Journal of Business & Technology Law

Volume 13 | Issue 2 Article 5

Cyber Insurance, Data Security, and Blockchain in the Wake of the Equifax Breach

Kevin DiGrazia

KEVIN DIGRAZIA*

Cyber Insurance, Data Security, and Blockchain in the Wake of the Equifax Breach

I. INTRODUCTION

We are now in an era where we rely on interconnected smart devices in almost every aspect of our lives.[1] With the added convenience of being able to access your banking information via your smartphone or asking Alexa to order more paper towels, we are exposing our personal data to a host of new cybersecurity threats.[2] The digital revolution has enabled us be a part of a highly interconnected world where we are constantly connected to the Internet of Things ("IoT")[3] including things such as smart TVs, thermostats, cellphones, cars and even industrial control systems ("ICS").[4] By connecting all of these devices and digitalizing troves of sensitive or proprietary data, it opens the door for bad actors to perpetrate malicious attacks.[5] The malicious cyber-attacks can come in various forms depending on the intended target and the motivation of the hacker, which is why it is no wonder cyber risks are one of the biggest threats of our age.[6]

* Kevin DiGrazia is a student at The University of Maryland Francis King Carey School of Law, a CPA, and a Senior Associate at PricewaterhouseCoopers. The opinions stated in this paper are those of the author and should not be attributed either to PwC or to its clients.

1. *See* Lee Rainie & Janna Anderson, *The Internet of Things Connectivity Binge: What Are the Implications?*, PEW RES. CTR.: INTERNET & TECH. (June 6, 2017), http://www.pewinternet.org/2017/06/06/the-internet-of-things-connectivity-binge-what-are-the-implications/.

2. *Id.*

3. 1 MEGAN COSTELLO, DATA SECURITY AND PRIVACY LAW § 5:83, WestLaw (database updated June 2017) (defining the IoT as "the ever-expanding network of internet-enabled appliances to an already existing infrastructure of computers and mobile devices").

4. ALLIANZ GLOBAL CORP. & SPECIALTY, A GUIDE TO CYBER RISK MANAGING THE IMPACT OF INCREASING INTERCONNECTIVITY 27 (Sept. 2015), https://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRisk Guide.pdf.

5. *See* SYMANTEC, 2016 INTERNET SECURITY THREAT REPORT (Paul Wood et al. eds., 2016), https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf (reporting that smart home devices such as TVs and door locks can be hacked similar to industrial control systems and manufacturing plants).

6. *Insurance 2020 & beyond: Reaping the dividends of cyber resilience,* PWC (2015), https://www.pwc.com/gx/en/industries/financial-services/insurance/publications/insurance-2020-cyber.html.

With recent high profile cyberattacks like WannaCry and the Equifax breach, consumers, regulators and companies should be on heightened alert to our country's biggest vulnerabilities. In the case of the WannaCry attack, hackers were able to infect more than 300,000 computers in over 150 countries around the world in a matter of several days, including many hospitals, which were unable to access patients' medical records.[7] In the Equifax breach, hackers were able to access "people's names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers."[8] These two cybersecurity incidents help illustrate the potential catastrophic impact that a hacker can have on millions of people around the world.

To address these risks, companies have begun purchasing cyber insurance as both a standalone policy and as an endorsement to their current policies.[9] Cyber insurance policies are usually bucketed into two general categories: first-party coverage; and third-party defense and liability coverage.[10] As discussed below, first-party coverage may cover the costs of data-breach notifications, credit monitoring, and lost profits.[11] Third-party liability coverage provides coverage for regulatory fines, settlements and judgments against the insured amongst many other coverage options.[12]

This note will begin by evaluating how the IoT has evolved and the new risks connectivity brings to both businesses and individuals.[13] Part III of this note looks at how insurance companies have been drafting their traditional insurance policies to exclude cyber related liability and the risks businesses and consumers face if they rely on their traditional insurance policies for coverage for a cyber-related incident.[14] Part III also provides a brief overview of the potential benefits of standalone cyber insurance policies as a source of protection in the case of a cyber-attack, but notes that purchasers of the policy must understand what coverage they are buying because of the lack of standardized cyber insurance policies.[15] Next, this note will examine the silent cyber risk that potentially implicates multiple lines of insurance in the event of a large-scale cyber-attack and its impact on the re-insurance markets.[16] It will also evaluate the use of blockchain technology as an alternative to Social Security numbers

7. Tyrone R. Childress et al., *No More Tears: Insurance Coverage For The "WannaCry" Ransomware Attack,* 22 CYBERSPACE LAW. *1–2 (July 2017).

8. Sheena Gressin, *The Equifax Data Breach: What to Do*, FED. TRADE COMM'N: CONSUMER INFO. (Sept. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.

9. Michael Rossi, *Cyber Liability Issues for Large Companies*, IRMI (Nov. 2003), https://www.irmi.com/articles/expert-commentary/cyber-liability-insurance-market-update.

10. *See infra* Section III.

11. *See infra* Section III.

12. *See infra* Section III.

13. *See infra* Section II.

14. *See infra* Section III.

15. *See infra* Part III.

16. *See infra* Part IV.

as a form of identification in an age where bad actors are easily able to access a consumer's personally identifiable information ("PII").[17] Finally, this note will address the current data privacy laws, their effectiveness in protecting consumers, and evaluates the potential of model data protection and network security laws.[18]

II. IMPACT OF THE IOT ON THE CYBER INSURANCE MARKETS

A. Current Connectivity of Devices

The IoT has somewhat of an amorphous definition depending on which scholar or government agency is providing the definition. One definition put forth in a government report describes the IoT as "an expansion of the global infrastructure through existing and evolving interoperable information and communication technologies that incorporates the interconnection of physical and virtual systems to enable new and automated capabilities."[19] A more reader friendly version of the definition from the same report describes the IoT as:

> *A decentralized network of objects, applications, and services that can sense, log, interpret, communicate, process, and act on a variety of information or control devices in the physical world. However, the IoT differs from previous technological advances because it has surpassed the confines of the computer networks and is connecting directly to the physical world.*[20]

Although most people have heard of the IoT, most people do not realize how it affects them. On the consumer side, some cars, thermostats, baby monitors, refrigerators, and anything that is able to connect to the internet is considered a smart device. These devices are a part of the IoT and can be a gateway for hackers to enter the home. In a 2012 incident, hackers accessed the security cameras sold by TRENDnet, accessed the video feeds without passwords, and watched unsuspecting victims go about their daily routines inside their homes.[21] The Federal Trade Commission ("FTC") brought a case against TRENDnet alleging that TRENDnet

17. *See infra* Part V.

18. *See infra* Part VI.

19. The President's National Security Telecommunications Advisory Committee, NSTAC Report to the President on the Internet of Things, ES-1, November 19, 2014, http://www.dhs.gov/sites/default/files/publications/NSTAC/'20Report%20to%20the%20President%20on%20the%20Internet%20ofo20Things%2ONov%202014%20%28update%20%20%20.pdf (citing the Industrial Internet Scoping Report issued by NSTAC in February 2014 summarizing the work of a subcommittee).

20. *Id.* at 1.

21. Kim Zetter, *Flaw in Home Security Cameras Exposes Live Feeds to Hackers*, WIRED (Feb. 7, 2012, 2:34 PM), https://www.wired.com/2012/02/home-cameras-exposed/.

represented that its products were secure, which was false and misleading, and that it failed to take reasonable steps to prevent unauthorized access to the video feeds.[22] In 2014, the FTC issued a final order, which was only an insignificant punishment for TRENDnet, prohibiting them from misrepresenting the security of their cameras, and requiring them to provide free technical support to their customers for two years.[23]

Cyber-attacks on ICS are of paramount concern to our national security and viewed as one of the largest risks.[24] As operational control technology becomes increasingly connected to the internet, it opens the door for bad actors to control physical processes.[25] ICS are generally defined as the "different types of control systems and associated instrumentation, which include the devices, systems, networks, and controls used to operate and/or automate industrial processes."[26] They can also be found in almost every field imaginable, including manufacturing, food and beverage, HVAC management, brewing, and even pharmaceuticals.[27] Hackers have proven they are able to access ICS as demonstrated in the 2014 incident where a spear phishing[28] exploit enabled hackers to take control of the ICS of a German steel mill and caused massive damage by disabling the regulator that shutoff the furnace.[29] In another example, hackers were able to gain access to the control system of a dam in upstate New York through a cell modem. Luckily, the water gates were not connected to the system at the time because they were down for maintenance.[30]

22. In the Matter of Trendnet, Inc., A Corp., No. 122-3090, 2014 WL 556262, at 4–5 (F.T.C. Jan. 16, 2014) (stating that Section 5(a) of the Federal Trade Commission Act, codified at 15 U.S.C. §45(a) gives the agency the authority to regulate security standards).

23. *FTC Approves Final Order Settling Charges Against TRENDnet, Inc.,* FED. TRADE COMM'N (Feb. 7, 2017), https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc.

24. *The Role of Cyber Insurance in Risk Management: Hearing Before the Subcomm. on Cybersecurity, Infrastructure Protection, and Security of the H. Comm. on Homeland Security*, 114th Cong. 9 (2016) (statement of Cong. John Ratcliffe, Chairman, S. Comm. on Cybersecurity, Infrastructure Protection, and Security Tech.).

25. *The Role of Cyber Insurance in Risk Management: Hearing Before the Subcomm. on Cybersecurity, Infrastructure Protection, and Security of the H. Comm. on Homeland Security*, 114th Cong. 12 (2016) (statement of Matthew McCabe, Senior Vice President, Network Security and Data Privacy, Marsh FINRPO).

26. *See generally Industrial Control System*, TREND MICRO, https://www.trendmicro.com/vinfo/us/security/definition/industrial-control-system (last visited Jan. 11, 2018) (providing a description of ICSs).

27. LUCY L. THOMSON, CYBER PHYSICAL RISKS (2016).

28. "Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization or business. Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user's computer." *What is Spear Phishing? – Definition,* KASPERSKY LAB, https://usa.kaspersky.com/resource-center/definitions/spear-phishing (last visited Feb. 12, 2018).

29. *Hack Attack Causes 'Massive Damage' at Steel Works,* BBC (Dec. 22, 2014), http://www.bbc.com/news/technology-30575104.

30. *The Role of Cyber Insurance in Risk Management: Hearing Before the Subcomm. on Cybersecurity, Infrastructure Protection, and Security of the H. Comm. on Homeland Security*, 114th Cong. 12 (2016) (statement of Matthew McCabe, Senior Vice President, Network Security and Data Privacy, Marsh FINRPO).

B. Overview of Insurance

Insurance helps individuals and companies address the inevitable risks they face on a daily basis. Insurance, at its most basic level, is an arrangement for transferring and distributing risks from one party (usually the insured) to another party (the insurer).[31] Insurance companies spread risk among a large pool of policyholders by collecting premiums from policyholders. In exchange, they cover large risks of loss identified by a contract known as an insurance policy.[32] The insurability of a specific risk is determined by two key factors: the frequency of the risk and the severity of the risk.[33] Insurance policies are usually designed to cover low-frequency, high-severity losses, such as a house fire, or high-frequency, low-severity incidents, such as car crashes.[34] However, there are some areas — those that are high-frequency, high-severity risks and those that are unpredictable risks, such as terrorist attacks — that pose significant challenges to the insurance industry's attempt to provide affordable coverage to cover those risks.[35]

Businesses and individuals have historically looked to insurance policies to transfer or mitigate the future risk of loss.[36] However, insurance companies have recognized the massive potential liability associated with policies that do not exclude coverage for cyber-related incidents and have begun adjusting their standard policies to exclude cyber-related coverage.[37] Insurance companies realize the cyber insurance market is poised for explosive growth, with projections for premiums reaching over $20 billion by 2025.[38] Because cyber insurance is the future of the industry, insurance companies have not completely pulled out of the market, but are taking a much more calculated approach to the market.[39] Insurance companies have achieved this by carefully designing endorsements and exclusions for traditional policy lines, in addition to creating standalone cyber insurance policies with very specific definitions

31. PRACTICAL LAW COMMERCIAL TRANSACTIONS, INSURANCE BASICS FOR IN-HOUSE COUNSEL. *See also* AM. INS. ASS'N, PROPERTY-CASUALTY INSURANCE BASICS 1, www.aiadc.org/AIAdotNET/docHandler. aspx?DocID =319988.

32. *Id.*

33. *Id.*

34. *Id.*

35. *Id.*

36. STEVEN PLITT ET AL., COUCH ON INSURANCE § 1:9 (3d ed. rev. 2017).

37. *See* Matt Dunning, *Insurers Prepare for Implementation of New Cyber Liability Exclusions*, BUS. INS. (Jan. 1, 2014, 12:00 AM), http://www.businessinsurance.com/article/20140119/NEWS04/301199978 (noting that the Insurance Services Office (ISO) recently revised its commercial liability forms to exclude coverage for many forms of cyber related damages).

38. ALLIANZ GLOBAL CORP. & SPECIALTY, A GUIDE TO CYBER RISK MANAGING THE IMPACT OF INCREASING INTERCONNECTIVITY 24 (Sept. 2015), https://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRisk Guide.pdf.

39. PWC, INSURANCE 2020 & BEYOND: REAPING THE DIVIDENDS OF CYBER RESILIENCE 4 (2015), https://www.pwc.com/gx/en/industries/financial-services/insurance/publications/insurance-2020-cyber.html.

for cyber coverages and exclusions, which include separate limits for different types of cyber exposure.[40]

III. CYBER INSURANCE OVERVIEW

A. Policy Basics

Cyber insurance policies are a relatively new insurance product, especially as a standalone policy.[41] Based on the type of policy purchased, cyber insurance is intended to protect the insured against the costs associated with hacking, cyber-attacks, and data breaches.[42] Cyber policies generally cover first-party losses because of a cyber-event relating to responding to a breach, such as legal and forensic costs, notification costs, crisis communications, reputational damage mitigation, lost profits and operating costs, and cyber extortion.[43] Additionally, many policies cover third-party liability for failing to protect data, credit card liability, defense costs for regulatory actions and fines, and media liability.[44]

The cyber insurance market is a virtual wild west of insurance policies with no standardization of coverage or policy language, which makes it almost impossible to compare policy pricing and coverage.[45] The value of cyber insurance policies is widely debated. Some commentators believe that the amount firms have to pay in premiums and deductibles for the insurance coverage would be comparable to the amount the firm would have to pay out of pocket to cover the costs of the breach.[46] To make matters worse, the firm may have been able to prevent the cyber-attack had they used the money spent on the premiums and deductible to secure their networks.[47]

40. *Id.* at 10.

41. Brian D. Brown, *The Ever-Evolving Nature of Cyber Coverage*, INS. J. (Sept. 22, 2014), https://www.insurancejournal.com/magazines/features/2014/09/22/340633.htm (noting that the fist cyber insurance policy was written in 1997).

42. Sean Harrington, *Cyber Insurance: What Minnesota Lawyers Need to Know*, BENCH & B. MINN. (Nov. 6, 2015), http://mnbenchbar.com/2015/11/cyber-insurance/.

43. *See* AIG, CYBEREDGE®: END-TO-END CYBER RISK MANAGEMENT SOLUTIONS (2015), http://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/aig-cyberedge0418finalsingle-brochure.pdf (describing the coverage provided by their "End-to-End Cyber Risk Management Solutions").

44. *See* CHUBB, CYBER ENTERPRISE RISK MANAGEMENT (2017), https://www2.chubb.com/us-en/_assets/doc/17010185-cyber-erm-12.17.pdf (describing the coverage available with their Cyber ERM).

45. See SASHA ROMANOSKY ET AL., CONTENT ANALYSIS OF CYBER INSURANCE POLICIES: HOW DO CARRIERS WRITE POLICIES AND PRICE CYBER RISK? 35 (2017), http://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/06/WEIS_2017_paper_28.pdf, for an in-depth analysis of the variations between the various cyber insurance policies.

46. John Pescatore, *BitPay Sues Insurance Company After Cyberattack Claim is Rejected,* SANS NEWSBITES, Sept. 29, 2015, https://www.sans.org/newsletters/newsbites/xvii/76 (discussing reasons why cyber insurance policies may not be the best option for some firms).

47. *Id.*

Others believe that cyber insurance may be a good investment for small to medium-sized firms that would be severely affected by a cyber-attack but do not have the funds to have IT risk audits and the backend infrastructure to detect or prevent a cyber-intrusion.[48] In fact, small to medium-sized business are a prime target for hackers because they do not have the expertise or the funds that a large company has to defend their network.[49] As a result, over 50% of small and midsize businesses ("SMB's") experienced a breach in 2016.[50] Congress has acknowledged the threat of cyber-attacks on small businesses, noting that "over 60 percent of those [SMBs] attacked go out of business."[51] To address this threat, Congress has introduced legislation, Making Available Information Now to Strengthen Trust and Resilience and Enhance Enterprise Technology ("MAIN STREET") Cybersecurity Act, which would provide small businesses with resources to protect themselves from cyber-attacks.[52] Cyber insurance may also be a valuable investment for large companies, especially those with vast amounts of consumer data such as retailers, cloud storage providers, companies in the healthcare field, financial institutions, and email providers such as Yahoo.[53]

According to a report by Allianz Global Corporate and Specialty, cybercrimes cost the global economy "approximately $445 billion a year" and although data breaches have been the focus of cyber-attacks in the past, Allianz sees future threats coming from "intellectual property theft, cyber extortion and the impact of business interruption (BI) following a cyber-attack or from operational or technical failure."[54]

48. *See* PWC, MANAGING CYBER RISKS IN AN INTERCONNECTED WORLD (Sept. 30, 2014), http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (noting that larger companies are heavily investing time and money in safeguarding their networks and assets while small companies often do not have the funds or think they are too insignificant to attract cyber-attacks). Small and medium sized companies can protect themselves through "managed security services" or purchasing cyber insurance. *Id.*

49. SYMANTEC, 2016 INTERNET SECURITY THREAT REPORT (Paul Wood et al, 2016), https://www.symantec.com/security-center/threat-report (finding that small and medium sized businesses with 1-2,500 employees made up 65% of the spear-phishing attacks in 2015 while 35% of the attacks were aimed at companies with greater than 2,500 employees).

50. PONEMON INST., THE 2016 STATE OF SMB CYBERSECURITY IN SMALL & MEDIUM-SIZED BUSINESSES (June 2016), https://signup.keepersecurity.com/state-of-smb-cybersecurity-report/.

51. *National Cybersecurity Institute at Excelsior College*: *Hearing Before the H. Comm. On Small Business, Big Threat: Protecting Small Businesses from Cyber Attacks,* 114th Cong. 61 (2015) (statement of Dr. Jane LeClair, Chief Operating Officer, National Cybersecurity Institute at Excelsior College).

52. *Thune Introduces Legislation to Improve Cybersecurity Resources for Small Businesses,* JOHN THUNE FOR U.S. SENATOR FOR SOUTH DAKOTA (Mar. 29, 2017), https://www.thune.senate.gov/public/index.cfm/2017/3/thune-introduces-legislation-to-improve-cybersecurity-resources-for-small-businesses.

53. Todd Haselton, *Yahoo Just Said Every Single Account was Affected by 2013 Attack — 3 Billion in All*, CNBC (Oct.4, 2017, 7:50 AM), https://www.cnbc.com/2017/10/03/yahoo-every-single-account-3-billion-people-affected-in-2013-attack.html.

54. *Businesses Must Prepare for New Generation of Cyber Risks,* ALLIANZ (Sept. 9, 2015), https://www.allianz.com/en/press/news/studies/150909_businesses-must-prepare-for-cyber-risks. html/.

Insurance companies are trying to underwrite policies to meet the market demand, which is growing at a double-digit rate with projections reaching the $20 billion or more mark for cyber related insurance policies.[55]

B. Coverage Gap Issues

Firms purchasing cyber insurance should understand what their current insurance policies will cover, and what duplicate coverage and peril gaps exist. With the surge in automation of the IoT and the Industrial Internet of Things ("IIOT"), hackers will increasingly be able to cause physical damage to machinery and other equipment.[56] This poses a challenge for an insured because in most cases, a standard property or Commercial General Liability ("CGL") policy will not cover damages resulting from a cyber-attack.[57]

One of the most challenging aspects of understanding cyber insurance policies is trying to determine how the untested policy language will affect coverage for specific perils in various industries.[58] For example, Massachusetts Bay Insurance Co. denied coverage in 2015 when the Bitcoin exchange CFO was phished and divulged his email credentials to the hacker, which enabled them to fraudulently transfer over $1.85 million worth of Bitcoins.[59] According to Bitpay, the policy offers coverage for "loss of or damage to 'money,' . . . resulting directly from the use of any computer to fraudulently cause a transfer of that property" and the policy was specifically amended to include Bitcoins in the definition of "money" in the policy.[60]

C. How Insurance Companies Respond to Risks

The language in most current CGL policies is based off of the standard policies drafted by the Insurance Service Office ("ISO"), Inc.[61] The current CGL policies have three areas of coverage under Section I, Coverage A – which addresses bodily injury and property liability damage, Coverage B which addresses personal and advertising

55. *Cyber Risk 2025 - The Next 10 Years. . .*, ALLIANZ (2015), http://www.agcs.allianz.com/insights /expert-risk-articles/cyber-risk-2025/.

56. *See generally* LUCY L. THOMSON, CYBER PHYSICAL RISKS (2016) (detailing past cyber-attacks on physical infrastructure connected to the IoT and the damage the hackers were able to inflict).

57. *See infra* Sections III.C & III.D.

58. *See infra* Sections III.C & III.D.

59. Thomas Parry, *Bitcoin Processor Sues Insurer for Phishing Attack Coverage*, 11 WESTLAW J. INS. BAD FAITH, *1 (Oct. 14, 2015).

60. *Id.*

61. *See* ISO, VERISK INS. SOL., http://www.verisk.com/insurance/about/faq.html (last visited Nov. 23, 2017) ("ISO began life in 1971 as Insurance Services Office. While we still serve the property/casualty insurance marketplace, our business has expanded greatly. Therefore, in recent years, we have not used the old name in most of our communications with customers and others.").

injuries and Coverage C which addresses medical payments.[62] The CGL form has been in effect since the 1940s and purchased by the majority of businesses to cover a wide range of risks, but it was not designed to protect the insured from *all* risks.[63] Prior to the 1940s, the liability policies, which were the predecessors to the CGL policies, were written to cover a specific hazard.[64]

In the 1970s and 1980s, insurance companies had to address the issues of asbestos and toxic dumping.[65] In asbestos cases, the coverage issue stemmed from identifying when the insurance policies were triggered and when they began to provide coverage.[66] A common example of this is when a factory worker was exposed to asbestos for twenty years but did not manifest symptoms until ten years after she stopped working at the factory. Over those thirty years, the manufacturer could have had five or six different insurance policies in place that could all potentially share in the liability years after the policy term had ended.[67] After decades of litigation, the majority of courts have rejected the manifestation theory of liability and adopted the position that the policies in effect from the first exposure through discovery are triggered, requiring all insurers that had policies during that period to cover the losses.[68] This approach also implicated all of the policy limits in place because the insurance company could be liable up to the policy's cap for each year the policy was in place creating massive liabilities for the insurance companies many years after the policy period ended.[69] As a result of the asbestos litigation, the CGL policy was updated in 1986 to exclude asbestos related liability.[70]

In the early 1970s, insurance companies began to realize that there was a significant increase in pollution-related claims and attempted to limit their exposure to this liability by updating the standard CGL policy in 1973 to exclude coverage for damage caused by pollution.[71] To address rampant unacceptable hazardous waste

62. INS. SERV. OFFICE, INC., COMMERCIAL GENERAL LIABILITY COVERAGE FORM CG 00 01 04 13 (2012).

63. 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, 270 (2012).

64. AMERICAN BAR ASS'N, THE REFERENCE HANDBOOK ON THE COMPREHENSIVE GENERAL LIABILITY POLICY: INSURANCE COVERAGE LITIGATION COMMITTEE 1–2 (2010).

65. *Id.* at 158–62.

66. *Id.* at 109–25 (discussing the various types of triggers of CGL policies and how they affected the insurance companies' requirements to payout claims).

67. *Id.*; JEFFREY W. STEMPEL & ERIK S. KNUTSEN, STEMPEL AND KNUTSEN ON INSURANCE COVERAGE 521–22 (4th ed. 2016).

68. Jeffrey W. Stempel, *Assessing the Coverage Carnage: Asbestos Liability and Insurance After Three Decades of Dispute*, 12 CONN. INS. L.J. 349, 353 (2006).

69. *Id.* at 376.

70. *Id.*

71. AMERICAN BAR ASS'N, THE REFERENCE HANDBOOK ON THE COMPREHENSIVE GENERAL LIABILITY POLICY: COVERAGE PROVISIONS, EXCLUSIONS, AND OTHER LITIGATION ISSUES 209 (Peter J. Neeson eds., 1995) ("The initial pollution exclusion clause introduced in the 1973 revision to the CGL standard-form policy has become known as the 'sudden and accidental' pollution exclusion for it disclaims coverage 'for bodily injury or property damage

practices, Congress passed the Comprehensive Environmental Response, Compensation and Liability Act of 1980 ("CERCLA"), which imposed retroactive, joint, and several liability for all parties involved with site hazardous waste dumping.[72] The Environmental Protection Agency ("EPA") has brought enforcement actions against many companies, such as fines and remediation costs associated with the companies' improper disposal or handling of hazardous substances.[73] As these claims were litigated, insurance companies realized that courts were interpreting the "sudden and accidental" pollution exclusion differently than the drafters had intended.[74] To address the increased exposure and mounting claims, the CGL form was modified again in 1986 to remove the "sudden and accidental" pollution exclusion and replace it with an "absolute pollution exclusion" which attempts to expressly exclude almost every discharge of a pollutant.[75]

As will be discussed below in the case of cyber insurance policies, when the insurance industry faces a large financial risk such as asbestos litigation or pollution related claims, the industry usually creates an exclusion for those specific risks or narrowly tailors their exposure to those risks.[76] Although insurance companies try to limit or eliminate their exposure to risks such as earthquakes and flooding, sometimes the government has to step in to either back a program or establish a new insurance program. For example, the National Flood Insurance Program ("NFIP")[77] was established to provide affordable flood insurance to the public because of insurance providers pricing flood insurance policies at an unaffordable rate.[78]

Although cyber related insurance coverage is a relatively new idea for insurance, the courts and the insurance companies have been litigating the basic elements of the policies for at least the past several decades.[79] As a result of the litigation, the ISO determined it needed to modify the standard CGL form multiple times throughout the years to limit the exposure it created for cyber related insurance

arising out of the discharge, dispersal, release or escape' of pollutants except in circumstances in which the loss results from a 'discharge' that is 'sudden and accidental.'").

72. 42 U.S.C. §§ 9601-9675 (1982 & Supp. IV 1986).

73. Stephen Mountainspring, *Insurance Coverage of CERCLA Response Costs: The Limits of Damages in Comprehensive General Liability Policies*, 16 ECOLOGY L.Q. 755, 755 (1989).

74. AMERICAN BAR ASS'N, THE REFERENCE HANDBOOK ON THE COMPREHENSIVE GENERAL LIABILITY POLICY: COVERAGE PROVISIONS, EXCLUSIONS, AND OTHER LITIGATION ISSUES 209-10 (Peter J. Neeson eds., 1995).

75. *Id.* ("…the absolute pollution exclusion is drafted so as to 'absolutely' preclude coverage for pollution claims without regard to causation issues or fault of the insured.").

76. *See infra* Section III.D.

77. 42 U.S.C. § 4001.

78. R. Jason Richards, *The National Flood Insurance Program: A "Flood" of Controversy*, 82 FLA. B.J. 8, 9-10 (2008) (describing the state of the flood insurance market in 1968 which required the government to create NFIP).

79. *See infra* Section III.D.

losses similar to the changes made to the language for other possible catastrophic exposures in the past.[80]

D. GRAY AREA IN COVERAGE

Prior to the paradigm shift towards the complete digitization of companies, the CGL policy was able to adequately provide an insured coverage if there was a physical loss of property because at that time, all of the company's records were physical.[81] As more and more information became stored digitally, courts had to decide whether the loss of use of data would be a physical loss under the CGL policy.[82] In 2000, the court in *American Guarantee & Liability Insurance Company v. Ingram Micro., Inc.*, found that "'physical damage' is not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality" where a power outage took down the insured's mainframe computer and was required to reprogram the lost data.[83] However, the court in *Ward General Ins. v. Employers Fire Ins. Co.,* reached a different conclusion by finding that information, by nature, is merely a series of zeros and ones that can be manipulated without damaging the medium the data was stored on.[84] The court determined that since there was not any physical damage to the medium the data was stored on, the loss of data was not covered under any of the plaintiff's policies since the plaintiff did not incur a "physical loss."[85]

In light of the uncertainty of how courts would interpret the definition of a physical loss, the ISO decided to modify their standard Commercial General Liability Coverage Form.[86] The new language in the form clarified the definition of property damage to explicitly exclude electronic data.[87] Shortly after the update to the form in

80. *See infra* Section III.D.

81. *See infra* Section III.D.

82. *See infra* Section III.D.

83. Am. Guarantee & Liab. Ins. Co. v. Ingram Micro, Inc. No. 99–185 TUC ACM, slip op. at 2 (D. Ariz. Apr. 18, 2000).

84. *See* Ward Gen. Ins. Servs., Inc. v. Employers Fire Ins. Co., 114 Cal. App. 4th 548, 556 (2003), as modified on denial of reh'g (Jan. 7, 2004) (finding that information and data that was lost when an Oracle database crashed was not covered under the insured's policies because data does not have material existence).

85. *Id.* at 557.

86. 2 KEN BROWNLEE & ROBERT PERSONS, EXCESS LIABILITY RIGHTS & DUTIES OF COMMERCIAL RISK INSUREDS & INSURER § 14:2, WesLlaw (database updated May 2017) (noting that I.S.O. CG 00 01 10 01 (2000) defines "property damage" differently than earlier forms).

87. *See* INS. SERV. OFFICE, INC., COMMERCIAL GENERAL LIABILITY FORM CG 00 01 10 01 (2000) (defining property damage under V Definitions section 17 as "For the purposes of this insurance, electronic data is not tangible property. As used in this definition, electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, heard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment).

2001, the ISO made another significant update to their insurance policy in 2004 in section P (under the exclusions), which tried to exclude the insurer's liability for electronic data.[88]

In 2013, the ISO modified the standard CGL for Section A to clarify that under the exclusion P, "Electronic Data," the CGL would provide coverage for a "bodily injury" as a result of the loss of use of data, corruption of the data or the inability to access the data.[89] However, in the same update, the ISO made several updates to Section B of the policy to limit liability related to electronic and cyber publications[90] similar to the mandatory endorsement CG 24 13 04 13.[91] Although many of these changes were aimed at tightening cyber related exposure to third-party claims, the ISO's actions further reinforce the notion that barring specific endorsements or an independent insurance policy, an insured is not likely to find cyber related coverage under their CGL policies.

To further limit exposure, the ISO issued a series of endorsements, which essentially eliminated an insured's coverage for cyber related events.[92] The endorsement CG 21 06 05 14 specifically excludes coverage under Coverage A for damages relating to intellectual property and third loss or disclosure of third party information.[93] This shift in coverage under the CGL is logical because when the previous versions of the CGL were drafted, hacking and the costs associated with a data breach and physical damage caused by cyber related activities was not as prevalent and standalone cyber insurance policies were not widely available on the market.[94] It seems to be the intention of the ISO and the insurance companies to sell

88. *See* INS. SERV. OFFICE, INC., COMMERCIAL GENERAL LIABILITY FORM CG 00 01 12 04 (2003) (defining Electronic Data exclusion as "Damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data. As used in this exclusion, electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.").

89. INS. SERV. OFFICE, INC., COMMERCIAL GENERAL LIABILITY COVERAGE FORM CG 00 01 04 13 § I.A. (2012).

90. *Id.* at § I.B.

91. INS. SERV, OFFICE, INC., AMENDMENT OF PERSONAL AND ADVERTISING INJURY DEFINITION CG 24 13 04 13 (2012) (this endorsement modified the "personal and advertising injury" definition to remove coverage for "oral or written publication, in any manner, of material that violates a person's right of privacy.").

92. *ISO Comments on CGL Endorsements for Data Breach Liability Exclusions*, INS. J. (July 18, 2014), https://www.insurancejournal.com/news/east/2014/07/18/332655.htm.

93. *See* INS. SERV. OFFICES, INC., EXCLUSION—ACCESS OR DISCLOSURE OF CONFIDENTIAL OR PERSONAL INFORMATION AND DATA-RELATED LIABILITY—WITH LIMITED BODILY INJURY EXCEPTION CG 21 06 05 14 (2013) (establishing that "(1) any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information; or (2) The loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.").

94. *ISO Comments on CGL Endorsements for Data Breach Liability Exclusions*, INS. J. (July 18, 2014), http://www.insurancejournal.com/news/east/2014/07/18/332655.htm.

separate standalone cyber insurance products that can better address an insured's need for cyber related insurance.[95] The ISO recently produced an insurance policy, *Information Security Protection Policy,* (EC 00 10 01 14), aimed at addressing eight separate insuring categories: (1) security breach expense; (2) security breach liability; (3) replacement or restoration of electronic data; (4) business income and extra expense; (5) extortion threats; (6) public relations expense; (7) website publishing liability; and (8) programming errors and omissions liability.[96] Although the ISO has promulgated this new cyber insurance policy suite, it is unclear whether any insurance companies are utilizing the forms and if so, to what extent.

IV. INSURANCE AND REINSURANCE MARKETS MAY NOT BE ABLE TO ABSORB LOSSES FROM A LARGE SCALE CYBER-ATTACK

A. A Cyber-Attack Could Cost Over $70 Billion in Insurance Claims

According to the 2015 Lloyd's Emerging Risk Report, if there was a cyber-attack on the U.S. power grid, it could potentially cost the U.S. economy more than $1 trillion dollars and cost insurance companies over $70 billion.[97] Under one scenario, a piece of malware is introduced into the electric grid and overloads the system, taking it down and resulting in a loss of power for the northeast between twenty-four hours in some spots and weeks in others.[98] The scenario illustrates the point that a cyber-attack can implicate multiple lines of insurance in a very large geographic region.[99] For example, companies unable to function as a result of the power outage could put in claims for property loss of perishable items that went bad, lost profits under their business interruption policies, and any collateral damage such as fire or vandalism that occurred during the power outage.[100]

While the scenario in the Lloyd's report demonstrates how quickly a single cyber-attack can inflict billions of dollars in damage, the scenario fails to fully capture the amount of cyber risk businesses could face.[101] The real risk addressed later in the report is that the cyber risk itself is not constrained by physical boundaries and can easily be scaled and orchestrated with a couple lines of malicious code.[102] However,

95. *Id.*

96. VERISK INS. SOL., ISO'S CYBER INSURANCE PROGRAM 1 (2016), http://www.verisk.com/ downloads/iso-cyber-insurance-program.pdf.

97. LLOYDS, EMERGING RISK REPORT – 2015: SOCIETY & SECURITY: BUSINESS BLACKOUT 4 (2015), https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2015/business-blackout/business-blackout20150708.pdf [hereinafter LLOYDS, SOCIETY & SECURITY].

98. *Id.*

99. *Id.*

100. *Id.*

101. *Id.*

102. LLOYDS, SOCIETY & SECURITY, *supra* note 97**Error! Bookmark not defined.**, at 25.

the report tries to down play the risk too much when it claims that there are many barriers that impede bad cyber actors such as fear of retribution and the resources needed to orchestrate the attack.[103]

B. Banks Need to Invest in Cyber Security Guards

Bank and cyber-currency exchange platforms are prime targets for cyber bank robbers.[104] According to Kaspersky Lab, it has direct knowledge of over $300 million in cyber thefts but believes the actual amount could be triple that amount (over $1 billion) just in 2015.[105] In another attack in 2016, over $81 million dollars were siphoned from the Federal Reserve Bank of New York.[106] With the rise of digital currencies such as Bitcoin and Ethereum, hackers are raiding Bitcoin exchanges and stealing hundreds of millions of dollars' worth of the digital currencies.[107] Meanwhile, bank robbers who went in-person to bank locations and took physical money were only able to haul in about $9.5 million in 2009 and around $38 million in 2011 from over 5,000 robberies.[108]

C. Basic Elements of Insurance Risk Diversification

Based on the nature of cyber events, an exploited vulnerability could have a massive cascading effect causing trillions in insured losses.[109] This poses a significant challenge to insurance companies attempting to underwrite cyber insurance policies

103. *Id.*

104. LLOYDS, EMERGING RISK REPORT – 2015: BITCOIN: RISK FACTORS FOR INSURANCE (2015), https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2015/bitcoin—final.pdf.

105. David E. Sanger & Nicole Perlroth, *Bank Hackers Steal Millions via Malware,* N.Y. TIMES (Feb. 14, 2015), https://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html.

106. Michael Corkery, *Hackers' $81 Million Sneak Attack on World Banking*, N.Y. TIMES (Apr. 30, 2016), https://www.nytimes.com/2016/05/01/business/dealbook/hackers-81-million-sneak-attack-on-world-banking.html.

107. Luke Graham, *$32 Million Worth of Digital Currency Ether Stolen by Hackers*, CNBC (July 20, 2017, 7:41 AM), https://www.cnbc.com/2017/07/20/32-million-worth-of-digital-currency-ether-stolen -by-hackers.html; Bloomberg, *Ethereum Bandits Stole $225 Million This Year*, FORTUNE (Aug. 28, 2017), http://fortune.com/2017/08/28/ethereum-cryptocurrency-stolen-bitcoin/.

108. Brian Krebs, *Cyber Crooks Leave Traditional Bank Robbers in the Dust*, KREBS ON SECURITY (Mar. 9, 2010), https://krebsonsecurity.com/2010/03/cyber-crooks-leave-bank-robbers-in-the-dust/; *Bank Crime Statistics 2011*, FBI (Apr. 24, 2012), https://www.fbi.gov/stats-services/publications/bank-crime-statistics-2011/bank-crime-statistics-2011.

109. LLOYDS, SOCIETY & SECURITY, *supra* note 97, at 4 (noting that the cost insured cost could range from 21 to 71 billion in the example used while costing the economy up to $1 trillion in economic damage); *see also* Steve Morgan, *Cyber Crime Costs Projected To Reach $2 Trillion by 2019,* FORBES (Jan. 17, 2016, 11:01 AM), https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#5cc5ee0b3a91 (projecting that the costs of data breaches will be $2.1 trillion by 2019).

because of the potential "lumpiness" of the claims related to a catastrophic loss.[110] Insurance companies have developed sophisticated modeling tools and can generally anticipate losses related to natural disasters, but several insurance companies have been caught off-guard by disasters, such as the losses related to Hurricane Katrina, which accounted for over $38 billion in insured losses and caused the fourth largest insurer in Florida to go bankrupt.[111]

Loss models used by insurance companies for policies such as car insurance, life insurance, and homeowner's insurance, can reasonably predict the anticipated loss based on a large number of independent risks, that when aggregated, follow a predictable pattern over time.[112] However, a large cyber incident could potentially trigger all of the cyber insurance policies underwritten by an insurance company, irrespective of geographic location, which would create a situation far worse than other catastrophic losses suffered by the insurance industry from incidents such as Hurricane Katrina.[113] A small-scale example of this is the recent exploit Wannacry, which was a worm[114] that spread by exploiting vulnerabilities in the Microsoft Windows operating system and encrypting the files on the system until the ransom was paid.[115] This incident affected tens of thousands of computers in over seventy-four countries, which resulted in locking hospitals out of their patient data among other things.[116] The Wannacry incident demonstrated that even if there is a robust re-insurance market, a large scale cyber-attack could bankrupt the insurance companies issuing the policies and the re-insurers because the insurance companies are trying to issue policies to cover rapidly evolving human created threats which are typically hard to model and insure.[117]

110. *See* Patricia Born & W. Kip Viscusi, *The Catastrophic Effects of Natural Disasters on Insurance Markets*, 33 J. RISK & UNCERTAINTY 55, 55-56 (2006) (finding that insurance companies may go bankrupt or be forced to exit a market in the face of a catastrophic event).

111. *Id.* at 56.

112. *Id.* at 55.

113. *See generally id.* at 56.

114. *See* Margaret Rouse, *Security Search*, TECH TARGET, http://searchsecurity.techtarget.com/definition/worm (last visited Jan. 3, 2018) ("A computer worm is self-replicating malware that duplicates itself to spread to uninfected computers.").

115. Lily Hay Newman, *The Ransomware Meltdown Experts Warned About is Here*, WIRED (May 12, 2017, 2:03 PM), https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/.

116. *Id*.

117. Sam Friedman & Adam Thomas, *Demystifying Cyber Insurance Coverage*: *Clearing Obstacles in a Problematic but Promising Growth Market*, DELOITTE INSIGHTS, (Feb. 23, 2017), https://dupress.deloitte.com/dup-us-en/industry/financial-services/demystifying-cybersecurity-insurance.html.

D. Implications for Re-insurance Market

Another issue facing the cyber insurance market is the risk of a cascading cyber event triggering the re-insurance coverage for the insurers.[118] Under the McCarran-Ferguson Act,[119] states were given supremacy over the federal government to regulate insurance. States are responsible for: "(1) ensuring that consumers are charged a fair and reasonable price for insurance products; (2) protecting the solvency of insurers; (3) preventing unfair practices and overreaching by insurers; and (4) guaranteeing the availability of coverage to the public."[120] Under most state regulations, insurance companies are required to undergo periodic examination-audits during which, state regulators and the National Association of Insurance Commissioners ("NIAC")[121] examine the insurance companies' detailed financial records to determine whether they have adequate funds to meet their current and future policy obligations.[122]

As discussed above, companies storing large amounts of data could be liable for the costs of complying with the various state reporting requirements for data breaches, class action lawsuits, virtual bank robberies, and massive cascading cyber events.[123] In a 2014 Market Bulletin, Lloyd's of London raised the concern that their managing agents may not be properly pricing or adequately quantifying the potential exposure in their cyber policies.[124] Diversifying the risk in the cyber insurance market requires an in-depth scenario analysis of potential exposures due to a cyber-incident.[125] The policies currently in force are not designed for the "Internet of Things," in which a hacking event could trigger overlapping cyber, homeowner's insurance, business interruption and even auto insurance policies.[126]

118. *See* Steve Evans, *Cyber Risk Aggregation a Threat to Re/Insurer Solvency*, REINSURANCE NEWS (June 1, 2017), https://www.reinsurancene.ws/cyber-risk-aggregation-threat-reinsurer-solvency/ (noting that the Wannacry attack struck computers in over 150 countries and demonstrated the impact that a computer hack could have around the world).

119. The McCarran–Ferguson Act, 15 U.S.C. §§ 1011–1015 (2012).

120. ROBERT H. JERRY II & DOUGLAS R. RICHMOND, UNDERSTANDING INSURANCE LAW 89 (LexisNexis 5th ed. 2012).

121. For additional information about NIAC, visit http://www.naic.org/index_about.htm.

122. JERRY ET AL., *supra* note 120, at 94.

123. *See supra* Sections II–IV.

124. TOM BOLT, CYBER RISKS AND EXPOSURES: REF: Y4842 (Nov. 25, 2014), https://www.lloyds.com/~/media/Files/The-Market/Communications/Market-Bulletins/2014/11/Y4842.pdf.

125. *Id.*

126. *Id.*

V. BLOCKCHAIN BASED IDS TO REPLACE SOCIAL SECURITY NUMBERS

A. Social Security Numbers Were Not Designed to Be Utilized as a Secret Code to Access Credit Information

As a result of the numerous security breaches both at the federal level with the Office of Personal Management ("OPM") breach, the recent Equifax breach and other high profile breaches, individuals can no longer reasonably anticipate that their Social Security numbers will be secure.[127] The potential for massive breaches associated with the continued use of Social Security numbers is inevitable and it puts companies that store the information at risk.[128] It also puts consumer in the unenviable position of constantly paying for credit monitoring, costs to freeze their accounts, and other risks of identity theft.[129]

The current protocol for notifying consumers that their identity has been stolen does little to protect consumers.[130] In most cases, when a company identifies that their customers' data may have been compromised, based on the state, there are varying breach notification requirements.[131] However, other than the mandatory breach notification, most companies will only offer consumers affected by the breach one free year of credit monitoring as a mea culpa for their transgressions.[132]

As a result of the numerous breaches, including the most recent Equifax breach, it is almost inconceivable for any regulator to believe that we can continue using Social Security numbers as a key data point for allowing consumers to access credit, file taxes and drain bank accounts.[133] According to the Social Security Administration ("SSA"), the Social Security number was created in 1936 to keep track of the earnings

127. John Carlin & David Newman, *The Equifax Breach Proves it's Time to Stop Using Social Security Numbers,* CNBC (Oct. 9, 2017, 3:05 PM), https://www.cnbc.com/2017/10/04/equifax-breach-time-to-stop-using-social-security-numbers-commentary.html.

128. *Id.*

129. Yuki Noguchi, *After Equifax Hack, Consumers Are On Their Own. Here Are 6 Tips to Protect Your Data,* NPR (Sept. 14, 2017, 4:34 PM), https://www.npr.org/2017/09/14/550949718/after-equifax-data-breach-consumers-are-largely-on-their-own.

130. Marc Rotenberg, *Equifax, the Credit Reporting Industry, and What Congress Should Do Next*, HARVARD BUS. REV. (Sept. 20, 2017), https://hbr.org/2017/09/equifax-the-credit-reporting-industry-and-what-congress-should-do-next.

131. Dana B. Rosenfeld, Alysa Zeltzer Hutnik & Christopher M. Loeffler, *State Data Breach Laws Agency Notice Requirements Chart: Overview*, WESTLAW, https://1.next.westlaw.com/Document/I1559f980eef211e28578f7ccc38dcbee/View/FullText.html (search in search bar for the title of the document; then click on "Practical Law") (last visited Mar. 3, 2018) (providing a detailed chart describing the data breach notification requirements by state).

132. Rotenberg, *supra* note 130.

133. *Id.* (noting that the credit records of over 143 million consumers were compromised during the Equifax breach in 2017).

history of U.S. workers for the purposes of calculating their retirement benefits.[134] The SSA and the Department of Health and Human Services have made it clear that Social Security numbers were never intended to be used as an identifier for individuals.[135] The SSA recognizes that "[t]he universality of SSN ownership has in turn led to the SSN's adoption by private industry as a unique identifier."[136]As a result, its "universality has led to abuse of the SSN" most notably in the area of identity theft.[137]

An alternative method of identifying and tracking individuals needs to be established especially in light of the fact that bad actors now have enough data on at least half of the people in the United States to steal their identity.[138] This sentiment has been echoed by academics and even the former Equifax CEO Richard Smith in his testimony before the House Energy and Commerce Committee.[139] One of the most popular options proposed by security experts is to utilize multifactor biometrics to verify a person's information such as voice/facial recognition, iris scans, and fingerprints.[140] Another alternative that has been proposed is the use of blockchain, "which creates a public ledger of transactions."[141] This technology is already being utilized by Estonia as the "backbone for a digital ID system its citizens use for medical services, travel checkpoints and even for voting."[142]

B. Background on Blockchain

There has been a lot of buzz around blockchain, and digital currencies that utilize the blockchain technology like Bitcoin.[143] Bitcoin, and the underlying blockchain technology have been touted as a potential market disrupter because it may have many more applications ranging from trading platforms, smart contracts and even

134. Carolyn Puckett, *The Story of the Social Security Number*, SOC. SEC. ADMIN. (2009), https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html.

135. *Id.*

136. *Id.*

137. *Id.*

138. Rotenberg, *supra* note 130 (noting that half of the US population's data was exposed in the Equifax breach).

139. Nafeesa Syeed & Elizabeth Dexheimer, *The White House and Equifax Agree: Social Security Numbers Should Go*, BLOOMBERG (Oct. 3, 2017, 7:15 PM), https://www.bloomberg.com/news/articles/ 2017-10-03/white-house-and-equifax-agree-social-security-numbers-should-go.

140. Kaya Yurieff, *Why are we still using Social Security numbers as ID?*, CNN (Sept. 13, 2017, 8:40 AM), http://money.cnn.com/2017/09/13/technology/social-security-number-identification/index.html.

141. Hayley Tsukayama, *Your Social SecurityNumber May Not Be Secure. But How Could We Replace It?*, WASH. POST (Sept. 20, 2017), https://www.washingtonpost.com/news/innovations/wp /2017/09/20/your-social-security-number-may-not-be-secure-but-how-could-we-replace-it/?utm_term =.ca7bf5d6b5ec.

142. *Id.*

143. Alan Morrison & Subhankar Sinha, *A Primer on Blockchain*, PWC (Dec. 6, 2016) http://usblogs.pwc.com/emerging-technology/a-primer-on-blockchain-infographic/.

medial record repositories.[144] The value behind the blockchain technology is that it allows participants in the network to confirm a transaction, like a bitcoin exchange, without the need for a trusted third party intermediary like a bank.[145] This technology will increase security because of the decentralized nature of the blockchain, reduce transaction cost by eliminating intermediaries, decrease transaction time, and increase transparency because the blocks are all public.[146]

At the most basic level, blockchain is a decentralized ledger of all transactions in a network.[147] The chain is made up of blocks, which are essentially ledgers of the transactions that have been cleared and attached to the master ledger and can no longer be changed.[148] For example, if someone in the network requests a transaction, the transaction is broadcast to the other computers (nodes) in the network.[149] The network then validates the transaction using the underlying algorithm, and once verified, a new block is time stamped and chronologically added to the network's blockchain in a way that is permeant and unalterable.[150] The blockchain ecosystem is designed to be irreversible and auditable in near real time by every participant in the network.[151]

C. Blockchain as a Digital Identity

The transition to a blockchain based ID system would perhaps be the best solution for a country as large as the U.S. because it would not require the government to collect biometric data about its citizens, and it would create an audit trail to help prevent fraudulent transactions.[152] Additionally, the benefit of using blockchain algorithms is that as the technology improves, the algorithm can be updated to keep up with the technology.[153] Such technology could spark a digital revolution in the U.S., allowing the ID to be used to validate digital signatures on documents, prevent voter fraud, and provide a centralized record of the transaction.[154] One of the biggest challenges to the adoption of the digital blockchain approach is the fear that digital

144. Henry Hwangbo, *Blockchains: Bitcoin's Boundless Building Blocks*, PWC (Jan. 28, 2016), http://usblogs.pwc.com/emerging-technology/block-chains-bitcoins-boundless-building-blocks/.

145. *Id.*

146. *Id.*

147. *Id.*

148. *Id.*

149. Alan Morrison & Subhankar Sinha, *A Primer on Blockchain*, PWC (Dec. 6, 2016), http://usblogs.pwc.com/emerging-technology/a-primer-on-blockchain-infographic/.

150. *Id.*

151. *Id.*

152. Kalev Leetaru, *Replacing US Social Security Numbers With Estonia's Cryptographic Model?*, FORBES (Oct. 15, 2017, 6:42 PM), https://www.forbes.com/sites/kalevleetaru/2017/10/15/replacing-us-social-security-numbers-with-estonias-cryptographic-model/#74c1a2d72aab.

153. *Id.*

154. *Id.*

records will be maliciously modified or destroyed.[155] However, this concern is theoretically moot because the encrypted public ledger that the data is stored on "cannot be erased or rewritten without leaving a record of the previous data."[156] Based on the blockchain design, the data is considered incorruptible because it is a decentralized and distributed digital ledger that prevents the records from being modified.[157]

Companies like IBM and SecureKey have been developing and testing blockchain based identity solutions based on a "user centric model, also known as self-sovereign identity," which would allow users to control who has access to their personal information and could allow third parties like banks, without revealing details (like social security numbers or biometric information) behind the identity.[158] This technology is currently being used in a pilot program by several large Canadian banks and has enabled the banks to eliminate the need to check credit scores.[159] At the 2017 "Platform for Change" Summit at the United Nations, companies like PricewaterhouseCoopers, Microsoft and MasterCard have worked collaboratively to try to develop global digital IDs with technologies like blockchain.[160] The goal of the UN program is to "enable access to digital identity for every person on the planet" by 2030.[161] The global ID based on the blockchain technology would ultimately reduce the ability of bad actors across the world from accessing and manipulating personally identifiable information ("PII").[162]

IV. CYBER DATA BREACH REPORTING REQUIREMENTS

A. NY Department of Financial Services (DFS) (23 NYCRR500)

New York is one of the first states to implement comprehensive regulations establishing minimum required security practices.[163] The new regulation requires banks, insurance companies, and other financial institutions to comply with basic

155. Suzanne Woolley, *Want to Ditch Social Security Numbers? Try Blockchain,* BLOOMBERG (Oct. 9, 2017, 11:54 AM), https://www.bloomberg.com/news/articles/2017-10-09/want-to-ditch-social-security-numbers-try-blockchain

156. *Id.*

157. *Id.*

158. *Trust Me: Digital Identity on blockchain,* IBM INST. FOR BUS. VALUE (Apr. 2017), https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03823USEN&.

159. *Id.*

160. *ID2020 Summit Spotlights Technology and Digital Identity at the United Nations*, PWC (June 20, 2017), https://press.pwc.com/News-releases/id2020-summit-spotlights-technology-and-digital-identity-at-the-united-nations/s/cb3d1d10-813b-4826-8d1b-0b408fe8f739.

161. *Id.* (quoting the Executive Director of ID2020 Dakota Gruener).

162. *Trust Me: Digital Identity on blockchain,* IBM INST. FOR BUS. VALUE (Apr. 2017), https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03823USEN&.

163. 23 NYCRR 500, http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf.

security practices and risk assessment procedures outlined in the regulation to better safeguard consumer's private information and better protect New York's financial services industry as a whole.[164] The new regulations force financial institutions to seriously evaluate their cyber security posture and risk profile through detailed testing, training and planning.[165] One of the cornerstones of the regulation is the annual compliance representation that the Board of Directors or Senior Officer(s) of the Covered Entity are required to complete, certify and submit to the New York Department of Financial Services ("NYS DFS").[166] Although this regulation only impacts a limited number of institutions regulated by NYS DFS, it is a significant step in the right direction to helping bolster the security posture of companies in the U.S.[167] Commentators believe that other states will follow the lead of New York regulators and implement similar regulations once the regulations in New York are fully implemented.[168]

B. Data Breach Notification Laws

Most states have enacted security breach law that require the entity to notify individuals that their Personally Identifiable Information ("PII") has been compromised.[169] Currently, forty-eight states and most territories have enacted breach notification laws, with only Alabama and South Dakota not requiring notification.[170] Under most state breach notification laws, there is a safe harbor for companies that have encrypted data accessed. Recently, Tennessee passed an even more protective breach notification law that requires companies to report breach even if the data was encrypted.[171] Previously, companies were protected by a presumptive safe harbor provision in the state data breach laws that exempted them from the notification requirements if their data was encrypted.[172] The new legislation

164. *Id.*

165. *Id.*

166. *Id.*

167. *Frequently Asked Questions Regarding 23 NYCRR PART 500*, N.Y. DEPT. OF FIN. SERV. (Dec. 12, 2017), http://www.dfs.ny.gov/about/cybersecurity_faqs.htm (because of the Nationwide Cooperative Agreement, Revised as of December 9, 1997, only banks based in NY will be subject to these new regulations. This means that banks with branches in NY will not be subject to the regulations).

168. Daniel A. Cotter et. al., *The New York State Department of Financial Services Issues New Cybersecurity Regulations,* 27 WESTLAW J. INS. COVERAGE *1 (Dec. 1, 2016) 2016 WL 701599 (discussing the influence that NY DFS has in the banking community which will likely induce other regulators to follow suit).

169. *Security Breach Notification Laws*, NCSL (Apr. 12, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

170. *Id.*

171. Stephen Embry, *State Data Breach Notification Laws Just Got Crazier*, A.B.A. (May 2016), https://www.americanbar.org/publications/youraba/2016/may-2016/state-data-breach-notification-laws-just-got-crazier.html.

172. *Id.*

could be the start of a paradigm shift requiring companies to notify affected parties whenever their data is potentially compromised, whether encrypted or not.[173]

This shift could also have significant impacts on the way cyber insurance policies provide coverage and in the case of large breaches, could require varied reporting requirements depending on the types of information compromised, and the location of the person whose information was compromised.[174] According to a recent survey conducted by the Ponemon Institute, the average cost of a compromised record containing sensitive information was about $255 dollars per record and averaged $7.35 million per breach, not including breaches involving over 100,000 records.[175] Based on the new requirements, companies could potentially be on the hook for millions of dollars for breaches of records, even if the records are encrypted.[176] Companies should understand the coverage their cyber insurance policies provide in the case of a data breach with the various state and federal reporting requirements because in some instances, the cyber insurance policies may not provide coverage which would be in compliance with all of the state and federal requirements.[177]

VII. CONCLUSION

The IoT has created a world where almost everything that we do is reliant on data and interconnected computer systems. The string of escalating cyber events should be a warning to business, consumers, regulators and insurance companies about the potential catastrophic damage that can result from a cyber-event. However, there are several steps that Congress, businesses, and consumers can take to protect themselves today.

First, companies can develop an alternative multifactor unique identifier for consumers to use in place of Social Security number that could use a combination of blockchain and/or biometric data.[178] Second, Congress must pass comprehensive laws that establish minimum data security requirements for any company that has access to sensitive personal information, set harsh penalties for those that fail to comply, and open the gate for consumers to obtain redress in instances where their

173. *Id.*

174. Suzanne Woolley, *Your Social Security Number Now Looks Like a Time Bomb. It Is*, BLOOMBERG (June 1, 2017), https://www.bloomberg.com/news/articles/2017-06-01/identity-theft-feeds-on-social-security-numbers-run-amok.

175. PONEMON INST., 2017 COST OF DATA BREACH STUDY (June 13, 2017), https://www.ponemon.org/library/2017-cost-of-data-breach-study-united-states.

176. *Id.*

177. Stephen Embry, *State Data Breach Notification Laws Just Got Crazier*, A.B.A. (May 2016), https://www.americanbar.org/publications/youraba/2016/may-2016/state-data-breach-notification-laws-just-got-crazier.html.

178. *See supra* Section V.

PII is compromised.[179] Finally, insurance companies can help businesses increase their cyber posture by offering more competitive rates to those businesses with sound security practices. However, above all else, insurance companies must remain aware of the overall potential exposure that they have to a cyber-event due to the interconnected nature of the IoT.

179. *See supra* Section VI.