THE UGLY TRUTH ABOUT CYBER INSURANCE & GOVERNMENTAL DATA BREACHES

Sean Andrés Rapela[*]

I. Introduction

Just as the sun rises and sets, the wind blows, and the tides change; cyberattacks and data breaches occur.[1] Cyberattacks come in an array of forms, but, generally: ransomware, malware, phishing, and denial-of-service attacks are the usual suspects in data breaches.[2] Tracking software, wiretapping, and spear phishing are additional forms of threats that exist under the general umbrella of cyberattacks.[3] Furthermore, cyberattacks are not waning, but instead are increasing

[*] J.D. Candidate, Suffolk University Law School, 2021; B.A. in Political Science & International Affairs and English, Wake Forest University, 2018. Sean can be reached at seanrapela@gmail.com.

[1] *See* Juliana De Groot, *The History of Data Breaches*, DIGITAL GUARDIAN (Jan. 3, 2019), *archived at* https://perma.cc/TM38-PHXW (stating that "since 2011, however, the number of data breaches reported in the United States has been rising steadily"); *see also* James Cook, *The world's 10 biggest cybercrime hotspots in 2016, ranked*, BUSINESS INSIDER (May 14, 2017), *archived at* https://perma.cc/VU5U-B3GS (showing that in 2016, the United States accounted for 23.96% of cyber threats detected).

[2] *See* De Groot, *supra* note 1 (explaining data breaches often occur as a result of negligence or hacking, and the cyberattacks can generally be classified as ransomware, malware, phishing, or denial-of-service attacks); *see also* Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Insurance: How Companies Act as "Compliance Managers" for Businesses*, 43 LAW & SOC. INQUIRY 417, 418 (2018) (listing the different types of cyberattacks including "hackers, malware, viruses, tracking software, wiretapping, eavesdropping, robocalls, and solicitation").

[3] *See* Talesh, *supra* note 2, at 418 (listing the subcategories of cyberattacks including malware, viruses, tracking software, wiretapping, ransomware, and phishing).

exponentially with consumers' increasing reliance on technology.[4] According to the Computer Sciences Corporation, by end of 2020, over a third of data will pass through the cloud and increase data generation by 4,300 percent.[5] Additionally, cyberattacks do not discriminate, as they impact nearly every major industry and cost breached organizations a massive three to seven million dollars per breach on average.[6]

While corporate America is often the target of widely publicized breaches, such as the recent Marriot and Equifax breaches, cyberattacks pose a potentially greater threat to United States national security, and in particular government entities.[7] For example,

[4] *See* Talesh, *supra* note 2, at 418 (confirming that "As people become more reliant on electronic communication and organizations collect and maintain more information about their consumers, the opportunity for bad actors to cause problems for organizations and the public is growing exponentially.").

[5] *See id*. (according to the Theft Resource Center (TRC), there were 781 data breaches in 2015, and this is the second highest year on record since the TRC began tracking in 2005); *see also* De Groot, *supra* note 1 (outlining CSC's projections from a 2012 report).

[6] *See* Talesh, *supra* note 2, at 418 (indicating that cyberattacks impact almost all industries, including, but not limited to, "financial services, health care, government, entertainment, online gaming, retail, law, insurance, social networking, and credit card processing"). Additionally, recent reports reveal that "the average cost of a data breach event for an organization is between 3 and 7 million dollars." *Id.* *See also* John L. Rockenbach, *The Case for a Federal Cyber Insurance Program*, 97 NEB. L. REV. 555, 556 (2018) (stating that large quantities of wealth are lost annually to cyberattacks); *see also* Matt Egan, *Report: Cyber Crime Costs Global Economy up to $500B a Year*, FOX BUS. (July 22, 2013), *archived at* https://perma.cc/NJA9-8RUQ (revealing that cybercrime has a devastating impact on the economy); *see also* Stephanie Cohen & Mark Morril, *A Call to Cyberarms: The International Arbitrator's Duty to Avoid Digital Intrusion*, 40 FORDHAM INT'L L. J. 981, 983 (2017) (affirming that cyberattacks are "increasingly pervasive against corporations, law firms, government agencies and officials and other custodians of large electronic data sets of sensitive information"); *see also* Peter T. Leeson & Christopher J. Coyne, *The Economics of Computer Hacking*, 1 J. L. ECON. & POL'Y 511, 511 (2005) (confirming that "[i]n a 2004 survey of American companies and government agencies conducted by the Computer Security Institute, over half of respondents indicated a computer security breach in the past 12 months and 100 percent of respondents indicated a web site-related incident over the same period.").

[7] *See* Talesh, *supra* note 2, at 417–18 (revealing that the United States is an attractive target for cyberattacks); *see also* Larry Dignan, *Marriott faces massive data breach expenses even with cybersecurity insurance*, ZDNET (Nov. 30, 2018), *archived at* https://perma.cc/9WA7-U4N5 (predicting that "Marriott's total tab for a data breach affecting as many as 500 million consumers is going to cost

cyberattacks on government agencies, including the United States Postal Service breach, resulted in tens of millions of exposed records.

Many large companies have turned to cyber insurance as a way to mitigate the risks of cyberattacks, but government entities are largely uninsurable due to obsolete infrastructure and operating systems. Therefore, the government must take alternative measures to protect the data citizens are obligated to entrust it with, including Social Security numbers, dates of birth, and addresses. This Note argues that a cyber relief program, potentially through a tax, is necessary to aid all government entities in recovery from data breaches and cyberattacks. This Note will focus on why cyber insurance works for private organizations, but why a broader program is needed to protect government entities. Three possible avenues exist for this purpose. A Social Security-like payroll tax, a cyber excise tax, or a taxpayer alternative in the form of a federally funded insurance program. Each option could protect both the government and victims (citizens) of a data breach.

II. History

A. As Cyberattacks Increase, Organizations Turn to Cyber Insurance

Cyberattacks account for potentially more than four hundred billion dollars in losses annually, and many companies have turned to cyber insurance to mitigate these losses.[8] While there is limited data on the cyber insurance market, first-party loss and third-party liability

billions of dollars over the next few years, based on the average cost of megabreaches."). Additionally, "Equifax's 2017 data breach impacted 145.5 million US consumers whose personally identifiable information was impacted by an attack. In March 2018, Equifax disclosed that 2.4 million more US consumers were impacted." Dignan, *supra*.

[8] *See* 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, 391 (2017) (proffering the dollar amount of losses caused by cyberattacks); *see also* Talesh, *supra* note 2, at 419 (explaining that "[c]yber insurance is insurance designed to provide both first-party loss and third-party liability coverage for data breach events, privacy violations, and cyber attacks."); *see also Cybersecurity Insurance*, DEP'T OF HOMELAND SEC. (June 30, 2016), *archived at* https://perma.cc/6W2U-RJHT (describing cyber insurance as a way to "mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage").

coverage for cyberattacks is rapidly evolving.[9] Roughly one in three organizations have some form of cyber insurance.[10] However, cyber insurance may not remain a sustainable option for many organizations, as cyberattacks are an indefatigable risk, and, due to a recent growth in threats, policy premiums are expected to jump from two-and-a-half billion to almost eight billion by 2020.[11] Executives in many organizations are dejected at the thought of this, and despite the profound threat cyberattacks carry, many of these same executives express "compliance fatigue," as a result of never ending and expensive process of conforming with multiple security structures.[12]

B. How the Courts Interpret Cyber Insurance

Despite increasing policy premiums, the coverage that cyber insurance provides is likely inadequate due to the interpretation of the

[9] *See* Talesh, *supra* note 2, at 419 (describing generally that "[c]yber insurance is insurance designed to provide both first-party loss and third-party liability coverage for data breach events, privacy violations, and cyber attacks."); *see also* Scott J. Shackelford, *The Law of Cyber Peace,* 18 CHI. J. INT'L L. 1, 3 (2017) (confirming that "cyber insurance is probably the fastest growing insurance in the world").

[10] *See* Talesh, *supra* note 2, at 419 (claiming that "[w]hereas most companies did not have cyber insurance a decade ago, one in three organizations now has insurance specifically protecting against cyber and data theft losses."). *See also Cyber Liability Insurance*, EMBROKER (Apr. 19, 2020), *archived at* https://perma.cc/6JL3-DEDY (suggesting that "any business that uses technology or manages any digital information" should invest in cyber insurance, even small and medium sized businesses).

[11] *See* Trang, *supra* note 8, at 405 (declaring that "[c]urrently, the insurance market views cyber risk as 'a risk like no other' because of limited publicly available data and the quick evolution and proliferation of threats. Quick growth in threats is why annual gross written premiums are expected to increase from $2.5 billion to $7.5 billion by the end of the decade."); *see also* Talesh, *supra* note 2, at 419 (suggesting that "[r]ecent estimates suggest that the global insurance market collected approximately $2 billion in cyber insurance premiums and that this will rise by a magnitude of three to five times by 2020.").

[12] *See* Talesh, *supra* note 2, at 419 (explaining that "[a]lthough many organizations do have formal policies in place, the majority of organizations do not believe they are sufficiently prepared for a data breach, have not devoted adequate money, training, and resources to protect consumers' electronic and paper-based information from data breaches, and fail to perform adequate risk assessments."). "In fact, because complying with multiple security frameworks is difficult, time consuming, and expensive, many organizations express 'compliance fatigue.'" *Id*. *See* Rockenbach, *supra* note 6, at 571 (stating that "[b]y the late 1990s, business losses to security breaches ranged into the hundreds of billions," and many of the current cybersecurity measures in place are inadequate).

courts.[13] In general, there are three principal types of cyber insurance policies: (1) commercial general liability policies, (2) crime/fidelity cyber insurance policies, and (3) cyber policies—these policies work to shift the risk that comes as a result of having to respond, investigate, defend, and mitigate cyberattacks.[14] For example, when it comes to commercial general liability policies, which organizations often rely on to cover losses in data breaches, the courts typically have found no coverage.[15] However, for organizations with crime/fidelity cyber insurance policies, the results are more encouraging as the courts are more willing to find that coverage applies.[16] For instance, the Sixth

[13] *See* Trang, *supra* note 8, at 406 (citing that "[i]nsurance products and the applicable law have not been 'keeping pace with the emergent ubiquity of information technology in commercial enterprises.'"); *see also* Mark A. Collins, *Courts' Approach to Cyber Insurance Continues to Evolve*, JD SUPRA (May 21, 2019), *archived at* https://perma.cc/PYM4-XZQ4 (explicating that "[j]udicial treatment of policy provisions continues to evolve, and while existing precedent decided on other lines of coverage may provide some guidance, courts have yet to interpret many key cyber insurance policy provisions."); *see also* Zurich Am. Ins. v. Sony Corp. of Am., 2014 N.Y. Misc. LEXIS 5141, at *72 (Sup. Ct. 2014) (finding that coverage does not exist when publication is carried out by a third party and not the insured party).

[14] *See* Collins, *supra* note 13 (asserting that "companies purchase cyber insurance to protect against the risks of computer hacking and data breaches," and the three most prevalent policies are "comprehensive general liability (CGL), crime/fidelity and cyber insurance"); *see also* Talesh, *supra* note 2, at 419 (demonstrating that cyber insurance provides "some risk shifting for the costs associated with having to respond, investigate, defend, and mitigate against the consequences surrounding a cyber attack"); *see also* Daniel Schwarcz, *Coverage Information in Insurance Law*, 101 MINN. L. REV. 1457, 1500 (2017) (reaffirming that "[l]iability insurers attempt to avoid covering cyber-related liability in their general liability policies, principally for adverse selection reasons.").

[15] *See* Trang, *supra* note 8, at 406 (clarifying that state courts are yet to come to an agreement as to whether or not coverage includes loss of electronic data because of its lack of tangibility); *see also* Collins, *supra* note 13 (confirming that "most courts have rejected coverage for cyber incidents under CGL policies"); State Auto Prop. & Cas. Ins. Co. v. Midwest Comput. & More, 147 F. Supp. 2d 1113, 1115–16 (W.D. Okla. 2001) (holding that "computer data cannot be touched, held, or sensed by the human mind; it has no physical substance. It is not tangible property.").

[16] *See* Collins, *supra* note 13 (revealing that "[c]ourts have reached varying results when determining coverage for cyber-related losses under computer fraud provisions in crime/fidelity policies."). *See also* Collins, *supra* note 13 (stating that courts have historically taken a narrow view of what constitutes covered "computer fraud"). "A pair of 2018 appellate court decisions held that computer fraud coverage applied to "social engineering" schemes (an attack that relies on human interaction to manipulate users into making security mistakes) could have a large

Circuit held that where a phishing attack took place resulting in payments to an unintended bank account, the insured suffered direct losses that the organizations cyber insurance policy covered.[17]

Perhaps the most promising of the cyber insurance policies are cyber policies, also simply known as cyber-insurance policies, for these policies have the potential to protect both the breached organization and the consumers the breach victimizes.[18] Still, the cases involving this type of cyber insurance policy paint an incomplete picture, as this is still a newly developing body of law.[19] Nevertheless, organizations are often disinterested in tackling cyber security, and the disconcerting trend that exists is that cyber insurance is implemented in response to regulation by the government rather than organizations

impact on claims under this line of coverage." *Id*. *See* 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, 47 (2017) (indicating that "some crime policies will include a computer fraud rider that may allow coverage for certain expenses related to costumer communications, public relations, lawsuits, regulatory defense costs, and fines imposed by credit card vendors"); *see also* Medidata Sols. Inc. v. Fed. Ins. Co., 729 F. App'x 117, 118 (2d Cir. 2018) (ruling that Medidata's data losses were covered by insurance where phishing through a "fraudulent entry of data into the computer system" resulted in a "change to a data element").

[17] *See* Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455, 465 (6th Cir. 2018) (holding that where "[a]n employee of the insured received emails purportedly from the company's Chinese vendor, directing payment on outstanding invoices to a new bank account that was not, in fact, controlled by the vendor," the insured suffered a 'direct' loss when it mistakenly transferred funds to an impersonator, and that the impersonator's spoofing scheme constituted 'computer fraud.'"). *See* Trang, *supra* note 8, at 393 (defining phishing as "a method where a seemingly legitimate email from the employee's company asks the target employee to login on a false but seemingly official company website").

[18] *See* Trang, *supra* note 8, at 415–16 (detailing that "[c]yber-insurance has the potential to protect not just the breached company, but also millions of consumers."). "Cyber risks have high potential damages that may put a company out of business." *Id*. *See also* Collins, *supra* note 13 (cautioning that "[t]here is not yet a significant body of case law interpreting cyber insurance policies."). "These policies typically include first and third party coverage for network security and data privacy events, and there are a wide variety of coverage options available."). *Id*.

[19] *See* Trang, *supra* note 8, at 415–16 (reiterating that there is not significant case law available to interpret cyber insurance policies); *see also* Am. Tooling Ctr., Inc., 895 F.3d at 461 (defining what constitutes computer fraud); *see also* Medidata Sols. Inc., 729 F. App'x at 118 (describing what triggers insurance coverage as a result of fraudulent entry).

recognizing the risk and acting without government intervention.[20] As a result of this trend, many cyber insurance companies seek litigation avoidance rather than discouragement of illegal conduct.[21]

C. Expensive and Illusive: Cyber Insurance is Difficult to Obtain

Cyber insurance is difficult for many large companies, let alone small businesses, to obtain as a result of the expensive policies and often inadequate coverage.[22] As a result of the courts' indecisiveness when it comes to cyber insurance, new polices are created and old policies are updated or revised on a regular basis, and with so many different policies it is often extremely difficult for organizations to choose one.[23] Furthermore, even if an organization overcomes the

[20] *See* Rockenbach, *supra* note 6, at 584 (stating that "[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."); *see also* Norah C. Avellan, *The Securities and Exchange Commission and the Growing Need for Cybersecurity in Modern Corporate America*, 54 WASHBURN L.J. 193, 217 (suggesting that corporations are "under no concrete governmental obligation to ensure they remain aware of every cybersecurity event their corporation encounters"); *see also* John Winn & Kevin Govern, *Identity Theft: Risks and Challenges to Business of Data Compromise*, 28 TEMP. J. SCI. TECH. & ENVTL. L. 49, 54 (2009) (indicating that "in the federal sector, the focus has shifted somewhat from criminal enforcement to regulation"); *see also* Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 BERKELEY TECH. L.J. 909, 943 (2003) (reiterating that the government's response to cybercrime has been reactionary rather than aggressive).

[21] *See* Rockenbach, *supra* note 6, at 584 (emphasizing that the courts' rulings on cyber insurance are not facilitating a positive trend). *See* Trang, *supra* note 8, at 406 (confirming that the courts are coming to different results when analyzing whether or not cyber insurance coverage applies in cases for cyber-related-loss); *see also* Zurich Am. Ins. v. Sony Corp. of Am., 2014 N.Y. Misc. LEXIS 5141, at *1–74 (Sup. Ct. 2014) (holding that coverage does not exist when publication is carried out by a third party and not the insured party).

[22] *See* Rockenbach, *supra* note 6, at 585 (detailing the reasons why cyber insurance is difficult to obtain); s*ee also* Talesh, *supra* note 2, at 420 (claiming that many organizations are hesitant to acquire cyber insurance because it is extremely expensive).

[23] *See* Rockenbach, *supra* note 6, at 587 (confirming that obtaining cyber insurance can prove a daunting task because "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."); *see also* Julie Zhu, *Greater China cyber insurance demand set to soar after WannaCry attack - AIG*, REUTERS (Aug. 9, 2017), *archived at* https://perma.cc/X98U-BATS

time consuming process of choosing a cyber insurance policy, cyber insurance is extremely expensive, and, for the most part, only very large companies can afford it.[24] For instance, ahead of their breach, Equifax maintained 125 million dollars of cyber insurance coverage.[25] Moreover, the success of recent class action suits, such as the one that Target faced, has driven the price of cyber insurance up to the point where deductibles are so high that few companies can secure policy limits beyond fifteen million dollars.[26] Consequently, the question as to whether or not cyber risk is insurable is a legitimate question, for massive losses, lack of information, and failure in effective risk pooling all point to an arguably unsustainable system.[27]

D. The Government's Failure to Address Cybersecurity

While the courts have struggled to keep up with cyber insurance in the private sector, government entities are even further

(confirming that AIG, an cyber insurer "saw an 87 percent jump in enquiries for cyber insurance policies in May compared to April for Greater China," and that this increase suggests that organizations are beginning to see the importance of cyber insurance).

[24] *See* Rockenbach, *supra* note 6, at 587–88 (outlining that "insurers serve well as regulators of cyber risk, but this engagement and the overwhelming nature of the risk has led cyber insurance to be expensive."); *see also* Dignan, *supra* note 7 (revealing that Equifax maintains a 125 million dollars of cybersecurity coverage).

[25] *See* Ben Lane, *Equifax expects to pay out another $100 million for data breach*, HOUSINGWIRE (Feb. 14, 2020), *archived at* https://perma.cc/KG8V-S262 (describing the cost of Equifax's cyber insurance coverage).

[26] *See* Rockenbach, *supra* note 6, at 587–88 (confirming that "[i]ncreased regulation and the recent success of class action suits will lead to further increases."). Target and Anthem faced a tripling of insurance premiums after breaches. *Id*. Anthem agreed to a $25 million deductible in order to obtain $100 million in limits. *Id*. *See also* Judy Greenwald, *Target has $100M of cyber insurance, $65M of D&O cover: Sources*, BUSINESS INSURANCE (Jan. 14, 2014), *archived at* https://perma.cc/BSY2-PGB2 (revealing that despite Target's large cyber insurance policy the financial damage to the corporation is enormous).

[27] *See* Rockenbach, *supra* note 6, at 591 (arguing that "[t]he 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."). "A primary concern of the insurance industry is simply whether cyber risk is insurable." *Id*. *See* Trang, *supra* note 8, at 405 (hypothesizing that cyber risk may not be insurable because cyberattacks present a "a risk like no other," there is limited data available, and cyberattacks evolve too quickly).

behind.[28] There is a misconception that cybersecurity is a new problem; however, in 1965 the Brooks Act led to the creation of the National Institute of Standards and Technology which regulates security standards.[29] Furthermore, computer viruses date back to the 1990s, and by the turn of the century, business losses to security breaches were already in the hundreds of billions.[30] In recent years, Congress demonstrated they are hesitant to react to cybersecurity, as over one hundred cybersecurity bills were introduced over the past few years, yet the vast majority of them were not successful.[31] Consequently, current public law is largely reactive, and unorganized.[32] To date, public law contains no remedy for

[28] *See* Collins, *supra* note 13 (emphasizing that the courts are still grappling with how to address cyber insurance); *see also* Rockenbach, *supra* note 6, at 571 (proclaiming that the United States public law response to cyber risk is historically inadequate); *see also* Matt Williams, *Why Most Governments Don't Carry Cyber Insurance*, GOVERNMENT TECHNOLOGY (Aug. 7, 2013), *archived at* https://perma.cc/X22X-E9X5 (explaining that government agencies use antiquated systems and lack the expertise necessary to secure high-value data, and as a result cyber risk is essentially uninsurable at the government level).

[29] *See* Rockenbach, *supra* note 6, at 571 (articulating that "[g]overnment 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."). *See also About NIST*, NAT. INST. STANDARDS & TECH.(June 14, 2017), *archived at* https://perma.cc/PY8F-D4AM (describing the National Institute of Standards and Technology).

[30] *See* Rockenbach, *supra* note 6, at 571 (noting that "Computer viruses date to the 1990s."). "By the late 1990s, business losses to security breaches ranged into the hundreds of billions." *Id*. "Cyber insurance policies began to appear by the late 1990s." *Id*. *See* Talesh, *supra* note 2, at 418 (suggesting that the United States is an attractive target for cyberattacks).

[31] *See* Rockenbach, *supra* note 6 at 572–73 (addressing the issue that "[c]urrent public law has three glaring deficiencies: it is overly voluntary, it is overly reactive, and it lacks involvement of the national security infrastructure."). "These deficiencies have rendered the public law structure largely ineffective." *Id*. *See also* Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 467 (2008) (highlighting that laws and regulations enacted by Congress "have either ignored government data mining entirely or failed to provide any structure for when data mining is appropriate, how it should be conducted, and/or how privacy is to be protected."). *See also* 47 U.S.C.S. § 551 (LexisNexis 2020) (the Cable Act of 1984 does not allow for cable providers to provide the government with the data of their customers).

[32] *See* Rockenbach, *supra* note 6, at 571 (describing that Congress inadequately addressed cyber security); *see also* Julia N. Mehlman, *If You Give a Mouse a Cookie, It's Going to Ask for Your Personally Identifiable Information: A Look at*

government entities, private entities, or victims of cyberattacks, and in the past the government has often turned to taxes to address legislative gaps.[33]

E. Social Security: How the Government Implements Necessary Tax Systems

In general, a lot of federal revenue is collected from payroll taxes, such as Social Security, which are regressive taxes; meaning that the rate is constant rather than proportional.[34] Congress enacted the

the Data-Collection Industry and a Proposal for Recognizing the Value of Consumer Information, 81 BROOK. L. REV. 329, 353 (2015) (pleading that "the need for regulation of the data-collection industry cannot be stressed enough."); *see also* Nelly Rosenberg, Comment, *An Uphill Battle: FTC Regulation of Unreasonable Data Security as an Unfair Practice*, 66 DEPAUL L. REV. 1163, 1174 (2016) (confirming that "Congress reviewed dozens of proposed bills concerning broad oversight of privacy and data security, but has not yet passed any comprehensive laws."); *see also* Ariana L. Johnson, *Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation*, 20 N.C. BANKING INST. 277, 298 (2016) (stating that "[t]he financial sector continued to actively voice its desire for Congress to delineate specific legal protections for private entities that wish to share cyber threat information with one another and the federal government.").

[33] *See* Justin (Gus) Hurwitz, *Cyberensuring Security*, 49 CONN. L. REV. 1495, 1516 (2017) (stressing that "[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."). *See also* David J. Bier, *Integrating Integrity: Confronting Data Harms in the Administrative Age*, 99 B.U. L. Rev. 1799, 1801 (2019) (affirming that "[c]ommonly, no post-breach remedy is available to harmed parties. And when one is available, it is woefully inadequate."). Furthermore, because "between fourteen and thirty-three percent of data-breach victims ultimately become victims of fraud, at least twenty million Americans are likely to suffer real world consequences." *Id*. Consequently, some victims have had to take matters into their own hands, and as a result make out-of-pocket purchases for credit card monitoring services or freezes on credit reports. *Id*. at 1808.

[34] *See generally* Social Security Act, 42 U.S.C. § 402 (referencing the Social Security Act legislation); *see also* Deborah A. Geier, *Integrating the Tax Burdens of the Federal Income and Payroll Taxes on Labor Income*, 22 VA. TAX REV. 1, 3 (2002) (asserting "[w]hile the tax debate centers on the federal income tax burden, provocative empirical studies published by economists Andrew Mitrusi and James Poterba in 2000 show that nearly two-thirds of American households now pay more in federal payroll taxes than income taxes . . ."); *see also* Neil H. Buchanan, *Social Security is Fair to All Generations: Demystifying the Trust Fund, Solvency, and the*

Social Security Act as a response to the Great Depression, which caused millions of Americans to lose their life-savings.[35] Nearly everyone retires at some point, and a person is not entirely responsible for all aspects of their retirement, for an individual does not know when they will die.[36] Therefore, the Social Security system provides an additional barrier between retirement and insolvency before death.[37] The Social Security system operates through the payroll tax, and this means that the labor income of every American contributes the pool.[38] Additionally, the current structure of the Social Security payroll tax collects from both employers and employees at an equal rate.[39]

Promise to Younger Americans, 27 CORNELL J. L. & PUB. POL'Y 237, 253 (2017) (explaining that the "Social Security Act was enacted in 1935, in the midst of the Great Depression"); *see* Julia Kagan, *Regressive Tax*, INVESTOPEDIA (May 25, 2020), *archived at* https://perma.cc/44EF-RXLJ (defining a regressive tax as "a tax applied uniformly, taking a larger percentage of income from low-income earners than from high-income earners. It is in opposition to a progressive tax, which takes a larger percentage from high-income earners.").

[35] *See* Social Security Act, 42 U.S.C. § 402 (citing the creation of Social Security).

[36] *See* Buchanan, *supra* note 34, at 253.

> Social Security, therefore, also provides protection for the rest of society from those who would fail - due to excess optimism, myopia, or any other reason - to protect themselves with adequate income for their entire lives. Even those who are willing and able to save for their retirements can fail to protect themselves adequately; and when their plans - or their failure to plan - puts them in difficult financial straits, it is the rest of society that will pay.

Id.

[37] *See id*. at 252 (illustrating that the Social Security system provides an additional kind of safety net: protection against running out of money before death."). *See also* Social Security Act, 42 U.S.C. § 402 (referencing the Social Security Act and age for retirement to receive benefits at 62).

[38] *See* Buchanan, *supra* note 34, at 253 (explaining that "[t]he simplest aspect of the Social Security system is the *payroll* tax, which is paid beginning with the first dollar of labor income."). "It is not, however, levied against any unearned income, such as income from rents, interest, dividends, and so on." *Id. See* Claire Boyte-White, *How is Social Security Tax Calculated*, INVESTOPEDIA (Apr. 17, 2020), *archived at* https://perma.cc/YH2M-N83E (describing that Social Security is a regressive tax).

[39] *See* Buchanan, *supra* note 34, at 253 (clarifying that "[t]he payroll tax rate is constant rather than graduated - currently 12.4%, with 6.2% collected from the gross wages or salary of the worker and 6.2% collected from the worker's employer."); *see also* Boyte-White, *supra* note 38 (explaining that "[t]his percentage is determined by law each year and applies to employees and employers . . . [t]hose who are self-employed are liable for the full 12.4%").

Therefore, it logically follows that the Social Security system plays a crucial role in the long-term financial planning of United States citizens, and the nearly universal government run retirement system also serves as an economic stabilizer—for even when the market declines, retirees do not need to cut their spending to conserve their wealth.[40] Still, the Social Security system has its disadvantages, for the retirement age to receive benefits continues to increase, and many retirees are waiting until later in life to claim benefits in order to receive maximum payouts.[41] However, Americans recognize the importance of the Social Security system, and a large number are willing to pay even more taxes in order to ensure its survival.[42]

F. Unrelenting: Cyberattacks Will Continue to Plague Public and Private Sectors

With the continuing growth of cyber-crime, it is impossible to ignore the always looming threat of cyberattacks and data breaches.[43] When private organizations or government entities are breached, the result is a long and expensive process that almost certainly involves

[40] *See* Buchanan, *supra* note 34, at 254 (demonstrating that "[t]he Social Security system has become an essential part of people's long-term financial planning . . . Social Security benefits are now a bulwark supporting the consumption expenditures that prop up the U.S. economy"); *see also* Geier, *supra* note 34, at 47 (stating that "[w]hen congress adopted the Social Security system, there were few pension plans and few participants.").

[41] *See Social Security Act*, HISTORY (Jan. 26, 2018), *archived at* https://perma.cc/A374-R7F6 (stating that "[s]till, despite attempts to keep it solvent, Social Security faces a major long-term shortfall. The retirement age to receive full benefits continues to increase and many beneficiaries are claiming benefits much later in life to receive maximum payouts, often at age 70."); *contra* Social Security Act, 42 U.S.C. § 402(a)(2) (stating that old-age insurance benefits to not begin until the citizen has reached age 62).

[42] *See Social Security Act*, *supra* note 41 (claiming that "[d]espite the program's pitfalls, most Americans want Social Security to continue and consider it a retirement lifeline, according to a National Academy of Social Insurance survey."). And eighty-one percent of them are willing to pay more taxes to ensure it. *Id.* Whether politicians are listening and can come up with a viable solution remains to be seen. *Id. See also* Buchanan, *supra* note 34, at 254 (affirming that American citizens recognize the importance of the Social Security system, for it is an essential part of everyone's long-term financial planning).

[43] *See* Amy Martinez, *Data-breach settlements and cyber-security lawsuits*, FLA. TREND (Jan. 25, 2019), *archived at* https://perma.cc/CU64-C9J4 (acknowledging the rise of cyber-crime, and that this increase has resulted in a growth in class action cases).

the legal system.[44] For instance, the Target data breach took place in 2013, and five years and millions of dollars later the U.S. Court of Appeals for the 8th Circuit affirmed a lower court's ten million dollar settlement agreement between Target and impacted customers.[45] Typically, a data breach costs a company around three million dollars, but this does not account for further damage to an organization's reputation.[46] Moreover, many data breaches are far more expensive than just three million dollars, for Marriot's recent breach potentially impacted 500 million consumers and will likely cost billions of dollars over the next several years.[47] Equifax faced a similar situation in 2017 where a data breach resulted in over one-hundred and forty million victimized consumers.[48] Thankfully, Equifax's cyber insurance policy covered a large portion of the expenses that resulted from the breach, but their policy still included a seven and a half million dollar deductible.[49] While cyber insurance offers some protection to private

[44] *See id*. (revealing that "[l]ast year, the U.S. Court of Appeals for the 8th Circuit confirmed a lower court's approval of a $10-million settlement between Target and customers affected by a 2013 data breach."); *see also* Sciaroni v. Target Corp. (*In re* Target Corp. Customer Data Sec. Breach Litig.), 892 F.3d 968 (8th Cir. 2018) (affirming the approval of the settlement agreement).

[45] *See* Martinez, *supra* note 43 (demonstrating how long it takes for the courts to work through a data breach); *see also* Sciaroni, *supra* note 44 at 972 (noting that the case came "as a result of the 2013 Target security breach" and litigation only concluded five years later).

[46] *See* Martinez, *supra* note 43 (claiming that "[a] data breach typically costs a small business about $3 million, not counting loss of reputation and good will, according to the Ponemon Institute, a privacy and information management research firm."); *see also* Trang, *supra* note 8, at 415–16 (suggesting that cyberattacks cost organizations millions of dollars and have the potential to put companies out of business).

[47] *See* Dignan, *supra* note 7 (predicting that "Marriott's total tab for a data breach affecting as many as 500 million consumers is going to cost billions of dollars over the next few years, based on the average cost of megabreaches.").

[48] *See id*. (comparing Marriott to "Equifax's 2017 data breach impacted 145.5 million US consumers whose personally identifiable information was impacted by an attack. In March 2018, Equifax disclosed that 2.4 million more US consumers were impacted.").

[49] *See id*. (explaining the impact of Equifax's cyber insurance policy). Equifax also made the following statement about their cyber insurance:

> We maintain $125.0 million of cybersecurity insurance coverage, above a $7.5 million deductible, to limit our exposure to losses such as those related to the 2017 cybersecurity incident. During the three months ended September 30, 2018, the Company has not recorded any insurance recoveries. During the nine months ended September 30, 2018, the Company has recorded insurance

organizations, virtually uninsurable government entities are left essentially unable to obtain any sort of cyber insurance.

III. Premise

A. Cyber-Attacks are More Prevalent Than Ever

Nearly every aspect of the average consumer's life today is connected to the internet in some capacity. From waking up to an iPhone's alarm, starting a car remotely, or running the dishwasher from your phone at work, people are always connected.[50] In such an age of connectivity, the door is ajar for cyberattacks and data breaches, and as society moves towards more connectivity, the attacks and breaches will increase congruently.[51] Large companies consistently make headlines for data breaches that occur, and when they occur, consumer data is usually compromised and exposed.[52] More recent breaches include Michaels's, Dairy Queen, Home Depot, JPMorgan Chase, and Sony, which all exposed data like Social Security numbers and the debit card information of millions of consumers.[53]

> recoveries of $45.0 million. Since the announcement of the 2017 cybersecurity incident in September 2017, we have recorded and received insurance recoveries of $95.0 million for costs incurred through September 30, 2018.

Id.

[50] *See* Kevin Digrazia, *Cyber Insurance, Data Security, and Blockchain in the Wake of the Equifax Breach*, 13 J. BUS. & TECH. L. 255, 255 (2018) (highlighting how connected consumers are through smart devices); *see also* Talesh, *supra* note 2, at 418 (affirming that people are increasingly reliant on their devices for electronic communication, and this creates a lot of opportunity for cyberattacks).

[51] *See* Digrazia *supra* note 50 (referencing the Equifax breach where "hackers were able to access "people's names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers"). *See* Dignan, *supra* note 7 (indicating that in regards to Marriott's breach, "[f]or about 327 million of those guests, personal information such as date of birth, gender, email, passport numbers, and phone numbers may have been exposed . . . in some cases, payment card information may have been exposed.").

[52] *See* Clara Kim, *Granting Standing in Data Breach Cases: The Seventh Circuit Paves the Way Towards a Solution to the Increasingly Pervasive Data Breach Problem*, 2016 COLUM. BUS. L. REV. 544, 544 (2019) (explaining how often data breaches occur and what happens to consumer data when they occur at private companies).

[53] *See id*. at 548–49 (detailing recent data breaches of "household names such as Michaels (2.6 million payment cards), Sally Beauty (280,000 credit and debit cards), New York State (22.8 million private records of New Yorkers taken over

Government entities are not safe from data breaches either; for instance, New York State fell victim to a breach resulting in the exposure of 22.8 million private records of New Yorkers over an eight year period.[54] Furthermore, government entities are more prone to data breaches, as data suggests that they were responsible for the most breaches in 2018, and even worse, these breaches on average took two-and-a-half times longer to detect.[55] While private organizations get most of the attention concerning data breaches, government entities have quietly skirted scrutiny while routinely exposing information.

---

eight years), Dairy Queen (600,000 debit and credit cards), Home Depot (56 million credit and debit cards), Jimmy John's (216 stores), JPMorgan Chase (76 million households and 7 million small businesses), and Sony (47,000 social security numbers, which were exposed more than 1.1 million times on 601 publicly-posted files stolen by hackers)."); *see also* 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, 264 (2012) (highlighting Sony Corporation's breach, and confirming that "Sony made headlines for breaches of its Playstation Network and Qiocity services in April as hackers accessed Sony's clients' personal information."); *see also* Matt Egan, *The Disclosure Debate: When Should Companies Reveal Cyber Attacks*, FOX BUS. (Oct. 28, 2011), *archived at* https://perma.cc/2T4U-ASVU (revealing that "Concerns about companies' cyber-security disclosure policies have mounted amid new reports suggesting recent high-profile attacks have been more damaging than the public was initially led to believe."); *see also* 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, 375 (2015) (indicating that "by the time Home Depot formally confirmed the breach Monday, September 8, 2014, two consumer class action suits had already been filed . . . ").

[54] *See* Podolack, *supra* note 53, at 374 (demonstrating that government entities are targeted in data breaches and cyber-attacks as well); *see also* NewsCore, *Hackers Claim Third Attack on Arizona Police*, FOX NEWS (Nov. 4, 2015), *archived at* https://perma.cc/E7TS-WGEF (revealing that the Arizona Police Department was hacked "amid a broader spate of digital break-ins targeting governments and corporations.").

[55] *See* Gopal Ratnam, *Government and health care sectors had most breaches in 2018*, ROLL CALL (June 4, 2019), *archived at* https://perma.cc/4LR4-DXNS (confirming that the government sector had the most breaches in 2018). Data breaches take, on average, 2.5 times longer to detect in government entities than they do in the private sector. *Id. See also* Paul R. DeMuro, *Keeping Internet Pirates at Bay: Ransomware Negotiation in the Healthcare Industry*, 41 NOVA L. REV. 349, 357 (2017) ("In 2015, healthcare organizations were targeted by cybercriminals more than most other industries."). Furthermore, "older technology, such as copy machines, are also connected to the organizations servers," and "these technologies are very vulnerable to cyberattacks." *Id.* at 359–60.

B. Data Breaches to State Governmental Entities

Unlike the private sector, citizens are not able to choose to withhold information like Social Security numbers, dates of birth, or tax filings from the government, and the government has not done enough to protect this information it requires from its citizens.[56] Data breaches in the government are not uncommon, in addition to the data breach of New York State, Utah faced a data breach in 2012 that resulted in the exposure of 800,000 Utahan's personal information.[57] Furthermore, a recent study of security breaches involving government entities uncovered 443 breaches involving 168,962,628 records.[58] This study involved a sample of government agencies over a four and a half year period:[59]

---

[56] *See* A. Michael Froomkin, *Symposium: Security Breach Notification Six Years Later: Government Data Breaches*, 24 BERKELEY TECH. L.J. 1019, 1019 (2009) ("Private data held by the government is not the same as private data held by others."). "Much of the government's data is obtained through legally required disclosures or participation in licensing or benefit schemes where the government is, as a practical matter, the only game in town." *Id*. *See also* Fernando M. Pinguelo & Bradford W. Muller, *Virtual Crimes, Real Damages: A Primer on Cybercrimes in the United States and Efforts to Combat Cybercriminals*, 16 VA. J.L. & TECH. 116, 120 (2011) (reiterating that the government is an "appealing target for cybercriminals, as their networks hold some of their citizens' most vital information, including health and driving records, educational and criminal records, professional licenses, and tax information."); Gregory T. Nojeim, *Cybersecurity and Freedom on the Internet*, 4 J. NAT'L SEC. L. & POL'Y 119, 120 (2010) (indicating that "computer hackers have penetrated systems containing designs for a new Air Force fighter jet and stolen massive amounts of information.").

[57] *See* Daniel J. Marcus, *The Data Breach Dilemma: Proactive Solutions For Protecting Consumers' Personal Information*, 68 DUKE L.J. 555, 558 (2018) (citing a data breach that occurred in Utah); *see also* Kim, *supra* note 52 at 548 (referencing a New York State data breach that resulted in the exposed records of citizens).

[58] *See* Natasha Bach, *160 Million Government Records Exposed in Data Breaches Since 2014, Study Finds*, FORTUNE (July 25, 2019), *archived at* https://perma.cc/VZ8Q-W78T ("A new study has discovered 443 breaches involving 168,962,628 records in the past 4.5 years."); *see also* Paul Bischoff, *Government Breaches – can you trust the US Government with your data?*, COMPARITECH (July 24, 2019), *archived at* https://perma.cc/3CZ4-BBUY (citing Comparitch's study of the 443 breaches).

[59] *See Bach*, *supra* note 58 (stating the scope and length of the study); *see also* Froomkin, *supra* note 56, at 1022 ("Governments hold a wide variety of data on natural and legal persons, great both in scope and in scale."); *see also* Peter Suciu, *Government Data Breaches by the Numbers – OPM Hack Remains One of the Worst*, CLEARANCEJOBS (July 26, 2019), *archived at* https://perma.cc/LNE6-

Government Agency	**Year**	**Number of Compromised Records**
U.S. Postal Service	2018	60,000,000
Off. of Personnel Mgmt.	2015	21,500,000
Cal. Sec'y of State	2017	19,200,000
Gov't Payment Service, Inc.	2018	14,000,000
Ga. Sec'y of State	2015	6,000,000
Off. of Child Support Enf't	2016	5,000,000
Off. of Personnel Mgmt.	2015	4,200,000
U.S. Postal Service	2014	3,650,000
Los Angeles County 211	2018	3,200,000
Wash. Dep't of Fishing and Wildlife	2016	2,435,452

Governmental entities in Washington D.C. were victimized by the most data breaches with thirty-seven reported cases compromising 95,166,900 records.[60] In 2018, the United States Department of State experienced a breach involving its cloud-based email service that exposed the personal information of employees.[61] Even more troubling than the breaches themselves perhaps are the lack of remedies available to the victims.[62] In a recent data breach in

UNUV (listing the "top 10 largest data breaches of government entities by number of records exposed since 2014").

[60] *See* Bach, *supra* note 58 (revealing that Washington D.C. has more breaches than any other state in the US).

[61] *See* DSM, *The 6 Biggest U.S. Government Data Breaches and How to Protect Your Data*, DSM (Sept. 20, 2018), *archived at* https://perma.cc/BB6K-6U5C ("State Department experienced a data breach within its unclassified Microsoft Office 365 cloud-based email service, compromising the personal information of a small number of employees.").

[62] *See* Froomkin, *supra* note 56, at 1021 (alleging that "the remedies available to victims of a government data breach are often less than those available to victims of private sector data breaches."). *See also* James Emory Tucker, Jr., *Invisible Wounds of Modern Warfare: A Remedy for Nascent, Latent Injuries Servicemembers Sustain in Cyber Battlespace*, 11 J. MARSHALL L.J. 1, 19 (2018) ("Remedies for the victims of cybersecurity breaches or hacks experience various complications in the aftermath, but Federal and state governments have been slow to provide remedies to those affected."); *see also* Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, 2015 U. ILL. J.L. TECH. & POL'Y 341, 353 ("Just as in the case of national security matters and issues involving war, it appears consumers need to rely on their government to protect them."); *see also*

Pasquotank County, North Carolina, a hacker operating outside of the United States accessed a server housing billing information related to emergency medical transportation services resulting in the exposure of Social Security numbers, dates of birth, and other medical information.[63] While the county offered access to identity theft protection services, the remedy does not address the radius of the risk of compromised data.[64]

C. Data Breaches in the Federal Government Today

One of the largest and most recent breaches to occur took place when the United States Postal Service discovered that hackers compromised their Informed Delivery feature to commit fraud and identity theft.[65] When the United States Postal Service announced that they fixed the flaw, they also revealed that the cyberattack exposed the personal information of sixty million users, including email addresses, usernames, user IDs, account numbers, street addresses, and phone

Derek E. Baumbauer & Oliver Day, *The Hacker's Aegis*, 60 EMORY L.J. 1051, 1067 (2011) ("Organized crime entities, malware operators, and governments pay well for vulnerabilities in important software products, particularly those with no known patch or defense."); *see also* John P. Carlin, *Detect, Disrupt, Deter: A Whole-Of-Government Approach to National Security Cyber Threats*, 7 HARV. NAT'L SEC. J. 391, 396 (2015) ("A whole-of-government approach is critical to success in disrupting national security cyber threats.").

[63] *See Pasquotank County Notice of Data Breach to Consumers*, OFF. VT. ATT'Y. GEN. (Feb. 25, 2019), *archived at* https://perma.cc/V3GM-UQLF (stating that a data breach occurred in Pasquotank County, North Carolina).

[64] *See* Cody Gredler, *The Real Cost of Identity Theft*, CS ID A PART OF EXPERIAN (Sep. 9, 2016), *archived at* https://perma.cc/26W9-4CPD (illustrating that in 2016 the DOJ found that the average cost of identity theft to the victim is $1,343, but this does not account for poor credit scores or loan denials years later). *See also* Tucker, Jr., *supra* note 62, at 19 ("Typically, companies or government agencies whose cybersecurity has been breached offer varying packages of identity and credit monitoring, identity restoration services, and identity theft insurance in an attempt to help their clients brace for impact."). Moreover, "cybersecurity breaches leave the consumer damaged, vulnerable for future victimization, and without much recourse." *Id.*

[65] *See 10,000 BREACHES LATER: TOP FIVE MILITARY AND GOVERNMENT DATA BREACHES*, ITRC (Oct 17, 2019), *archived at* https://perma.cc/3AWR-G8WX [hereinafter *10,000 BREACHES LATER*] (detailing that United States Postal Service issued an alert that cybercriminals were using the Informed Delivery feature to commit fraud and identity theft); *see also Informed Delivery by USPS*, USPS (Jan. 31, 2020), *archived at* https://perma.cc/8MNC-W3BF (detailing the recently hacked informed delivery program that allows for users to Digitally preview their mail and manage their packages).

numbers.[66] Additionally, Government Payment Service, Inc., who contracts with thousands of federal, state, regional and local governments to process payments stemming from fees and fines, exposed fourteen million customer records as a result of a data breach to their payment portal in September 2018.[67]

While many of these breaches can have dire consequences, some breaches can even prove deadly, such as the recent US Army breach that leaked sensitive information about immigrant recruits.[68] Furthermore, cyberattacks are a direct threat to the safety and integrity of the United States Government as countries move towards utilizing more cyber warfare tactics.[69] Government entities, at all levels, are far from immune to data breaches, and when they do occur, the consequences often carry a weight greater than the remedies available to victims.[70]

D. Cyber Insurance Can Mitigate Data Breach and Cyberattack Damages

Cyberattacks cost over an estimated $400 billion annually for companies and governments across the globe, and this price tag

[66] *See 10,000 BREACHES LATER*, *supra* note 65 (detailing the data exposed as a result of the United States Postal Service breach).
[67] *See id.* (explaining the scope of the United States Postal Service breach).
[68] *See* Alex Horton, *Hundreds of immigrant recruits risk 'death sentence' after Army bungles data, lawmaker says*, WASH. POST (Mar. 6, 2019), *archived at* https://perma.cc/7D77-34CR (noting that "sensitive information about hundreds of immigrant recruits from nations such as China and Russia . . . could aid hostile governments in persecuting them or their families").
[69] *See* Andrea M. Matwyshyn, *Cyber Harder*, 24 B.U. J. SCI. & TECH. L. 450, 451 (2018) (stating that "both the United States and the United Kingdom publicly identified Russia as the author of the malware—allegedly a part of Russia's hybrid warfare' aimed primarily at destabilizing Ukraine."). Additionally, many could argue that even the most recent U.S. presidential elections were impacted by attacks on vendors. *Id.* at 452–53. *See also* 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) (stating that cyber threats are "the greatest danger to US national security outside of weapons of mass destruction.").
[70] *See* Froomkin, *supra* note 56, at 1021 (alleging that "the remedies available to victims of a government data breach are often less than those available to victims of private sector data breaches."); *see also* Matwyshyn, *supra* note 69, at 453 (offering that the current cybersecurity approaches by the United States Government are "clearly not succeeding, and the state of security looks bleak").

certainly will increase in the coming years.[71] However, companies, at least in the private sector, understand the importance of cybersecurity and in 2015 the cyber security industry generated 75.4 billion dollars.[72] While cyber insurance is not yet widely known, a market for it has existed since the 1970s, and today annual cyber premiums are at 2.5 billion dollars.[73]

Roughly one in three organizations possess cyber insurance or some form of it in order to provide remedies for risk aversion, and it also makes available compensation for victims of data breaches.[74] Furthermore, as of 2015, there are more than 120 different insurance groups that are issuing cyber insurance policies in the United States.[75] Rather than familiar insurance names such as Geico or State Farm, many of these large companies turn to cyber insurance providers that specialize more in the financial services industry.[76] While one might look at cyber insurance as a way for organizations to recover after a

[71] *See* Lauren Miller, *Cyber Insurance: An Incentive Alignment Solution to Corporate Cyber-Insecurity*, 7 J.L. & CYBER WARFARE 147, 152 (2019) ("A 2017 report by McAfee estimates that cyberattacks cost approximately $400 billion annually for companies and governments across the globe.").

[72] *See* Jeff Kosseff, *Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System*, 19 CHAP. L. REV. 401, 404 (2016) ("Companies are understandably concerned about the exposure of their customers' and employees' personal information, both because of potential legal liability and damage to their brand.").

[73] *See* Miller, *supra* note 71, at 161 (explaining that cyber insurance has been around for about 50 years, but it is still not that well known to the average American); *see also* Rockenbach, *supra* note 6, at 571 (reminding that computer viruses date back to the 1990s).

[74] *See* Michael Faure & Bernold Nieuwesteeg, *THE LAW AND ECONOMICS OF CYBER RISK POOLING*, 14 N.Y.U. J. L. & BUS. 923, 931 (2018) (emphasizing that organizations obtain cyber insurance in order to shift risk); *see also* Talesh, *supra* note 2, at 419 (stating that one in three organizations have cyber insurance); *see also* Miller, *supra* note 71, at 182 (proffering that cyber insurance can help victims get compensation); *see also* Christian Biener, et al., *Insurability of Cyber Risk: An Empirical Analysis*, 40 GENEVA PAPERS ON RISK & INSURANCE 131, 134-35 (2015) (indicating that there are two types of risk structure associated with cyber insurance, the risk the organization takes on and the transfer of that risk to the insurer through cyber insurance).

[75] *See* Talesh, *supra* note 2, at 419 (claiming that there are over 120 insurance companies that are writing cyber insurance policies as of 2015).

[76] *See* Geraldine Grones, *Top 10 cyber insurance companies in the US*, INS. BUS. AM. (Dec. 20, 2019), *archived at* https://perma.cc/NW69-V968 [hereinafter *cyber insurance companies*] (revealing that that insurance companies such as AIG and AXA, who generally focus on insuring financial services institutions, are some of the largest cyber insurers today).

data breach occurrs, cyber insurance policies also allow insurance companies to act as compliance managers to the companies that they insure.[77] This is because insurance companies have an incentive to improve the risk management techniques of the companies they insure, for better security measures means less breaches, and less breaches means less claims the insurance company must face.[78]

The private sector has increasingly endured risks of security breaches, while the public sector has not turned to cyber insurance.[79] For example, New York passed regulation in 2017 that required organizations operating under New York Banking Law, Insurance Law, or Financial Services Law to sustain a far-reaching cybersecurity program.[80] The implementation of programs like those required under New York Banking Law creates incentives for companies to have a direct role in implementing cyber security measures.[81] However, many government entities have not implemented cybersecurity systems, thus increasing the risk to personal data they process or

[77] *See* Talesh, *supra* note 2, at 420 (contending that "institutionalized risk management techniques developed within the insurance field can potentially improve organizational practices and compliance concerning data breach").
[78] *See id.* (describing how cyber insurance can incentivize better cybersecurity practices in insured organizations); *see also* Rockenbach, *supra* note 6, at 574 ("There 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.").
[79] *See* Brendan Heath, *Before the Breach: The Role of Cyber Insurance in Incentivizing Data Security*, 86 GEO. WASH. L. REV. 1115, 1128 (2018) ("The most direct way for the government to incentivize data security is to issue laws and regulations simply mandating the desired standards."); *see also* Williams, *supra* note 28 (affirming that the government does not have cyber insurance largely due to their obsolete operating systems and technology that create too much risk).
[80] *See* Heath, *supra* note 79, at 1128 (exhibiting that "New York State regulations effective March 1, 2017, require entities operating under the purview of New York Banking Law, Insurance Law, or Financial Services Law to maintain a comprehensive cybersecurity program that includes maintaining a written policy, chief information security officer, and data-breach response plan."); *see also* N.Y. Comp. Codes R. & Regs. tit. 23, §500.01-500.04, 500.16, 500.21 (2017) (citing the cybersecurity requirements for financial services companies).
[81] *See* Heath, *supra* note 79, at 1128–29 ("Having such specific requirements can potentially affect corporate governance as a whole, requiring directors and officers of covered companies to take a direct interest in implementing the cybersecurity standards."); *see also* Kosseff, *supra* note 72, at 417–18 (suggesting that cyber insurance can help businesses mitigate risk and encourage them to further invest in cybersecurity).

store.[82] Not only is the New York regulation the first of its kind in the country, but the financial burden this regulation puts on the entities that use it is still relatively unknown.[83] Recently, the National Rural Electric Cooperative Association, a lobby, suggested a less regulatory approach, as they voiced their opinion that the Terrorism Risk Insurance Program should extend to cover cyberattacks.[84] Governmental entities have neither adopted cybersecurity programs nor secured insurance to provide compensation for the victims of breach.

E. Cyber Taxes: An Uphill Battle

The proposal that a cyber tax be assessed to directly compensate the victims of governmental data breaches has not yet been proposed as a solution to remedy the problem of governmental data breaches.[85] However, the idea of providing tax incentives for cybersecurity is something that scholars have looked towards as a potential solution to increase cybersecurity measures nationwide.[86]

---

[82] *See* Heath, *supra* note 79, at 1129 (stating that a downside of this regulation is the uncertainty that comes with it).

[83] *See id*. (revealing that "certain key provisions, such as encryption requirements for data in transit and at rest, are flexible – the covered entity's chief information security officer may approve 'effective alternate compensating controls' if he or she determines that encryption is infeasible.").

[84] *See id*. at 1135 (discussing different approaches to the government's involvement in cyber security); *see also Our Organization*, AM.'S ELEC. COOP. (Jan. 31, 2020), *archived at* https://perma.cc/2GSK-RTHX (explaining that the NRECA represents consumer owned, not-for-profit electric cooperatives, public power districts, and public utility districts in the United States on matters such as, federal government relations and economic and technical research).

[85] *See* Nicholas F. Palmieri III, *Data Protection in an Increasingly Globalized World*, 94 IND. L. J. 297, 324 (2019) (asserting that "the United States has still not passed comprehensive national data protection legislation," but instead turned to alternative methods of enforcement: "self-regulation within the private sector and reliance on the Federal Trade Commission (and its broad authority) as the de facto cybersecurity agency"); *see also* Kosseff, *supra* note 72, at 401 (stating that there is not "a single U.S. law that comprehensively addresses cybersecurity").

[86] *See* Matwyshyn, *supra* note 69, at 494 (suggesting that "[e]ven if only a portion of the companies currently manufacturing vulnerable Internet of Things devices improve their security practices as a result of a tax incentive, a significant aggregate risk mitigation for national security results."). Furthermore, "the IRS might propose a series of tax incentives to assist small businesses in affording access to security consultants, part-time CISOs, penetration testers and other security professionals." *Id.* at 494–95. *See also* Palmieri, *supra* note 85, at 301

One scholar recommends that the federal government enact a tax incentive program for smaller businesses while making cyber insurance mandatory for larger businesses handling larger quantities of data.[87]

However, the federal government is reluctant to take steps towards implementing a tax incentive for cybersecurity because of the notion that this would cause a decrease in revenue.[88] The financial cost of implementing a tax incentive would result in cost-savings and a compensation fund for the direct victims harmed by governmental data breaches.[89]

The federal government could implement tax incentives for cybersecurity by offering tax credits to companies that invest in their cybersecurity or tax credit for entities that invest in cybersecurity companies.[90] Another option is that the federal government could aid victims of cyberattacks through a government fund.[91] Additionally, a

(indicating that "the creation of various tax incentives for companies to properly invest in and maintain cybersecurity infrastructure" is an alternative that would instead of "retroactively punishing companies for not properly protecting personal data, companies are proactively encouraged to establish adequate security measures with the knowledge that they can receive certain tax breaks or other benefits in return").

[87] *See* Tucker, Jr., *supra* note 62, at 15–16 (illustrating that in order to "make cybersecurity insurance premiums available to smaller businesses, the Federal government could establish a compulsory regime for larger businesses and tax breaks for smaller businesses," and that "[a]s it becomes more mainstream, even required by Federal law, consumers may eventually benefit from the provided or expected coverage").

[88] *See* Kosseff, *supra* note 72, at 415 (revealing that "[i]n response to an Executive Order directing departments to analyze potential cybersecurity policies, the Treasury Department wrote that Tax Incentives for cybersecurity 'would come at the expense of forgone revenue for the government or reallocation of existing fiscal obligations,' and recommended against further consideration of tax incentives").

[89] *See id.* at 416 (suggesting that "tax incentives could dramatically increase companies' investments in cybersecurity safeguards, preventing costly data breaches and stimulating economic growth"). Furthermore, an Atlantic Council report estimates that a fully secure Internet would lead to a net global economic net gain of $190 trillion. *Id*.

[90] *See id.* 416 (outlining the different ways that the government could implement a tax incentive for cybersecurity); *see also* Matwyshyn, *supra* note 69, at 493 (suggesting that the IRS implement a series of tax incentives to help smaller businesses afford cybersecurity infrastructure).

[91] *See* Kosseff, *supra* note 72, at 417–18 (pointing to the National Flood Insurance Program that Congress enacted as a model for a cyberattack relief program); *see also* Christine M. McMillan, *Federal Flood Insurance Policy: Making Matters Worse*, 44 HOUS. L. REV. 471, 479 (2007) (explaining that "under the NFIA, the

government cybersecurity insurance program could be organized like the National Flood Insurance Program, which paid out $17.8 billion after Hurricane Katrina.[92] Other commentators have suggested different models, such as an excise tax-like structure similar to the National Vaccine Injury Compensation Program.[93] Also, the Terrorism Risk Insurance Program provides another example of how the government can enter the insurance market in order protect its

federal government makes flood insurance available to communities if their state implements floodplain regulations consistent with federal standards"); *see also* Oliver A. Houck, *Rising Water: The National Flood Insurance Program and Louisiana*, 60 TUL. L. REV. 61, 64 (1985) (affirming that "the program requires participating local governments to regulate future development of their high-hazard areas in order to reduce future damages when the waters next rise").

[92] *See* Kosseff, *supra* note 72, at 417–18 (proffering that "if implemented properly, the program would help businesses mitigate risk, while encouraging companies to invest in cybersecurity infrastructure services."). Additionally, "such a program would not only benefit businesses, but it would be a net win for the American public, as the cyber security safeguards would result in fewer cybersecurity incidents." *Id*. For context, "Congress enacted the NFIP in 1968 to address concerns about building homes on rivers and other flood plains." *Id*. "NFIP flood insurance is available to property owners in communities that have adopted minimum floodplain management regulations that help to minimize the likelihood that a building would be damaged or destroyed in a flood." *Id*. *See also NAR Background: National Flood Insurance Program (NFIP)*, NAT. ASS'N. REALTORS (Feb. 29, 2020), *archived at* https://perma.cc/9JR5-TQ6A [hereinafter *NAR Background*] (revealing that the NFIP is 30 billion dollars in debt to the Treasury, and that the program had to borrow from the taxpayers in recent years). The NFIP is an alternative to taxpayer-funded disaster relief, as it is "purchased through private insurance companies but administered by the Federal Emergency Management Agency (FEMA) which sets rates and coverage terms." *Id*.

[93] *See* Bier, *supra* note 33, at 1821 (stating that The National Vaccine Injury Compensation Program ("VICP") makes "payments to remedy vaccine-related injury or death," and funding is "supplied via a seventy-five percent excise tax per vaccine dose, paid by the recipient of the vaccine, and directed" to a fund covering the VICP). Unlike a tax incentive system that worried the Treasury Department, with a program like this one neither congress nor Treasury loses money. *Id*. Additionally, if an excise tax-like system were implemented, Bier suggests that "firms that retain certain types of customer data will pay a small tax for every user." *Id.* at 1836. Furthermore, "[a] small excise-type tax on users will ensure the fund remains viable." *Id*. Moreover, "when businesses sell blocks of customer data to other businesses, customer data is exposed to greater risk," so "to account for this increased risk, firms engaging in such types of transaction should compensate the Fund accordingly." *Id*. *See also Excise Tax*, INVESTOPEDIA, (Jan. 19, 2020), *archived at* https://perma.cc/ZY8A-3J9F (defining an excise tax as "a legislated tax on specific goods or services at purchase").

citizens from unpredictable attacks.[94] No matter how the government decides to get involved, it must, and today there are many ways that the government can begin to both make victims whole again and protect its citizens from the inevitability of a cyberattack.

IV. Analysis

A. Cyberattacks Create the Need for a Protection Plan

In a society that is becoming increasingly intertwined with technology, a focus on protecting consumers is paramount.[95] No organization is safe from a cyberattack, as breaches occur across a gamut of organizations; however, targeted organizations can separate themselves in their ability to respond to a cyberattack.[96] Given that the implementation of cybersecurity measures may not entirely prevent these attacks, obtaining cyber insurance will mitigate risk and give the

[94] *See* Heath, *supra* note 79, at 1135 (noting that the Terrorism Risk Insurance Act of 2002 is an example of how the government can participate in the insurance market). *See also* Bier, *supra* note 33, at 1834 (revealing that "funds were created to compensate victims of the September 11 terrorist attacks and workers injured on the job[,]" and that "victim funds have even been proposed in the data-breach context.").

[95] *See* Talesh, *supra* note 2, at 418 (citing that "The number of data breaches tracked by the Identity Theft Resource Center (ITRC) in 2015 was 781, the second highest year on record since the ITRC began tracking breaches in 2005 (ITRC 2016)."). "These breaches affect virtually every major industry, including, but not limited to, financial services, health care, government, entertainment, online gaming, retail, law, insurance, social networking, and credit card processing." *Id*. *See also* De Groot, *supra* note 1 (revealing that according to Computer Sciences Corporation, by 2020 over a third of data will live or pass through the cloud and data generation will increase by 4,300 percent). *See also* Digrazia, *supra* note 50 (highlighting how connected consumers are through smart devices). Referencing the Equifax breach where "hackers were able to access 'people's names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers.'" *Id*. *See also* Kim, *supra* note 52 (explaining how often data breaches occur, and what happens to consumer data when they occur at private companies).

[96] *See* Talesh, *supra* note 2, at 418 (indicating that recent reports reveal that cyberattacks yielding a data breach regularly cost the breached organization between 3 and 7 million dollars); *see also* Rockenbach, *supra* note 6, at 556 (stating that cyberattacks are perhaps the greatest national threat to the United States). Large quantities of wealth are lost annually to cyberattacks. *See* Rockenbach, *supra*. *See* Miller, *supra* note 71, at 161 (explaining that cyber insurance has been around for about 50 years, but it is still not that well known to the average American). "A 2017 report by McAfee estimates that cyberattacks cost approximately $ 400 [sic] billion annually for companies and governments across the globe." *Id.* at 152.

direct victims a monetary remedy for the consequences of these inevitable breaches.[97]

While cyber insurance is relatively effective in mitigating some of the financial consequences of a breach, there is no requirement that entities obtain coverage.[98] Next, this Note will explore three possible government taxes and programs that could possibly remedy this: A Social Security-like payroll tax, a cyber excise tax, and a taxpayer alternative in the form of a federally funded insurance program.

B. Cyber Insurance Works for the Private Sector

Cyber insurance is extremely expensive and its effectiveness not widely known.[99] The uncertainty about the cost and effectiveness of cyber insurance makes organizations hesitate when debating whether to acquire it.[100] To date, courts have frequently ruled that cyber insurance policies do not cover cyber breaches.[101] It is unclear whether obtaining cyber insurance is a cost-effective solution given

[97] *See* Talesh, *supra* note 2, at 419 (explaining that "[c]yber insurance is insurance designed to provide both first-party loss and third-party liability coverage for data breach events, privacy violations, and cyber attacks."). One in three organizations have cyber insurance. *Id. See also* Trang, *supra* note 10, at 415–16 (detailing that "cyber-insurance has the potential to protect not just the breached company, but also millions of consumers."); *see also* Dignan, *supra* note 7 (indicating that after the 2017 Equifax breach, their cyber security policy covered over 95 million dollars in costs). "Equifax's 2017 data breach impacted 145.5 million US consumers whose personally identifiable information was impacted by an attack. In March 2018, Equifax disclosed that 2.4 million more US consumers were impacted." *See* Dignan, *supra* note 7. Equifax "maintain[s] $125.0 million of cybersecurity insurance coverage, above a $7.5 million deductible, to limit [their] exposure to losses such as those related to the 2017 cybersecurity incident." *Id.*

[98] *See* Rockenbach, *supra* note 6, at 587 (confirming that obtaining cyber insurance can prove a daunting task because "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.").

[99] *See* Rockenbach, *supra* note 6, at 587 (outlining that "insurers serve well as regulators of cyber risk, but this engagement and the overwhelming nature of the risk has led cyber insurance to be expensive.").

[100] *See id*. at 587–88 (affirming the expense and unproven nature of cyber insurances causes organizations to waver in acquiring it).

[101] *See* Talesh, *supra* note 2, at 419 (claiming that there are over 120 insurance companies that are writing cyber insurance policies as of 2015); *see also* Collins, *supra* note 13 (explicating that "[j]udicial treatment of policy provisions continues to evolve, and while existing precedent decided on other lines of coverage may provide some guidance, courts have yet to interpret many key cyber insurance policy provisions.").

the tendency of courts to rule that there is no coverage of foreseeable security breaches.[102] While there are only a few decided cases, there is a swirl of uncertainty over the value of cyber insurance, and the cost has been driven up by recent class action lawsuits sought by breach victims.[103]

However, the growing cost of cyber insurance and its uncertain value do not outweigh the benefits of coverage.[104] Cyberattacks and data breaches can cost affected organizations millions, if not billions, of dollars directly—not to mention the residual effects such as loss of consumer trust that undermine an organization's reputation.[105] Therefore, it is critical that organizations protect both themselves and their customers, and cyber insurance is the most effective way to do this in the private sector.[106] While the private sector is using cyber

[102] *See* Trang, *supra* note 8, at 406 (citing that "insurance products and the applicable law have not been 'keeping pace with the emergent ubiquity of information technology in commercial enterprises.'"); *see also cyber insurance companies*, *supra* note 76 (listing insurance companies such as AIG and AXA, who generally focus on insuring financial services institutions, but comprise some of the largest cyber insurers today); *see also* State Auto Prop. & Cas. Ins. Co. v. Midwest Computs. & More, 147 F. Supp. 2d 1113, 1116 (W.D. Okla. 2001) (holding that "computer data cannot be touched, held, or sensed by the human mind; it has no physical substance. It is not tangible property.").

[103] *See* Collins, *supra* note 13 (revealing that "[c]ourts have reached varying results when determining coverage for cyber-related losses under computer fraud provisions in crime/fidelity policies."). Also, "[t]here is not yet a significant body of case law interpreting cyber insurance policies." *Id.* "These policies typically include first and third-party coverage for network security and data privacy events, and there are a wide variety of coverage options available." *Id. See* Rockenbach, *supra* note 6, at 584 (stating that "[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." *Id.* at 587. "Increased regulation and the recent success of class action suits will lead to further increases." *Id.* Target and Anthem faced a tripling of insurance premiums after breaches. *Id.* at 587–88. Anthem agreed to a $ 25 million deductible in order to obtain $ 100 million in limits. *Id.*

[104] *See* Trang, *supra* note 6, at 415–16 (detailing that "cyber-insurance has the potential to protect not just the breached company, but also millions of consumers. Cyber risks have high potential damages that may put a company out of business.").

[105] *See* Martinez, *supra* note 43 (proffering that a data breach will generally cost a small business around three million dollars in addition to indirect losses stemming from damaged reputation and lost trust); *see also* Dignan, *supra* note 7 (predicting that Marriot's breach will cost them billions of dollars).

[106] *See* Dignan, *supra* note 7 (demonstrating that companies such as Equifax, for example, have had cyber insurance policies that covered a large portion of the expenses that resulted from a breach).

insurance on a large scale, government entities are still far behind in this space, and the impact this lag is having on American citizens is dangerous.[107]

C. Cyber Insurance is Not Viable for Government Entities

In the private sector, consumers have a choice of where they spend their money and share their data, but they do not have such a choice in disclosing such data to governmental entities.[108] In recent years, the public sector has been targeted for data intrusions by cybercriminals more than the private sector.[109]

Consumers have a choice whether to share data with a private entity, but this is not so with the federal government.[110] In contrast, all Americans have a duty to disclose information to the government.[111] The government does not have a corresponding duty to protect this

[107] *See* Rockenbach, *supra* note 6, at 571 (proclaiming that the United States public law response to cyber risk is historically inadequate). Additionally, "[c]urrent public law has three glaring deficiencies: it is overly voluntary, it is overly reactive, and it lacks involvement of the national security infrastructure. *Id. at* 573. These deficiencies have rendered the public law structure largely ineffective. *Id.* "There 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." *Id. at* 574. *See* Trang, *supra* note 8, at 405 (declaring that "[c]urrently, the insurance market views cyber risk as 'a risk like no other' because of limited publicly available data and the quick evolution and proliferation of threats. Quick growth in threats is why annual gross written premiums are expected to increase from $ 2.5 billion to $ 7.5 billion by the end of the decade."); *see also* Talesh, *supra* note 2, at 419 (suggesting that "[r]ecent estimates suggest that the global insurance market collected approximately $ 2 billion in cyber insurance premiums and that this will rise by a magnitude of three to five times by 2020.").

[108] *See* Froomkin, *supra* note 56, at 1022 (affirming that "[g]overnments hold a wide variety of data on natural and legal persons, great both in scope and in scale."). "Private data held by the government is not the same as private data held by others. Much of the government's data is obtained through legally required disclosures or participation in licensing or benefit schemes where the government is, as a practical matter, the only game in town." *Id. at* 1019.

[109] *See* Ratnam, *supra* note 55 (highlighting that the government sector had the most breaches in 2018).

[110] *See* Froomkin, *supra* note 56, at 1021 (alleging that "the remedies available to victims of a government data breach are often less than those available to victims of private sector data breaches").

[111] *See* Williams, *supra* note 28 (highlighting that government "agencies lack the systems, technical expertise and personnel to secure high-value data such as personal and financial information to current industry standards").

data, obtain cyber insurance or provide compensation to the victims of data breaches.[112] Even more perplexing, the government has understood the risk of cyberattacks for decades, but has failed to take any substantial action to protect itself and potential victims.[113] In recent history, government data breaches have manifested as more than just a monetary burden to victims, and carry even more potentially dire consequences.[114] While cyber insurance coverage is an increasingly valuable tool in the private sector, a requirement that government entities obtain cyber insurance is impractical.[115] The cost of cyber insurance for governmental entities would be exorbitant as their security and technologies for storing and processing data are out of date.[116] The cost of cyber insurance coupled with the unlikelihood that insurers would issue policies means government entities obtaining privatized insurance is not the answer.[117]

---

[112] *See* Froomkin, *supra* note 56, at 1021 (alleging that the government does not have adequate remedies for the victims of data breaches that occur on their watch).
[113] *See* Rockenbach, *supra* note 6, at 571 (articulating that "[g]overnment 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."). *See* Rockenbach, *supra.* (noting that "computer viruses date to the 1990s."). "By the late 1990s, business losses to security breaches ranged into the hundreds of billions. Cyber insurance policies began to appear by the late 1990s." *Id.*
[114] *See* Marcus, *supra* note 57, at 557 (revealing that a data breach in Utah in 2012 resulted in the exposure of the personal information of 800,000 citizens of Utah); *see also* Kim, *supra* note 52, at 548 (referencing a New York State data breach that resulted in the exposure of 22.8 million private records of New Yorkers over an eight year period); *see also* DSM, *supra* note 61 (indicating that the State Department faced a data breach within its cloud-based email service that exposed personal information of employees); *see also 10,000 BREACHES LATER*, *supra* note 65 (detailing that United States Postal Service's issued an alert that cybercriminals were using the Informed Delivery feature to commit fraud and identity theft); *see also* Horton, *supra* note 68 (noting that "sensitive information about hundreds of immigrant recruits from nations such as China and Russia … could aid hostile governments in persecuting them or their families").
[115] *See* Williams, *supra* note 28 (denoting that because the government has antiquated cyber security systems insurers would be extremely unlikely to insure government agencies, and if they did, the coverage would be too expensive).
[116] *See id*. (highlighting that government "agencies lack systems, technical expertise and personnel to secure high-value data such as personal and financial information to current industry standards").
[117] *See id*. (suggesting that government agencies do not have cyber insurance because governments "have a hard time accurately describing the details of how their data is secured to the satisfaction of insurers," and "the level of protection does not match the value of what" the cyber insurance providers would protect).

However, the government should attack this problem by implementing a payroll like tax to support a cyber insurance program to benefit government entities, and as a direct result, United States citizens.[118] Considering that the remedies for data breaches are distressingly insufficient, and attempts of breached public or private entities do not make the victim whole, the implementation of some sort of federal tax or fund could bridge that gap.[119]

D. Inevitability: How Social Security Provides a Path for a Cyber Tax

In 2017, New York enacted a regulation requiring that organizations operating under New York Banking Law, Insurance Law, or Financial Services Law to maintain a robust cybersecurity program.[120] While this regulatory solution may work well in the private sector, it is unlikely to be effective in the public sector.[121] If the federal government were to use a proven system such as the payroll tax, there is less uncertainty.[122] Implementing a payroll tax for programs like Social Security makes sense because the purpose of Social Security is to ensure everyone who retires is protected

[118] *See* Heath, *supra* note 79, at 1128 (theorizing that "the most direct way for the government to incentivize data security is to issue laws and regulations simply mandating the desired standards"); *see also* Talesh, *supra* note 2, at 420 (suggesting that "institutionalized risk management techniques developed within the insurance field can potentially improve organizational practices and compliance concerning data breach").

[119] *See* Tucker, Jr., *supra* note 62, at 19 (stating that typically, breached entities offer identity and credit monitoring services in an attempt to make victims whole again); *contra* Bier, *supra* note 33, at 1821 (countering that many organizations do not offer any recourse, and victims have had to take matters into their own hands, and as a result make out-of-pocket purchases for credit card monitoring services or freezes on credit reports).

[120] *See* Heath, *supra* note 79, at 1128 (exhibiting that "New York State regulations effective March 1, 2017, require entities operating under the purview of New York Banking Law, Insurance Law, or Financial Services Law to maintain a comprehensive cybersecurity program that includes maintaining a written policy, chief information security officer, and data-breach response plan.").

[121] *See id.* (suggesting that while this regulatory approach works in the private sector, the financial burden it imposes is still unknown, and would likely not be viable in the public sector).

[122] *See id.* (stating that one of the downsides of this regulation is the uncertainty that comes with it); *see also* Geier, *supra* note 34, at 2 (asserting "nearly two-thirds of American households now pay more in federal payroll taxes than income taxes.")

financially.[123] Similarly, given that nearly all American citizens will face a cyberattack to some extent in their life, a cybersecurity tax should be implemented akin to the Social Security tax.[124] Analogous to the Social Security system, if the government were to implement a payroll-like tax to support a cyber insurance program for government entities, American citizens could depend on the program's benefits when, not if, they are impacted by a cyberattack.[125]

Furthermore, unlike Social Security, where many American citizens often do not live to see its benefits, it is very likely that citizens would reap the benefits on multiple occasions of a payroll tax supporting a nationwide cyber insurance program and relief fund.[126] Also, employers contribute to Social Security as well, and so companies dealing with large amounts of data would also contribute to the nationwide cyber insurance fund under a Social Security-like payroll tax.[127] Therefore, if modeled after Social Security, a 6.2% tax on the gross wages or salary of the worker and 6.2% collected from

[123] *See* Buchanan, *supra* note 34, at 252 (explaining how social security works to help citizens with their inevitable retirement); *see also Social Security Act*, *supra* note 41 (indicating that Americans rely on Social Security as part of their retirement planning).

[124] *See* Buchanan, *supra* note 34, at 250 (citing the creation of Social Security and noting that "Social Security, therefore, also provides protection for the rest of society from those who would fail—due to excess optimism, myopia, or any other reason—to protect themselves with adequate income for their entire lives."). "Even those who are willing and able to save for their retirements can fail to protect themselves adequately; and when their plans—or their failure to plan—puts them in difficult financial straits, it is the rest of society that will pay." *Id.* "The Social Security system provides an additional kind of safety net: protection against running out of money before death." *Id.* at 252.

[125] *See id.* at 254 (demonstrating that "the Social Security system has become an essential part of people's long-term financial planning," and "Social Security benefits are now a bulwark supporting the consumption expenditures that prop up the U.S. economy").

[126] *See Social Security Act*, *supra* note 41 (stating that "Still, despite attempts to keep it solvent, Social Security faces a major long-term shortfall. The retirement age to receive full benefits continues to increase and many beneficiaries are claiming benefits much later in life to receive maximum payouts, often at age 70."). Additionally, "despite the program's pitfalls, most Americans want Social Security to continue and consider it a retirement lifeline, according to a National Academy of Social Insurance survey." *Id.* "And eighty-one percent of them are willing to pay more taxes to ensure it. Whether politicians are listening and can come up with a viable solution remains to be seen." *Id. See also* Gredler, *supra* note 64 (illustrating that in 2016 the DOJ found that the average cost of identity theft to the victim is $1,343).

[127] *See* Buchanan, *supra* note 34, at 252 (clarifying that the payroll tax collects the gross wages of both the employee and employer).

the employer would contribute a significant amount of capital to the fund.[128] Upon a breach, the government can use these funds, to a certain predetermined cap, to help remedy victims' damages.[129] The United States has the ability to implement a regressive tax, similar to the one used in the Social Security System, to support a cyber insurance program and relief fund, and doing so would greatly improve the efficiency of the government.[130] Finally, the fund would help bridge the gap between available remedies and what is needed to make victims whole after a cyberattack on the government.

E. Cyber Excise Tax to Create a Relief Fund

While the Social Security System model might have some citizens claiming that it is not fair that they have to pay for cyber relief when they use a fractional amount of data compared to large companies, a federally mandated excise tax on cyber-related transactions could remedy this situation.[131] For instance, a large company such as Facebook would pay a small tax for each user.[132] Moreover, companies that engage in buying or selling consumer data should have to pay a higher excise tax to reflect the inherent risk associated with the action.[133] Additionally, for the successful

[128] *See id*. (advising that "The payroll tax rate is constant rather than graduated currently 12.4%, with 6.2% collected from the gross wages or salary of the worker and 6.2% collected from the worker's employer.").
[129] *See id*. (suggesting that the government could use the funds collected in a payroll tax for cyberattacks to compensate victims).
[130] See *id.* at 285–86 (explaining that a regressive tax is used to support the Social Security System); *see also* Kagan, *supra* note 34 (defining a regressive tax as "a tax applied uniformly, taking a larger percentage of income from low-income earners than from high-income earners. It is in opposition to a progressive tax, which takes a larger percentage from high-income earners").
[131] *See* Bier, *supra* note 33, at 1835 (stating that if an excise tax-like system were implemented, Bier suggests that "firms that retain certain types of customer data will pay a small tax for every user"); *see also Excise Tax*, *supra* note 93 (defining an excise tax as "a legislated tax on specific goods or services at purchase").
[132] *See* Bier, *supra* note 333, at 1835 (proffering that companies that deal in consumers' data should have to pay a tax for each user or customer that would contribute to a relief fund); *see also Excise Tax*, *supra* note 993 (explaining that "consumers may or may not see the cost of excise taxes directly").
[133] *See* Bier, *supra* note 33, at 1835 (considering that "when businesses sell blocks of customer data to other businesses, customer data is exposed to greater risk," and in order to account for this risk, companies engaged in these transactions would have a higher excise task on each transaction); *see also* Cohen & Morril, *supra* note

execution of a cyber excise tax, and in order for it to promote better cybersecurity, firms that do not have cybersecurity measures meeting certain government standards would have to pay a higher excise tax.[134]

Because consumers would principally benefit from a fund created through a cyber-related excise tax, they should not remain unaccountable; consequently, there should be a tax on the purchase of any cyber-related device, such as an iPhone, that contributes to the relief fund as well.[135] One of the main strengths of a system such as this one is its self-sufficiency, for similar to the National Vaccine Injury Compensation Program where funding is supplied via a seventy-five cent excise tax per vaccine dose, a tax on every cyber-related transaction could easily fund the program.[136] Furthermore, unlike tax incentives for cybersecurity, an excise tax system would not take money away from Congress or the Treasury.[137] However, in implementing a cyber excise tax, a major concern is that companies and consumers may attempt to cut back on technology in order to avoid paying taxes, and this could stunt technological advances in all aspects.

6, at 983 (stating that cyberattacks are "increasingly pervasive against corporations, law firms, government agencies and officials and other custodians of large electronic data sets of sensitive information").

[134] *See* Bier, *supra* note 333, at 1835 (suggesting that companies that do not have proper cybersecurity standards should be subject to civil money penalties); *see* Heath, *supra* note 779, at 1128 (claiming that in order to incentivize data security the government should pass legislation requiring companies have cybersecurity that meets certain standards).

[135] *See* Digrazia, *supra* note 550, at 255 (illustrating how connected consumers are to their smart devices today); *see also* Talesh, *supra* note 2, at 418 (explaining that societies reliance on communication through electronic devices and constant connectivity creates increased risk for cyberattacks).

[136] *See* Bier, *supra* note 333, at 1821 (stating that The National Vaccine Injury Compensation Program ("VICP") makes "payments to remedy vaccine-related injury or death," and funding is "supplied via a seventy-five cent excise tax per vaccine dose, paid by the recipient of the vaccine, and directed" to a fund covering the VICP).

[137] *See* Kosseff, *supra* note 72, at 415 (revealing that "[in] response to an Executive Order directing departments to analyze potential cybersecurity policies, the Treasury Department wrote that Tax Incentives for cybersecurity 'would come at the expense of forgone revenue for the government or reallocation of existing fiscal obligations,' and recommended against further consideration of tax incentives.").

F. An Alternative to Tax: A Government Sponsored Cyber Insurance Program

Likely the last thing the American public would like to hear is that yet another tax is necessary, so a government sponsored cyber insurance program as an alternative could bring protection and remedy to citizens in the event of a cyberattack.[138] Similar to the National Flood Insurance Program, Congress could enact a cyber insurance program that is purchased through private insurance companies, but where rates and coverage terms are set by a federal agency.[139] Companies would need to have a certain, government determined, level of cybersecurity in order to qualify to purchase the cyber insurance program, and this would incentivize businesses to bolster their cybersecurity systems.[140]

However, unlike floods, cyberattacks occur at an unrelenting rate, and given that the NFIP is 30 billion dollars in debt to the treasury, mainly as a result of Hurricane Katrina, one Marriot-like breach could cripple a program like this, putting the burden right back on the taxpayers.[141] Considering that the average cost of a breach for an organization is between three and seven million dollars, and that in 2015, the Theft Resource Center reported there were 781 data breaches, more than roughly three-and-a-half trillion dollars in losses

---

[138] *See id.* at 418 (hypothesizing that "if implemented properly, the program would help businesses mitigate risk, while encouraging companies to invest in cybersecurity infrastructure services," and "[s]uch a program would not only benefit businesses, but it would be a net win for the American public, as the cybersecurity safeguards would result in fewer cybersecurity incidents.").

[139] *See id.* at 417–18 (pointing to the National Flood Insurance Program that Congress enacted as a model for a cyberattack relief program). *See also NAR Background*, *supra* note 92 (describing that the NFIP is purchased through private insurance companies, but the Federal Emergency Management Agency sets the rates and coverage terms).

[140] *See* Kosseff, *supra* note 72, at 418 (proffering that "[s]uch a program would not only benefit businesses, but it would be a net win for the American public, as the cyber security safeguards would result in fewer cybersecurity incidents.").

[141] *See NAR Background*, *supra* note 92 (revealing that the NFIP is 30 billion dollars in debt to the Treasury, and that the program had to borrow from the taxpayers in recent years). The NFIP is an alternative to taxpayer-funded disaster relief, as it is "[p]urchased through private insurance companies but administered by the Federal Emergency Management Agency (FEMA) which sets rates and coverage terms." *Id. See also* Dignan, *supra* note 7 (indicating that Marriot's breach will likely cost billions of dollars).

exist annually.[142] The likelihood of a government sponsored cyber insurance program, or even a backstop program for insurance claims related to cyberattacks, like the Terrorism Risk Insurance Act, covering losses of this size is close to impossible.[143] Therefore, a federal relief fund, akin to the September 11th Victim Compensation Fund, for cyber insurance is likely financially impracticable because of both the colossal amount of money cyberattacks cost and how frequently they occur.[144] Thus, while the idea of an alternative to the expenditure of more taxpayer dollars is appealing, it likely will not work, and the taxpayers will inevitably end up supporting the program with their own hard earned dollars.

G. A Tax Would Create More Efficient Government Cybersecurity Systems

Similar to the improvement in cyber security that cyber insurance brings in the private sector, a cyber insurance program and relief fund in the government sector could potentially bring often archaic government technology up to speed.[145] In the event that the government did implement a new tax allowing for the creation of government protection through a broad cyber insurance program, the hope is that the government would attempt to dramatically improve its cyber security practices in order for the tax to yield efficient results to

[142] *See* Talesh, *supra* note 2, at 418 (stating that the average cost of a breach is between three and seven million dollars, and according to the Theft Resource Center there were 781 data breaches in 2015).
[143] *See* Heath, *supra* note 79, at 1135 (noting that the Terrorism Risk Insurance Act of 2002 works as a backstop for insurance claims coming as a result of a terror attack); *see* Talesh, *supra* note 2, at 418 (according to the Theft Resource Center (TRC), there were 781 data breaches in 2015, and this is the second highest year on record since the TRC began tracking in 2005).
[144] *See* Bier, *supra* note 33, at 1834 (revealing that "funds were created to compensate victims of the September 11 terrorist attacks and workers injured on the job," and that "[v]ictim funds have even been proposed in the data-breach context"); *see also* Miller, *supra* note 71, at 152 (explaining that 2017 McAfee report estimates cyberattacks cost approximately $ 400 billion annually for companies and governments globally).
[145] *See* Williams, *supra* note 28 (highlighting that government "agencies lack the systems, technical expertise and personnel to secure high-value data such as personal and financial information to current industry standards."); *see also* Talesh, *supra* note 2, at 420 (implicating that cyber insurance works as an incentive to better risk management techniques and improve the cyber security policies of organizations that insurers insure).

the American citizens and keep the tax level low.[146] Still, there is always the risk that a payroll tax does not incentivize an improved cyber security system in the United States, but instead a tax, meant to help the American people, results in another hole in their wallet and the very same level of inadequacy from the government in responding to cyberattacks and protecting American citizens.

V. Conclusion

A payroll tax, similarly structured to the one used in the Social Security System, to create a broad cyber insurance program that includes a relief fund is the best way to provide remedies to victims and bolster American cybersecurity practices at the government level. Cyberattacks will occur, likely every person and organization in the United States will feel the impact of one at some point in their lifetime. Therefore, using a payroll tax akin to the one used in Social Security makes sense, for just as retirements occur, cyberattacks are also inevitable. A government plan for retirement exists, but citizens are left out in the cold by the government when they are victims of a cyberattack. While the feasibility of using this tax model to fund a broad cyber insurance program and relief fund still needs to pass the inspection of economists, accountants, policymakers and the like, it provides a solution to a glaring problem facing each and every citizen and entity in the United States.

[146] *See* Heath, *supra* note 79, at 1128–29 (reiterating that having such specific requirements regarding cyber security can potentially affect corporate governance as a whole, for directors and officers of covered companies may take a direct interest in implementing the cybersecurity standards); *see also* De Groot, *supra* note 1 (stating that "[s]ince 2011, however, the number of data breaches reported in the United States has been rising steadily[.]").