, social media, entertainment, and geolocation to our business uses of networks.[393] Businesses cannot afford to be without insurance and will not remain competitive without it.[394] Improved security and insurance against losses will become more important to new economic developments considering the risk associated with autonomous vehicles and aircraft

387. Romanosky et al., *supra* note 64, at 33 (internal citation omitted).
388. Hurwitz, *supra* note 66, at 1537–38.
389. Bonner, *supra* note 80, at 273.
390. LaRosa & Campbell, *supra* note 321, at 63.
391. *See id.*
392. Hurwitz, *supra* note 66, at 1500.
393. Rosenberg, *supra* note 56, at 1163–64.
394. Gordon, *supra* note 60, at 184–86.

control systems.[395] The DHS recognizes the critical nature of a vibrant cyber insurance market to overall security.[396] Losses are common and will affect many businesses.[397] It is worth repeating that cyber insecurity is potentially the United States' Achilles' heel.[398]

VI. FEDERAL CYBER INSURANCE: A SOLUTION TO CYBER RISK MANAGEMENT

In sum, the current cyber risk management ecosystem faces tremendous losses with little data about them. Potential remedies trigger competing constituent and political interests. Correlated losses challenge traditional notions of the working of insurance resulting in undercapitalization. Constituencies lack sufficient information to act in their best interest. National security institutions have narrowed possible responses through their own cyber activity. Other public law institutions fail to regulate effectively. Private law provides little or no remedy to those harmed. And the security failures keep coming, and coming, and coming.

A. Public/Private Collaboration Is Required

National cybersecurity depends on public and private cooperation because so much of the nation's critical infrastructure is private.[399] Moreover, the security of communications and information systems, including voice, data, video, and Internet, is indispensable to all other critical industries in the United States.[400] The private sector, however, has inadequate incentives to spend on security.[401] Recognizing an unusual circumstance in which national security depends so heavily on the private sector, President Obama opined that the only solution to the country's cybersecurity woes is through public and private collaboration:

> First, this has to be a shared mission. So much of our computer networks and critical infrastructure are in the private sector, which means government cannot do this alone. But the fact is that the private sector can't do it alone either, because it's government that often has the latest information on new threats. There's only one way to defend America from these cyber threats, and that is

395. *See* Caleb Kennedy, Note, *New Threats to Vehicle Safety: How Cybersecurity Policy Will Shape the Future of Autonomous Vehicles*, 23 MICH. TELECOM. & TECH. L. REV. 343, 343–50 (2017).

396. Gordon, *supra* note 60, at 202.

397. PONEMON INST., *supra* note 77, at 24.

398. *See* Trautman, *supra* note 45, at 386.

399. *See* Eastman, *supra* note 2, at 519–20, 528–31.

400. *Public Safety Tech Topic #20*, *supra* note 44.

401. Eastman, *supra* note 2, at 522, 529–31.

> through government and industry working together, sharing appropriate information as true partners.[402]

Collaboration has the potential to reduce the detection gap between cyberattack and detection.[403] Public and private cooperation and information sharing can assist the insurance industry with better data for premium calculations, and government backstops could alleviate risk concerns and affect risk pooling.[404] Academic formulations of global security approaches are available and the financial sector, one of the first data-regulated sectors, has served as a test bed for security approaches.[405] Public and private information sharing aided in mitigating attacks on ten major U.S. banks in 2012 and 2013.[406] More collaboration is necessary and has the potential to mitigate cyber losses, but even financial institutions hesitate to share information with the public, the government, and each other because of liability concerns.[407] Industry has focused on seeking safe harbor provisions in law,[408] but adequate and reliable insurance could provide the same comfort to permit information sharing.

The insurance industry recognizes that cyber risk is a problem of international scope and needs consideration at a national level.[409] Commentators have further noted that law enforcement related to cybersecurity needs to come from a federal level.[410] Somewhat overlooked acts by the federal government have had dramatic, positive impacts on cyber insurance. After exclusions of cyber risk were formalized in ISO forms in 2014,[411] the Federal Insurance Office classified cyber liability policies as qualifying under TRIP and required standalone cyber insurance policies to comply with TRIA effective April 2017.[412] This move encouraged the development of the standalone cyber insurance policy market.[413] TRIA, however, is not designed to address data breaches, but only acts of terrorism that manifest in damage to physical infrastructure, like the Natanz attack.[414]

---

402. Barack Obama, Former U.S. President, Remarks on Signing an Executive Order on Promoting Private Sector Cybersecurity Information Sharing in Stanford, California, *in* DAILY COMP. PRES. DOCS. (Feb. 13, 2015), at 3–4.
403. Lawrence et al., *supra* note 34, at 43–46.
404. *Id.* at 46, 52.
405. Gordon, *supra* note 60, at 203–08.
406. Johnson, *supra* note 58, at 284–85.
407. *Id.* at 297–98.
408. *Id.* at 298–99.
409. ELING & SCHNELL, *supra* note 41, at 35.
410. Trautman, *supra* note 45, at 355.
411. GILMORE & ARMILLEI, *supra* note 157, at 2.
412. Roddy, *supra* note 106, at 84.
413. *See* Romanosky et al., *supra* note 64, at 4.
414. Roddy, *supra* note 106, at 84.

Cyber insurance is one of the two most commonly suggested mechanisms for improving the cybersecurity ecosystem as a whole, but it faces pragmatic and logistical problems related to the insurance industry's unwillingness to underwrite broad policies.[415] The insurance industry has voiced willingness and has suggested public and private partnerships, including government mandated minimal security, information sharing, government backstops for extreme risk scenarios, better criminal enforcement, and anonymous reporting of security issues.[416] There is little doubt that the U.S. government must step in to address this weighty security issue.[417]

B. Defining the Threat Matrix

Before discussing different models of federal insurance programs and considering their potential application in cyber risk management, it is helpful to consider and classify the nature of cyber threats. For this purpose, this section will rely on Steven M. Bellovin's classification of threats in his book *Thinking Security*.[418] Bellovin classifies attackers by skill and determination or "degree of focus" as "joy hackers," "opportunistic hackers," "targetiers," or "advanced persistent threats."[419]

Joy hackers fit the stereotypical teenager in his parents' basement, having little skill or focus.[420] The hacking has little purpose other than potentially gaining knowledge.[421] Joy hackers can inflict damage, but ordinary care suffices for protection.[422] If security is sufficient, they will attack an easier target.[423] Joy hackers can develop more focus and become targetiers or develop skill and become opportunistic hackers.[424] In the 1990s, this was the most common type of hacker.[425] Now, however, most hackers have more specific motivation, whether pursuing criminal goals or hacktivism.[426]

Opportunistic hackers are more dangerous because of skill level.[427] They have an arsenal of vulnerabilities and techniques including zero days, but the attacks are random—only targeting if paid to or if they

415. Hurwitz, *supra* note 66, at 1497–99.
416. ELING & SCHNELL, *supra* note 41, at 10, 35–36.
417. Smith, *supra* note 81, at 408.
418. *See* BELLOVIN, *supra* note 36.
419. *Id.* at 34–35.
420. *Id.*
421. *Id.* at 35.
422. *Id.*
423. *Id.*
424. *Id.* at 34–35.
425. *Id.* at 32.
426. *Id.*
427. *Id.* at 35.

are annoyed by a target.[428] This group may be the most important to defend against.[429]

Targetiers are quite dangerous—aiming at a target and even dumpster diving to gain reconnaissance.[430] Even with low skills, dangerous methods can be purchased, even zero days.[431] Some are insiders out for revenge and already possess knowledge of a network.[432] They may also be paid to attack a target.[433]

The last and most dangerous classification of hackers is advanced persistent threats (APTs).[434] These attackers possess good intelligence and technical skill and make defense a difficult task.[435] Intelligence will allow these attackers to work around the strongest cryptography instead of through it.[436] Reconnaissance will be gained through burglary, bribery, and blackmail, and the vulnerabilities exploited will not always be online.[437] Efforts towards security will not be sufficient.[438] Levels of APTs range from sophisticated criminals, sometimes in government employ, like Alberto Gonzalez, to nation states, like Israel and the United States with Stuxnet.[439]

Possible models of federal insurance programs may be based on the previously used classification of cybersecurity constituency groups: consumers, investors, businesses, law enforcement, government, and national security entities.[440]

C. Federal Insurance Models

Federal insurance programs are pervasive. Provision of insurance consumes so much of the budget that the United States has been referred to as "an insurance company with an army."[441] Beyond healthcare, the U.S. government insures crops, livestock, individuals administering smallpox countermeasures, the domestic airline industry from war risk, U.S. investors from political risk in foreign countries, the maritime industry from war risk, pension benefits, losses from nuclear accidents, flood losses, bank and credit union deposits,

428. *Id.*
429. *Id.*
430. *Id.*
431. *Id.*
432. *Id.*
433. *Id.*
434. *Id.* at 34–37.
435. *Id.* at 36–37.
436. *Id.* at 39.
437. *Id.*
438. *Id.*
439. *Id.* at 33, 36–37.
440. Trautman, *supra* note 45, at 351.
441. Paul Krugman, Opinion, *An Insurance Company with an Army*, N.Y. TIMES (Apr. 27, 2011, 8:08 AM), https://krugman.blogs.nytimes.com/2011/04/27/an-insurance-company-with-an-army/.

commercial space launches, and commercial losses to terrorism.[442] These programs are managed by a variety of federal agencies and most were adopted during three time periods: in the 1930s Great Depression period, in the early 1970s, and in the early 2000s in response to the 9/11 attacks.[443] They insure vast amounts of assets ranging in premiums written at levels similar to that of the current cyber insurance markets (crop and livestock insurance) to amounts that exceed the private insurance market entirely.[444] For example, in 2003 the FDIC insured more than $2.9 trillion in bank deposits, and the Pension Benefit Guaranty Corporation insured more than $2.2 trillion in corporate retirement benefits.[445] On a different level altogether, Medicare and Medicaid currently expend in excess of $1 trillion per year combined.[446]

The purpose of this Comment is to begin a discussion about a federal insurance program for cyber risk management. It discusses three models of federal insurance to start this dialogue: federal backstop insurance (commercial space launch insurance and TRIP), FDIC coverage of bank deposits, and NFIP. Each of these models and the risk they intend to address contain parallels to cyber risk management issues discussed above. This short discussion serves as a starting point to scratch the surface of complex policy. Full analysis of the programs would require vast analysis not possible herein.

1. Federal Backstop Insurance (TRIP and Commercial Space Law)

Before 9/11, insurance companies did not address terrorism as a risk because of small, uncorrelated losses.[447] After the 9/11 attacks, banks required commercial projects to obtain terrorism coverage prior to funding.[448] No market, however, existed for this insurance because insurers and reinsurers left the market through exclusions.[449] Large commercial projects faltered.[450] To stabilize the insurance market and

442. *Insurance Programs*, CTR. FED. FIN. INSTITUTIONS (Aug. 26, 2004), https://web.archive.org/web/20040826092919/http:/www.coffi.org:80/pubs/Insurance%20Programs%20Rev1.pdf.
443. *See id.*
444. *See id.*
445. *Id.*
446. *NHE Fact Sheet*, CTRS. FOR MEDICARE & MEDICAID SERVS., https://www.cms.gov/research-statistics-data-and-systems/statistics-trends-and-reports/nationalhealthexpenddata/nhe-fact-sheet.html [https://perma.unl.edu/G3RS-MMBL] (last updated Apr. 17, 2018).
447. Andrew Gerrish, Note, *Terror CATs: TRIA's Failure to Encourage a Private Market for Terrorism Insurance and How Federal Securitization of Terrorism Risk May Be a Viable Alternative*, 68 WASH. & LEE L. REV. 1825, 1827 (2011).
448. *Id.* at 1828.
449. *Id.*
450. *Id.*

encourage the development of adequate private terrorism insurance, TRIA was adopted in 2002 with its corresponding program, TRIP.[451] This program, meant to be temporary, but having been extended, places the government in the place of reinsurer.[452] Should losses due to terrorism exceed thresholds and qualifying insurers suffer enough losses, the government will step in to cover most losses over the threshold amounts.[453] It requires insurers to disclose information and offer insurance meeting guidelines to qualify for the reinsurance.[454] In addition to premium surcharges and other mechanisms to offset government expenditure,[455] it extended jurisdiction for terrorism victims to attach assets of foreign countries for terrorism damages.[456]

Similarly, the Commercial Space Launch Act of 1984 and the SPACE Act of 2015 require businesses and government to undertake risk analysis (calculating maximum probable loss) as part of the space launch licensing regime.[457] Once done, the business constituent must provide insurance or demonstrate financial responsibility up to the maximum probable loss, but not exceeding a cap of $500 million for third-party claims, $100 million for U.S. government claims, or the amount of insurance available on the world market at a reasonable rate.[458] The regime requires that the insurance cover all participants including government, businesses, and third parties, and enforces a waiver of claims between the interested parties to a launch.[459] The government then reinsures claims beyond the maximum probable loss up to $1.5 billion.[460] The purpose of these statutes is to promote commercial development in an inherently risky environment, recognizing commercial space activities as high risk, high reward endeavors.[461] More specifically with respect to insurance, the legislation is intended to create an adequate pool of insurability.[462]

The backstop model is attractive in the context of cyber risk management for several reasons. First, it could address the risk that business and consumer constituents can never expect to address without government and national security intervention, APTs, and the extreme damages and correlated losses that result from APT attacks.

451. *Id.* at 1829.
452. *Id.*
453. *See id.* at 1831–32.
454. Roddy, *supra* note 106, at 84.
455. Gerrish, *supra* note 447, at 1832–37.
456. Rachel Waters, Note, *Banking on Jurisdiction:* Weinstein v. Islamic Republic of Iran, 3 WAKE FOREST J.L. & POL'Y 191, 201–02 (2013).
457. 51 U.S.C. § 50914(a)(1) (Supp. 2016).
458. *Id.* § 50914(a)(1), (3).
459. *Id.* § 50914(a)(4)–(5).
460. *Id.* § 50915(a)(1).
461. *Id.* § 50901.
462. Michael Dodge, *The U.S. Commercial Space Launch Competitiveness Act of 2015: Moving U.S. Space Activities Forward*, 29 AIR & SPACE L., no. 3, at 4 (2016).

Second, it could foster insurance market development by requiring risk analysis and capping private market losses. Federal insurance programs currently insure larger amounts of assets and pay out more than the private market can sustain.[463] Federal backstop insurance provides potentially limitless market capitalization to facilitate risk pooling, both by providing federal resources and by requiring large entities to insure as a regulatory matter. This capitalization could permit underwriting of policies that do not exclude common cyber events and regulatory policy provisions would take the place of judicial information. Third, it could provide a vehicle to share information between business and government who jointly share risk and liability for losses. Fourth, it could promote education by requiring disclosure of risk to those purchasing insurance from government to insurer to business or consumer purchaser. Fifth, the backstop programs may address the attribution problem, which can be problematic in both space vehicle accidents and terrorist attacks like in cyberattacks or security failures. Commercial space law places responsibility for inherent, unavoidable risk on the launcher with a government backstop. TRIA places responsibility for terrorist losses on an insurer with a government backstop. Finally, TRIA provides a model for government to recoup insurance costs and provides jurisdictional expansion for consumers to recover against foreign actor APTs.

2. FDIC

FDIC coverage is federal backstop in reverse, covering an amount of loss up to a cap. Hundreds of banks failed each year in the 1920s.[464] This accelerated in the 1930s because of withdrawal requests causing banks to restrict credit and created a disastrous cycle. As banks sought liquidity and consumer confidence plummeted, runs accelerated further, which caused banks to again seek more liquidity.[465] This cycle began to victimize large urban banks including the Bank of the United States in New York, one of the country's largest.[466] Eventually, this created an unusual circumstance where those concerned with losses due to bank failure and those concerned with the survivability of the banking structure as a whole were united in alarm to an extent that allowed legislation.[467] At the root of the problem was a toxic mix of failed government bank policies and poor bank manage-

463. *See Insurance Programs*, *supra* note 442; Romanosky et al., *supra* note 64, at 3 (demonstrating the 2003 FDIC insurance level of $2.9 trillion as compared with the 2015 market capitalization of cyberinsurance of $2 billion).

464. FED. DEPOSIT INS. CORP., FEDERAL DEPOSIT INSURANCE CORPORATION: THE FIRST FIFTY YEARS: A HISTORY OF THE FDIC 1933–1983, at 33 (1984), https://www.fdic.gov/bank/historical/firstfifty/ [https://perma.unl.edu/L54P-XNDC].

465. *Id.*

466. *Id.* at 35.

467. *Id.* at 33.

ment, including speculation with deposits.[468] Put in terms of constituents, consumers suffered losses beyond their control because of a toxic mix of bad business and poor government policy.

The FDIC was created with the Glass-Steagall Act as part of the Banking Act of 1933, which limited the interaction of commercial and investment banking.[469] The effect of insurance was immediate, and by 1934, bank deposits increased by almost one-quarter and banks stopped failing. It was so successful that industry opposition to accompanying regulation evaporated.[470] In order to qualify for insurance, banks had to meet capital requirements, realistic future earnings prospect requirements, quality management standards, and service of the community standards.[471] Insurance rates were based on one-twelfth of a percent of total bank deposits, half of the anticipated rate, and banks were not required to purchase FDIC stock as originally thought necessary.[472] Many emergency measures permitted to the FDIC by the Banking Act, such as issuing notes, never became necessary.[473]

The FDIC model is attractive in the context of cyber risk management for several reasons. First, it is the only federal insurance model that focuses primarily on the consumer. Just like looking for the "FDIC" sticker on the bank door, consumers could vet credit cards, financial institutions, investments, and even retail stores and online shopping websites by looking for a simple label. This would allow a consumer to rapidly assess his or her privacy interest without becoming educated in technology or security. Second, it could have a dramatic effect on basic security. For a small portion of per transaction costs, likely less than credit card processing fees, businesses could purchase per transaction or per consumer insurance so long as they met a set level of basic security measures. Very basic security methods can prevent four-fifths of breaches.[474] These protocols have been developed, but they need consistent application.[475] The backstop model addresses APT attacks and the FDIC model addresses the other three threat types with great affect against joy hackers and opportunistic hackers.

468. *Id.* at 33–39.
469. Banking Act of 1933, H.R. 5661, 73d Cong., 48 Stat. 162.
470. FED. DEPOSIT INS. CORP., *supra* note 464, at 49–50.
471. *Id.* at 52.
472. *Id.*
473. *Id.* at 52–53.
474. Rowe, *supra* note 3, at 415.
475. *See*, *e.g.*, BELLOVIN, *supra* note 36, at 203–89; Gordon, *supra* note 60, at 203–08.

3. NFIP

The last model considered is flood insurance. "The three basic components of the NFIP are: (1) the identification and mapping of flood-prone communities, (2) the requirement that communities adopt and enforce floodplain management regulations that meet certain minimum eligibility criteria in order to qualify for flood insurance, and (3) the provision of flood insurance."[476] In the late 1960s, Congress recognized that flood insurance was extremely difficult for homeowners to obtain.[477] Large, correlated losses made it uneconomical for the private insurance market to offer insurance or offer insurance at reasonable rates.[478] Consumers were unwilling to pay large enough premiums to support the market[479] due to lack of education and the seeming remoteness of the risk. The Federal Emergency Management Agency (FEMA) administers NFIP and controls policy terms.[480] In short, private insurers write NFIP policies, but the government pays losses under them.[481] Like cyber insurance, it is gap-filling insurance and is considered key-event insurance.[482]

The NFIP model is attractive in the context of cyber risk management for several reasons. First, it was developed to provide gap insurance in response to correlated failure great enough to render policy premiums prohibitive. This formulation has parallels with cyber insurance. NFIP was further developed with prevention in mind and models how an insurance program can bring uniformity across state and local regulation. It shows the possibility of educating on complex issues, such as floodplains and floodplain management. The policy is based on cost-benefit analysis with the cost of prevention being less than the cost of disaster relief. In the cyber ecosystem, this model demonstrates a method to deal with correlated failure and security interdependency. For example, if a Windows vulnerability was exploited across many systems, flood insurance could provide a model to address that loss. It could benefit all constituents with all threat levels, providing businesses and even consumers with reasonably priced insurance while handling large-scale damage and loss from APTs.

Corresponding regulation to qualify for insurance may improve security. NFIP is included here because it is the only model that suggests methods to regulate the powerful and elusive software and technology companies. For example, software and technology develop-

476. Nat'l Wildlife Fed'n v. FEMA, 345 F. Supp. 2d 1151, 1155 (W.D. Wash. 2004).
477. *Id.* at 1156.
478. *See* 42 U.S.C. § 4001 (Supp. 2016).
479. LaRosa & Campbell, *supra* note 321, at 62.
480. Gowland v. Aetna, 143 F.3d 951, 953 (5th Cir. 1998).
481. LaRosa & Campbell, *supra* note 321, at 62.
482. *Id.* at 60, 62.

ment would be regulated by insistence of the insurance program on certain cybersecurity standards before allowing businesses to insure at the government rate, like banks requiring flood insurance to mortgage properties. Businesses could pass these costs to the technology sector by demanding and creating a market for secure products. It is a model that is forward looking with insurance as part of a larger scheme to address security and reduce losses by controlling development, not just reacting to the ever-morphing cyber threat. Insurance has tackled correlated and monumental losses before, but cyber insurance must be unusually proactive due to the changing nature of the risk. The NFIP demonstrates how insurance efforts could control development over decades to reduce losses in the long term.

These models are provided to begin discussion of different approaches to different cybersecurity problems. A comprehensive program taking pieces from each should be considered. At this level of analysis, it is productive to discuss benefits and problems with national insurance at a broad, general level.

D. General Benefits of National Cyber Insurance

The involvement of the U.S. government in cyber insurance would be beneficial to education. Constituents in the ecosystem need knowledge to act, and this need ranges from insurers to business to consumers. The U.S. government has more information on cyber threats than any other entity. Bringing government into insurance and providing budgetary incentives to minimize loss has the potential to benefit other constituencies and allow the currently limited national security infrastructure a more productive role in preventing loss. Affordable insurance that covers a broad base of losses would allow businesses and the technology sector to share more freely with government, thus improving the scope of that clearinghouse without fear of existential liability exposure.

Affordability also would limit adverse selection and focus business on prevention instead of purchasing insurance to avoid prevention. Federal assets backing private insurers would allow insurers to continue with that unusually effective regulation instead of devolving in litigation prevention and lobbying. Broader coverage would improve the size of pool available to share risk and, like TRIA, a program could be developed as a temporary measure if the market were able to take over after the risk pool is sufficient.

Mandatory insurance (both generally and for federal contractors), strict liability for data breaches, and more rigid requirements for information sharing have been suggested as remedial measures.[483]

483. Bonner, *supra* note 80, at 277 (federal contractor mandatory cyber insurance); Hurwitz, *supra* note 66, at 1542–46 (strict liability encouraging insurance); John-

Having affordable cyber insurance available that covers common cyber events increases the potency of these programs. Strict liability is arbitrary and may target business interests in favor of consumers without providing negative incentives to software companies and the technology sector. It further fails to recognize the national security elements of the cyber ecosystem. A national cyber insurance program with affordable, comprehensive coverage and potential federal backstop would alleviate the harm from arbitrarily deciding what constituents should suffer because of federal policy. Furthermore, proposed liability regimes and insurance requirements are likely more viable politically if combined with affordable insurance.

The amount—trillions of dollars—that the federal government has proven it can insure would serve as the primary benefit of a federal program.[484] The chance of a self-sustaining risk pool with affordable premiums and broad coverage would require levels of capitalization that may exceed the level that the private market can provide.

E. Counterpoint: Possible Negative Results of National Cyber Insurance

Effective cyber insurance and regulation would be extremely complex and, therefore, very costly.[485] A tradeoff between defense spending and recognition of the societal cost of cyber losses and the policies that contributed to them would need to occur to make a program effective. The cost may be prohibitive, and federal insurance programs have shown weakness in recouping government outlays.[486] The complexity of the regulation needed is further concerning. The FDIC served as an important tool to address banking problems, but it depended on the quality of the underlying regulation. The FDIC failed to prevent the losses of 2007–2008 because the underlying law and regulation had been gutted since the 1930s.[487] It was critical, however, to the response.[488] Federal insurance has shown an ability to address monumental risk, such as flood loss, but regulation in the cyber ecosystem would need to be nimble and responsive to constant change in technology and threats.[489] This would test a lumbering bureaucracy.

---

son, *supra* note 58, at 297–302 (information sharing); Trang, *supra* note 57, at 409–17 (mandatory insurance generally).

484. *See Insurance Programs*, *supra* note 442.

485. Eastman, *supra* note 2, at 532–33.

486. Gerrish, *supra* note 447, at 1833–40 (describing issues with recovering money paid to insurers under TRIA).

487. *See* Arthur E. Wilmarth Jr., *The Road to Repeal of the Glass-Steagall Act*, 17 WAKE FOREST J. BUS. & INTELL. PROP. L. 441, 541–48 (2017).

488. *See* DIV. INS. & RESEARCH, FDIC, CRISIS AND RESPONSE: AN FDIC HISTORY, 2008–2013 (2017).

489. Eastman, *supra* note 2, at 532–33; Johnson, *supra* note 58, at 277–78.

Another federal insurance backstop program, TRIP, arguably stunted the development of a private terrorism insurance market.[490] By nationalizing insurance away from state regulation and creating uniform policy standards, TRIP minimized transaction costs to the point that state-regulated private insurers could not compete and the private market failed to develop. The temporary program thus has been extended and private insurers continue to exclude terrorism coverage.[491] The very efficiency of nationalizing insurance and removing policy variation crushed the private market. Cyber insurance is in its infancy now like terrorism insurance was after 9/11. Adoption of a successful national cyber insurance policy would likely threaten the success of an adequate private market developing. A private market has the potential to be more reflexive and a better regulator in an ecosystem of rapid change than a government program.

The final and most important risk associated with a national insurance program is overall efficacy in addressing the risk. NFIP arguably has failed in this measure. FEMA has oversight of local governments with respect to floodplain development and risk mitigation, but critics argue it cannot compel enforcement well enough to address the risk.[492] The goal of NFIP to expend money on prevention to save in disaster relief expenditures arguably has failed, too.[493] Private insurance, with its current small market and limited adoption, is able to effectively regulate, but transitioning this model to a comprehensive national program obviously is not guaranteed.

VII. CONCLUSION

U.S. policy led to fantastic developments in telecommunications and the Internet. The very qualities that made these developments successful made them insecure. National security institutions, other public law institutions, and private law cannot provide security. Insurance has potential and has shown to be uniquely adept in regulating for cybersecurity. The private cyber insurance market, however, is too small compared to the risks, and the insurance lacks in coverage, is not widespread, is expensive, is difficult to model, and is hard to obtain. As small businesses become the target of choice for hackers, a national cyber insurance program has promise for improving public and private collaboration, improving risk pooling, providing affordable premiums, protecting private insurers from "Cybergeddon" losses, and improving regulation. Government intervention into a private market

490. Gerrish, *supra* note 447, at 1833–48.
491. *Id.* at 1829–30, 1848–49.
492. Christine M. McMillan, Comment, *Federal Flood Insurance Policy: Making Matters Worse*, 44 HOUS. L. REV. 471, 501–02 (2007).
493. Oliver A. Houck, *Rising Water: The National Flood Insurance Program and Louisiana*, 60 TUL. L. REV. 61, 128–33 (1985).

is not to be taken lightly, but because of the overwhelming risk and failure of existing institutions, a national cyber insurance program merits further discussion.