THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

VOL. XVIII STLR.ORG SPRING 2017

NOTE

AVOIDING CYBER-PEARL HARBOR: EVALUATING GOVERNMENT EFFORTS TO ENCOURAGE PRIVATE SECTOR CRITICAL INFRASTRUCTURE CYBERSECURITY IMPROVEMENTS[†]

James Eastman[*]

* J.D. Candidate, 2017, The University of Texas School of Law. I am grateful to Professor Ronald Sievert for his guidance throughout the writing process. I am also indebted to the members of the Columbia STLR for their thorough editing assistance. And finally, I would like to thank my mother and father for their love and never-ending support.

"Our country will, at some point, face a major cyber event that will have a serious effect on our lives, our economy, and the everyday functioning of our society."[1]

1. Jordy Yager, *Napolitano Warns Large-Scale Cyberattack on US is Inevitable*, THE HILL (Aug. 27, 2013, 2:50 PM), http://thehill.com/policy/technology/318937-napolitano-warns-large-scale-cyber-attack-on-us-is-inevitable (warning given by Janet Napolitano toward the end of her tenure as the United States Secretary of Homeland Security).

I. INTRODUCTION: THE CURRENT STATE OF CYBERSECURITY IN THE UNITED STATES[2]

In 2013, hackers stole credit card information for over forty million customers from Target.[3] Several months before the breach, Target invested $1.6 million in a "malware detection tool," which had alerted Target that hackers had breached their computer systems.[4] But Target did nothing to prevent the hackers' completing the malware's installation.[5] After Target announced the breach, its profits dropped 46% from the amount reported in the same quarter the year before, revenue slumped 5.3%, and share prices fell 11%.[6] Target has incurred $148 million in breach-related costs to date, and that number is expected to increase as Target settles lawsuits with customers and banks over reissuing credit cards.[7] While investigations have not identified the attack's source, reports indicate that a seventeen-year-old Russian citizen created

2. *Cybersecurity*, MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY (11th ed. 2011) ("[M]easures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.").

3. *Data Breach FAQ*, TARGET.COM, https://corporate.target.com/about/shopping-experience/payment-card-issue-faq (last visited May 20, 2016).

4. Michael Riley, *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG (Mar. 17, 2014, 10:31 AM), http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data.

5. *Id.*

6. Susanna Kim, *Target (TGT) Profits Hit By Card Security Hack*, ABC NEWS (Feb. 26, 2014), http://abcnews.go.com/Business/target-profits-hit-card-security-hack/story?id=22680841; Maggie McGrath, *Target Profit Falls 46% on Credit Card Breach and the Hits Could Keep On Coming*, FORBES (Feb. 26, 2014, 9:21 AM), http://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/#33f6be405e8c.

7. Rachel Abrams, *Target Data Breach Costs at $148 Million, and Forecasts Profit Drop*, N. Y. TIMES (Aug. 5, 2014), http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html; Colin Lecher, *Target Will Face a Class-Action Lawsuit from Banks Over Data Breach*, VERGE (Sep. 16, 2015, 8:49 AM), http://www.theverge.com/2015/9/16/9336395/target-data-breach-banks-lawsuit-class-action.

the malware that infected Target's network, which he published on the Internet for any person to buy and use.[8]

In 2014, hackers stole account information of 83 million small businesses and households from JPMorgan.[9] Despite a $250-million expenditure to improve its cybersecurity, hackers breached a server that JPMorgan's security team had overlooked and failed to upgrade.[10] The security oversight was a simple flaw that JPMorgan's security team easily could have fixed, given the funds they had at their disposal.[11] Investigators linked the attack to a major crime syndicate involved in stock price manipulation and hacking-for-profit.[12]

In the same year, the U.S. government indicted five Chinese military hackers for hacking into several American private sector companies, including: Westinghouse Electric Co. (a nuclear power plant products and services provider), Allegheny Technologies Inc. (a specialty metals and components supplier for the aerospace and defense industries), and United States Steel Corp. (a major U.S. steel producer).[13] Later in 2014, the head of the National Security Agency, Admiral Michael Rogers, appeared before Congress and

---

8. Marie-Louise Gumuchian & David Goldman, *Security Firm Traces Target Malware to Russia*, CNN (Jan. 21, 2014, 5:50 AM), http://www.cnn.com/2014/01/20/us/money-target-breach.

9. Matthew Goldstein, Nicole Perlroth & Michael Corkery, *Neglected Server Provided Entry for JPMorgan Hackers*, N.Y. TIMES: DEALBOOK (Dec. 22, 2014, 8:41 PM), http://dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified.

10. *Id.*

11. *Id.* ("The computer breach at JPMorgan Chase this summer—the largest intrusion of an American bank to date—might have been thwarted if the bank had installed a simple security fix to an overlooked server in its vast network . . . .").

12. Jose Pagliery, *JPMorgan's Accused Hackers Had Vast $100 Million Operation*, CNN MONEY (Nov. 10, 2015, 5:27 PM), http://money.cnn.com/2015/11/10/technology/jpmorgan-hack-charges.

13. *See* Press Release, Dep't. of Just., U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor. *See generally Corporate Profile*, U.S. STEEL CORP., https://www.ussteel.com/uss/portal/home/aboutus/corporateprofile (last visited May 20, 2016) (giving general information about U.S. Steel); *About Westinghouse Nuclear*, WESTINGHOUSE ELEC. CO., http://www.westinghousenuclear.com/about (last visited May 20, 2016) (giving general information about Westinghouse Nuclear); *About ATI*, ATI METALS, https://www.atimetals.com/aboutati/Pages/default.aspx (last visited May 20, 2016) (providing general information about ATI Metals).

testified that "China and one or two other countries now have the ability to launch a cyberattack that could shut down the entire [U.S.] power grid," and that "[i]t is only a matter of when, not if . . . we are going to see something traumatic occur."[14]

Combined with Admiral Rogers' warning, these numerous breaches showcase some alarming truths about the state of American private sector cybersecurity. First, almost every sector of America's critical infrastructure ("CI") is exposed to serious cyberattacks that could cause severe monetary losses by affecting share prices and profits, as well as by creating litigation costs.[15] This poses a substantial threat to homeland security.[16] Second, in addition to monetary costs, the cyberattacks also pose a threat of potential physical damage to integral CI assets such as power grids.[17] Third, cyberattacks are carried out by a wide variety of different perpetrators, from cyber criminals to non-state and state actors.[18] And last, many successful cyberattacks like the Target and

---

14. Thomas R. Spencer, *Key Aspects of Evolving National Security Laws: Protecting Life and Property While Preserving Liberty*, *in* RECENT TRENDS IN NAT'L SEC. LAW 49, 71 (Thompson Reuters ed., 2015) (noting that while a cyberattack is unlikely to *directly* shut down the power for a large area due to the decentralized nature of individual power grids, grids are nonetheless vulnerable to "'cascading failures;' that is, as nearby grids take up the slack for a failed component, they become overloaded and fail in a chain of reactions.").

15. Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1506 (2013); *see* Exec. Order No. 13636, 3 C.F.R. § 13636 (2014), *available at* https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (last visited May 20, 2016) ("[T]he term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."); for a breakdown of sixteen sectors that encompass America's critical infrastructure, *see Critical Infrastructure Sectors*, DEP'T. OF HOMELAND SEC., https:// www.dhs.gov/critical-infrastructure-sectors (last visited May 20, 2016).

16. *Cybersecurity Overview*, DEP'T. OF HOMELAND SEC. (Sept. 27, 2016), https://www.dhs.gov/cybersecurity-overview.

17. Siobahn Gorman, *Electricity Grid in U.S. Penetrated by Spies*, WALL ST. J. (Apr. 8, 2009, 11:59 PM), http://www.wsj.com/articles/SB123914805204099085.

18. *See* Charles J. Demmer, *Proper Application of ADR Techniques Regarding Violent Non-State Actors*, 31 OHIO ST. J. ON DISP. RESOL. 207, 211–12 (2016); *see also* Charlotte Decker, *Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime*, 81 S. CAL. L. REV. 959, 964 (2008). The differentiation between cybercriminals, and non-state and state actors is important because government responses to attacks generally rely upon categorizing the enemy and designing an appropriate response. It would not make sense to consider, in the extreme,

JPMorgan breaches are the result of human error, such as ignoring red flags or neglecting to update servers.[19]

While cyberspace has benefited society tremendously as a source of education and innovation, the private sector's vulnerability to cyberattacks "represents one of the most serious national security challenges we must confront."[20] One reason is that America's private sector owns and operates 85% of America's CI.[21] This places it outside of the government's direct control and protection, thereby creating a substantial national security conundrum for the federal government.[22] The cyberattacks on Target (retail industry), JPMorgan (financial industry), and Westinghouse Electric Co. (nuclear industry) are representative of the multitude of cyberattacks that have penetrated America's private sector in recent years.[23] Fortunately, the private sector has

---

an act of war against a cybercriminal, whereas it might be appropriate against a state actor. Non-state actors "may refer to any association without nation-state status, which seeks to assert influence over international affairs," whereas a state actor is an actor acting on behalf of a government body. Demmer, *supra*, at 210. Cybercrime is typically not politically motivated as with state and non-state actor cyberattacks. Instead, "[t]he term 'cyber crime,' broadly defined as crimes 'perpetrated over the Internet, typically having to do with online fraud,' is generally thought to describe two main types of Internet-based behaviors: criminal activity targeting computers and the information stored on computers, and activities in which a computer is used to facilitate another, more traditional crime." Decker, *supra*, at 964.

19. *See* Evan M. Wooten, *The State of Data-Breach Litigation and Enforcement: Before the 2013 Mega Breaches and Beyond*, 24 COMPETITION: J. ANTI. & UNFAIR COMP. L. SEC. ST. B. CAL., no. 1, 2015, at 229, 230 ("[R]ecent data suggests that human error (35%) and system malfunction (29%) are nearly as common causes of data breach as malicious or criminal attacks (37%) . . . .").

20. The term "cyberspace" as used in this paper is defined as: "The interdependent network of information technology infrastructures, that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers." *Cyber Glossary*, U.S. DEP'T OF HOMELAND SEC.: NAT'L INITIATIVE FOR CYBERSECURITY CAREERS & STUDIES, https://niccs.us-cert.gov/glossary#c (last visited May 20, 2016); *see* Exec. Order 13636, *supra* note 15. In President Obama's 2013 Executive Order, he said that "[t]he cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront." Exec. Order 13636, *supra* note 15.

21. *Critical Infrastructure and Key Resources*, INFO. SHARING ENV'T, https://www.ise.gov/mission-partners/critical-infrastructure-and-key-resources (last visited May 20, 2016) ("The private sector owns and operates an estimated 85% of infrastructure and resources critical to our Nation's physical and economic security.").

22. *See id.*

23. *See* Kevin Granville, *9 Recent Cyberattacks Against Big Businesses*, N.Y. TIMES (Feb. 5, 2015),

not yet witnessed a cyberterrorist attack—it has only sustained monetary damages and loss of intellectual property.[24] But with another potentially devastating cyberattack looming on the horizon, cyberspace has become the new battleground of the twenty-first century.[25] As it stands now, America's CI is almost defenseless against such an attack.[26]

With America's CI exposed to a myriad of attacks from a diverse set of cyber aggressors, one major question arises: Assuming the majority of America's CI is outside of the government's direct control and protection, has the private sector succeeded in maintaining adequate cybersecurity measures to protect data and intellectual property, and to defend against a cyberattack that could have a "debilitating impact" on our way of life?[27] The answer to that question seems to be a resounding "no."[28]

---

http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html (listing other private industry cyberattack victims, including: Anthem, Sony Pictures, Staples, Home Depot, and Community Health Systems); *see also* PRICEWATERHOUSECOOPERS, MANAGING CYBER RISKS IN AN INTERCONNECTED WORLD: KEY FINDINGS FROM THE GLOBAL STATE OF INFORMATION SECURITY SURVEY 2015 10 (2014) ("[T]he total number of [cyber]security incidents detected by respondents climbed to 42.8 million [in 2014], an increase of 48% over 2013.").

24. Dorothy E. Denning, *Cyberterrorism*, *in* 2 GLOBAL DIALOGUE, Autumn 2000, 29. ("Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.").

25. *See generally* Tatiana Melnik, *New U.S. Sanctions Program Seeks to Give Government an Extra Tool to Fight Cyber-Attacks*, 17 J. HEALTH CARE COMPLIANCE, May–June 2015, at 53, 54 ("Large organizations—those with revenues of over $1 billion—reported that the financial losses attributable to the cyber-security incident increased from $3.9 million in 2013 to $5.9 million in 2014.").

26. *Critical Infrastructure and Key Resources*, *supra* note 21.

27. Exec. Order 13636, *supra* note 15.

28. *See IBM Study: Organizations Struggling to Defend Against Sophisticated Cyber Attacks*, IBM (Dec. 9, 2014), https://www-03.ibm.com/press/us/en/pressrelease/45625.wss

In 2013, President Obama issued Executive Order 13636 calling for "a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing" because "[r]epeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity."[29] Congress has been reluctant to regulate the private sector and set mandatory CI-wide minimum cybersecurity standards.[30] It is clear, however, that more needs to be done to protect America's CI from a successful cyberattack. This paper's purpose is to explore and evaluate congressional and agency efforts to guide the private sector toward improving cybersecurity short of direct legislative regulations, such as through agency adjudication and Congress's discretionary information exchange system, and to prepare corporations for current and further congressional and agency intervention in the cybersecurity arena. This paper proceeds in five parts.

Part II lays out the background necessary to understand the scope of the threat that cyberattacks pose to America's CI. This section first discusses and differentiates between cyberterrorism and cyber espionage. Understanding the distinctions will provide a more nuanced understanding of the cyber threats facing America's CI and how the private sector and government can tailor cybersecurity defenses to counter these threats. This section then examines why the military, law enforcement, Congress, and federal agencies are not the groups responsible for protecting America's CI, and why it is, in fact, the private sector that must be responsible for protecting the CI from destructive cyberattacks. However, this paper argues that because the private sector does not have an incentive to spend sufficient funds on cybersecurity, the burden must fall on Congress and agencies to motivate the private sector to improve CI cybersecurity.

Part III examines and evaluates current congressional and agency efforts to reach and guide specific industries toward improving their cybersecurity through direct regulation. The two agency efforts this paper examines are: (1) the Federal Trade Commission's ("FTC") "Safeguard Rule" and (2) the Department of Health and Human Services' ("DHHS") "HIPAA Security Rule."

In addition to attempting to reach specific industries, the government and government agencies have also tried to influence private sector cybersecurity practices on a larger scale. Part IV

("More than 80 percent of security leaders believe the challenge posed by external threats is on the rise, while 60 percent also agree their organizations are outgunned in the cyber war . . . .").

29. Exec. Order 13636, *supra* note 15.

30. Wooten, *supra* note 19, at 230 ("[T]here is no general data-security statute in the United States.").

introduces and analyzes two recent ways in which the government and its agencies have tried to do this: (1) the FTC's prosecution of businesses for data security failures as unfair practices, and (2) Congress' enactment of the Cybersecurity Act of 2015.

Part V highlights the need for the government to influence and incentivize the private sector to train and educate their employees on cybersecurity best practices because human error, not a lack of sophisticated cyber defenses, is the most common reason for successful breaches.

Part VI concludes the paper by arguing the following: for the sake of homeland security, the government needs to motivate the private sector to sufficiently improve its own cybersecurity because natural market forces will likely continue to be an inadequate driver in incentivizing the private sector to protect the nation.

II. BACKGROUND

A. An Overview of Cyberattack Sources Against the United States Private Sector

Almost every sector of American life relies on information technology systems ("IT systems") for a wide variety of tasks, including data storage, communication, and transactions between businesses and customers.[31] Vulnerabilities are inherent in the private sector's reliance on IT systems because of "interdependent components."[32] That is, the devices that the private sector uses to transmit information through cyberspace rely on other devices, and as such, exploiting a weakness in one device can "have a negative, cascading effect on others."[33] It is therefore no surprise that, with so much valuable information passing through a cyberspace containing intrinsic flaws, several different parties prey on these weaknesses to steal money, obtain classified information, or disrupt America's CI.[34] Definitions for the several distinct cyber aggressors that threaten national security are nebulous. As such,

---

31. In 2007, Estonia, "one of the most networked countries in the world," grinded to a halt when a cyberattack paralyzed the entire country, causing all credit card companies, telecommunication companies, and media companies to shut down. Sales, *supra* note 15, at 1504.

32. *See* Deborah Norris Rodin, *The Cybersecurity Partnership: A Proposal for Cyberthreat Information Sharing Between Contractors and the Federal Government*, 44 PUB. CONT. L.J. 505 (2015).

33. ERIC A. FISCHER ET AL., CONG. RESEARCH SERV., R42984, THE 2013 CYBERSECURITY EXECUTIVE ORDER: OVERVIEW AND CONSIDERATIONS FOR CONGRESS 2 (2013), https://www.fas.org/sgp/crs/misc/R42984.pdf.

34. Rodin, *supra* note 32, at 508.

understanding the difference among the various aggressors and the threats each pose will improve understanding of the cyber threats facing America's private sector. Among them, the most prevalent sources of major cyber threats to America's critical infrastructure are cyberterrorism and cyber espionage.

1. Cyberterrorism

During a speech to the Business Executives for National Security meeting in 2012, former U.S. Defense Secretary Leon E. Panetta said that a violent extremist group could perpetrate a cyberattack as destructive as the 9/11 terrorist attacks, and that such an attack could paralyze America.[35] While cyberterrorism has yet to be uniformly defined, the definition for domestic terrorism provides a sufficient starting point for fashioning a cyberterrorism definition.[36] Domestic terrorism is defined as an act dangerous to human life that is "intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction."[37] By substituting "an act dangerous to human life" with "a cyberattack dangerous to human life," this definition provides a basis for discussing cyberterrorism.[38]

There are specific characteristics that distinguish would-be cyberterrorist acts from other types of cyberattacks.[39] First, like traditional terrorist acts, "political, religious, racial, or social ideology" would be the driving force behind a cyber terrorist's actions.[40] Second, terrorists tend to carry out their agenda by

35. Jim Garamone, *Panetta Spells Out DOD Roles in Cyberdefense*, DEP'T. OF DEF. (Oct. 11, 2012), http://archive.defense.gov/news/newsarticle.aspx?id=118187.

36. Paul N. Stockton & Michele Golabek-Goldman, *Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat*, 25 STAN. L. & POL'Y REV. 211, 259 (2014) ("Given the international community's failure to achieve a consensus on the definition of terrorism, attempts to achieve universal agreement on a cyberterrorism definition may prove similarly futile.").

37. 18 U.S.C. § 2331(5)(A)–(B).

38. A cyberattack is "[a]n attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity." *Cyber Glossary*, *supra* note 20.

39. FISCHER ET AL., *supra* note 33, at 2.

40. *Homeland Threats and Agency Responses: Hearing Before the S. Comm. on Homeland Security & Governmental Affairs*, 112th Cong. 4 (2012) (prepared statement of Robert S. Mueller, III, FBI Director), http://www.hsgac.senate.gov/download/?id=7AB6DC14-F3F9-43E9-AAE0-4EA144C89447; 18 U.S.C. § 2331 (2012).

causing "mass destruction and not mass disruption." This likely explains why investigators have not linked any private sector cyber breaches to terrorist organizations.[41] Simply stealing a business's customer data or trade secrets would not lead to the type of "mass destruction" of physical assets or people that most terrorist organizations desire. Instead, through social media, terrorist groups would use cyberspace as a means of spreading propaganda, recruiting people who sympathize with their cause, and planning and executing attacks on physical locations in the U.S.[42]

Although "no unclassified reports have been published regarding a terrorist-initiated cyberattack on U.S. critical infrastructure," two possible cyberterrorism scenarios trouble policy makers. First, should terrorist organizations turn their focus from causing "mass destruction" to "mass disruption," the results could be devastating.[43] The second—more troubling—scenario is a cyberterrorist causing physical damage to U.S. CI assets through cyberspace that could harm American citizens. The following subsection discusses the Stuxnet Worm ("Stuxnet"), a cyber attack which caused physical damage to an Iranian nuclear power plant that could be replicated in the future against America as a cyberterrorist attack.

a. Stuxnet

41. Michael Hayden said at a Systems Engineering D.C. conference in 2014 that he did not "have a single example of cyber terrorism." Dennis Fisher, *Cyberespionage, Not Cyber Terror, Is the Major Threat, Former NSA Director Says*, THREAT POST (Apr. 3, 2014, 10:40 AM), https://threatpost.com/cyberespionage-not-cyber-terror-is-the-major-threat-former-nsa-director-says/105223/.

42. *See* United States v. Hassan, 742 F.3d 104, 120 (4th Cir. 2014) (noting the trial court's emphasis that Hassan, who was convicted of supporting terrorists by using Facebook to post messages and videos related to violent jihad, "was highly proficient in using technology to disseminate his beliefs and in seeking to recruit others to his violent ideology").

43. Fisher, *supra* note 41 (quoting former CIA and NSA director Michael Hayden). A "disruptive" act carried out by terrorists could be similar to one that occurred in 2012, when Syrian hackers hacked the Associated Press' Twitter account and sent out the tweet, "Breaking: Two Explosions in the White House and Barack Obama is injured[.]" Max Fisher, *Syrian Hackers Claim AP Hack that Tipped Stock Market by $136 Billion. Is It Terrorism?*, WASH. POST (Apr. 23, 2013), https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/. This caused the Dow to drop 150 points and erased "$136 billion in equity market value." *Id.*

In 2010, International Atomic Energy Agency inspectors were visiting one of Iran's uranium enrichment plants in Natanz.[44] During their inspection, they discovered that centrifuges used in the enrichment process were failing at an alarming rate.[45] The inspectors estimated that plant workers had replaced between one and two thousand centrifuges in the space of a few months.[46] Several months later, a computer security firm found malware in the plant's computer system that seemed to be "stealing configuration and design data from [control] systems, presumably to allow a competitor to duplicate a factory's production layout."[47] However, after delving deeper into Stuxnet's complex code, the security firm found that the malware was targeting industrial computer-assisted industrial control systems ("ICS").[48] ICS is a general term that encompasses several sub-systems vital to the operation of "industrial sectors and critical infrastructures," such as "electrical, water and wastewater, oil and natural gas, chemical, transportation, pharmaceutical . . . and discrete manufacturing."[49] Stuxnet targeted a specific aspect of the enrichment plant's ICS, namely its Programmable Logic Controllers ("PLCs").[50] PLCs run automated processes in the enrichment plant, and Stuxnet caused the PLCs to speed up the centrifuges required to enrich uranium to the point where they failed and had to be replaced.[51] As a result of the Stuxnet attack, the Natanz plant not only needed to remove the

---

44. Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*, WIRED (Nov. 3, 2014, 6:30 AM), http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet.

45. *Id.* ("Centrifuges are large cylindrical tubes—connected by pipes in a configuration known as a 'cascade'—that spin at supersonic speed to separate isotopes in uranium gas for use in nuclear power plants and weapons.").

46. K=1 Project, Center for Nuclear Studies at Columbia University, *Stuxnet: Tool of Nonproliferation or Pandora's Box*, COLUMBIA U. (Aug. 19, 2012), https://k1project.columbia.edu/news/stuxnet.

47. Hannah Lobel, *Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict*, 47 TEX. INT'L L.J. 617, 623 (2012).

48. Robert Kenneth Palmer, *Critical Infrastructure: Legislative Factors Preventing a "Cyber-Pearl Harbor"*, 18 VA. J.L. & TECH. 289, 308 (2014).

49. KEITH STOUFFER ET AL., NAT'L INST. OF STANDARDS AND TECHNOLOGY U.S. DEP'T OF COMMERCE, SPECIAL PUB. NO. 800-82, GUIDE TO INDUSTRIAL CONTROL SYSTEMS (ICS) SECURITY 2-1 (2011), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82.pdf.

50. Bruce Schneier, *The Story Behind the Stuxnet Virus*, FORBES (Oct. 7, 2010, 6:00 AM), http://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html.

51. Palmer, *supra* note 48, at 309–10 n.61.

virus but also replace all of their equipment, a two-year setback to the plant's nuclear capabilities.[52]

As the first malware designed to cause physical damage to industrial equipment,[53] Stuxnet and its effects on the Iranian enrichment plant showcase the possible effects of a similar cyberattack on American CI. The PLCs that Stuxnet altered are the same systems that are "vital to the operation of the U.S. critical infrastructures" and "are often highly interconnected and mutually dependent systems."[54] Several studies have shown that control systems that manage large parts of America's CI, such as PLCs controlling the power grid, are vulnerable to a Stuxnet-like attack that could cause physical damage to assets, leading to cascading power failures.[55]

The Stuxnet story is a cautionary tale for the type of harm a cyber weapon could cause the U.S. CI should terrorist organizations take their campaigns online. Although a Western power likely created Stuxnet to delay Iran's nuclear weapon program, if it was Iran who used a Stuxnet-like attack against a U.S. power grid or water treatment plant, it would likely be classified as cyberterrorism, especially if the attack did not simply result in parts of a reactor breaking down, but a full meltdown disaster.[56]

2. Cyber Espionage

Foreign economic and industrial espionage against the United States "represent[s] significant and growing threats to the nation's prosperity and security."[57] China and Russia are the two

---

52. Yaakov Katz, *Stuxnet Virus Set Back Iran's Nuclear Program by 2 Years*, JERUSALEM POST (Dec. 15, 2010, 5:15 AM), http://www.jpost.com/Iranian-Threat/News/Stuxnet-virus-set-back-Irans-nuclear-program-by-2-years.

53. *See Stuxnet Code* (Sept. 12, 2015, 11:24 AM), https://archive.org/details/Stuxnet.

54. *See* STOUFFER ET AL., *supra* note 49, at 1.

55. FISCHER ET AL., *supra* note 33, at 3.

56. PAUL K. KERR ET AL., CONG. RESEARCH SERV., R41524, THE STUXNET COMPUTER WORM: HARBINGER OF AN EMERGING WARFARE CAPABILITY 5 (2010).

57. OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS IN CYBERSPACE i (2011), http://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf [hereinafter FOREIGN SPIES STEALING]; *see also* American Enterprise Institute, *Gen. Alexander: Greatest Transfer of Wealth in History*, YOUTUBE (July 9, 2012), https://www.youtube.com/watch?v=JOFk44yy6IQ (recording speech of General Keith B. Alexander, who served as Director of the National

nations most often connected with economic and industrial espionage.[58] The U.S. government has linked several cyber breaches to Chinese government-sponsored activities, including a cyberattack against Anthem, a healthcare insurance giant.[59] Cyber espionage results in a breach of consumer data, but also more importantly, civil and military intellectual property and trade secrets, much of which is housed in the private sector.[60] In particular, the Pentagon has linked Chinese hackers to the breach of critical U.S. missile defense systems and combat aircraft designs.[61] If the U.S. CI continues to lose trade secrets at the rate it has over the past several years, the losses could undermine "the corporate sector's ability to create jobs, generate revenues, foster innovation, and lay the economic foundation for prosperity and national security."[62]

B. Who is Responsible for Critical Infrastructure Cybersecurity Oversight?

Who then is responsible for defending 85% of "infrastructure and resources critical to [America's] physical and economic security" from a catastrophic cyberattack originating from either a terrorist group or foreign power?[63] There are four possible candidates: the military, law enforcement agencies, Congress and government agencies, or the private sector.

Although the military has traditionally only considered air, land, sea, and space as domains requiring strategic defenses, it now

---

Security Agency, Chief of the Central Security Service, and Commander of the United States Cyber Command arguing that economic espionage "represents the greatest transfer of wealth in history").

58. FOREIGN SPIES STEALING, *supra* note 57, at 4–6.

59. Ellen Nakashima, *Security Firm Finds Link Between China and Anthem Hack*, WASH. POST (Feb. 27, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/02/27/security-firm-finds-link-between-china-and-anthem-hack/.

60. *Id.*

61. *See* Ellen Nakashima, *Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies*, WASH. POST (May 27, 2013), https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html; *see also* Ernesto Londoño, *Pentagon: Chinese Government, Military Behind Cyberspying*, WASH. POST (May 6, 2013), https://www.washingtonpost.com/world/national-security/pentagon-chinese-government-military-behind-cyberspying/2013/05/06/f4851618-b694-11e2-b94c-b684dda07add_story.html.

62. FOREIGN SPIES STEALING, *supra* note 57, at 3.

63. *Critical Infrastructure and Key Resources*, *supra* note 21.

considers cyberspace as the "largest ungoverned space in recorded human history" and a domain in need of protection.[64] But the military is not responsible for defending the private sector from attacks originating solely from cyberspace.[65] And while cybercrimes against American citizens fall within law enforcement's "investigable authority," its power to protect the CI is limited to reacting to an attack's aftermath, such as finding and prosecuting the culprits, not preventing cyberattacks.[66] While punishment for cybercrimes can itself be a deterrent for future cyber criminals, the effect is weak because law enforcement face several limitations: namely, a foreign country's unwillingness to cooperate with domestic U.S. law enforcement, inadequate resources, and the rapidly changing cyberspace landscape.[67]

With both law enforcement and the military unable to protect the private sector from cyberattacks, the responsibility to guard America's CI falls on the government, as well as the private sector itself. The government, however, must spend its limited resources on improving its own cyber defenses, which continuously fall victim to serious breaches, leaving the government in no position to protect the sprawling private sector.[68] Technology is progressing

---

64. John Bussey, *Gen. Michael Hayden Gives an Update on Cyberwar*, WALL ST. J. (Feb. 9, 2016, 10:49 PM), http://www.wsj.com/articles/gen-michael-hayden-gives-an-update-on-the-cyberwar-1455076153 (interviewing Michael Hayden).

65. Susan W. Brenner, *Cyber-Threats and the Limits of Bureaucratic Control*, 14 MINN. J.L. SCI. & TECH. 137, 196 (2013) (arguing the American military is "responsible for protecting the nation from externally-based attacks that threaten the social and economic viability of the country. The military's mission, though, is limited to protecting the country from demonstrable acts of war, i.e., from external attacks that can be attributed to a hostile nation-state and that involve the use of traditional military force.").

66. *Id.* at 194.

67. Aaron J. Burstein, *Amending the ECPA to Enable a Culture of Cybersecurity Research*, 22 HARV. J.L. & TECH. 167, 181 (2008).

68. *See* Julie Hirschfeld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. TIMES (July 9, 2015), http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html; *see also* Keith Collins, *The IRS is Using a System that was Hacked to Protect Victims of a Hack – And it was Just Hacked*, QUARTZ (Mar. 1, 2016), http://qz.com/628761/the-irs-is-using-a-system-that-was-hacked-to-protect-victims-of-a-hack-and-it-was-just-hacked/. The Office of Personnel Management announced in 2015 that hackers stole "sensitive information . . . from 19.7 million people who had been subjected to a government background check," including "Social Security numbers . . . addresses, health and financial history . . . details on their neighbors, friends and relatives; their travel destinations outside the United States; and any foreigners they had come into contact with." Davis, *supra*. In May 2014 hackers stole over 724,000 tax

faster than the government can keep up with, and, as such, the private sector is going to be responsible for America's cyber safety "in a way in which [we] have not been required to be responsible for [our] safety since the closing of the American frontier in 1890."[69]

It is difficult for the private sector alone to bear that responsibility because businesses lack the incentive to take necessary precautions to prevent a debilitating attack.[70] Private sector businesses do not adequately fund their cyber defenses for two possible reasons. First, because it is not the private sector's duty to protect national security interests, many businesses view cybersecurity as an externality.[71] That is, the private sector does not want to increase spending on cybersecurity because they do not fully internalize the benefits, while others may benefit by being a "free rider."[72] However, because companies pay vast sums in legal fees to customers affected by hackings, the mounting costs of litigation could possibly overshadow this externality argument in the future.[73] Second and more importantly, with a few exceptions like Target, most breaches do not translate into falling share

---

transcripts from the IRS website. Collins, *supra*. In an effort to provide taxpayers with a second layer of protection, the IRS gave taxpayers a secret PIN number that they have to put on their tax return for it to be filed: "If someone loses their PIN, they can retrieve it by logging into a service on the IRS website. And that login process is secured by *the same technology that hackers broke through in the original data breach*." *Id.* This has led to a second round of IRS breaches with hackers filing further fraudulent tax returns. *Id.*

69. Bussey, *supra* note 64.

70. Burstein, *supra* note 67, at 176–77.

71. *Id.*

72. *See* Eli Dourado & Jerry Brito, *Is There a Market Failure in Cybersecurity?*, MERCATUS CTR., GEO. MASON U. (Mar. 6, 2012), http://mercatus.org/publication/there-market-failure-cybersecurity; Sales, *supra* note 15, at 1520 ("A company that secures itself against intruders makes it harder for assailants to commandeer its systems to attack others. Investments in cyber-defense thus effectively subsidize other firms. Because the investing company doesn't capture the full benefit of its expenditures, it has weaker incentives to secure its systems. And because other companies are able to free ride on the investing firm's expenditures, they have weaker incentives to adopt defenses of their own.").

73. *See*, *e.g.*, Andrew Harris, *Target Must Face Bank Suits Over Customer Data Breach*, BLOOMBERG (Dec. 2, 2014, 3:22 PM), http://www.bloomberg.com/news/articles/2014-12-02/target-must-face-banks-claims-of-negligence-in-data-breach.

prices.[74] This is likely because the public has become numb to the sheer number of cyberattacks that have occurred in recent years.[75]

If the private sector has not sufficiently improved their cyber defenses and the government is unable to expend resources on directly protecting the private sector, the government could regulate the private sector in one of three ways.[76] The first way is mandating minimum cybersecurity standards that CI industries have to follow; the second is mandating that industries set their own standards; and the third is providing subsidies or incentives to adopt cybersecurity standards.[77] Attempts at all three approaches, however, have failed, and Congress has since been reluctant to regulate the private sector.[78] Instead, agencies have begun instituting measures, short of direct regulation, to encourage the private sector to improve their cybersecurity. Thus there is an inherent tension between the government and private sector over who exactly bears responsibility for improving CI cybersecurity. The following sections will discuss government agency attempts to regulate, via enforcement measures, financial institutions and the healthcare industry, which are both components of America's CI. The section will then examine two current congressional and

---

74. Elena Kvochko & Rajiv Pant, *Why Data Breaches Don't Hurt Stock Prices*, HARV. BUS. REV, (Mar. 31, 2015), https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices ("A judge recently ruled that Target will have to defend itself against accusations of negligence by banks, credit unions and consumers when it came to preventing the 2013 security breach.").

75. Sarah Hatzack, *Home Depot and JPMorgan are Doing Fine. Is it a Sign We're Numb to Data Breaches?*, WASH. POST (Oct. 6, 2014, 6:31 PM), https://www.washingtonpost.com/news/get-there/wp/2014/10/06/home-depot-and-jpmorgan-are-doing-fine-is-it-a-sign-were-numb-to-data-breaches/.

76. *Google Security Whitepaper*, GOOGLE CLOUD PLATFORM, https://cloud.google.com/security/whitepaper. It is worth noting here that there are many businesses in the private sector, such as sophisticated technology companies like Google, that are sufficiently incentivized to maintain good cybersecurity practices, such as encrypting customer data, toward building trust with their customer-base as they are especially public-facing. Companies like Google are distinguishable from companies like Target where their cybersecurity and data protection practices are not under constant public scrutiny as with large technology companies.

77. Greg Mgrditchian & Ernest A. Yazzetti, Jr., *2013 National Lawyers Convention International: Cybersecurity—The Policy and Politics of a Leading National Security Threat*, 41 RUTGERS COMPUTER & TECH. L.J. 194, 222 (2015) (summarizing the 2013 Federalist Society panel regarding cybersecurity, Internet privacy, and their global impact); ROBERT HOUSMAN & TIMOTHY OLSON, CTR. FOR AMER. PROGRESS, NEW STRATEGIES TO PROTECT AMERICA: A MARKET-BASED APPROACH TO PRIVATE SECTOR SECURITY 7 (2005), https://www.americanprogress.org/wp-content/uploads/kf/FECREPORT.PDF.

78. Mgrditchian & Yazzetti, Jr., *supra* note 77, at 222.

agency attempts to reach a wider range of CI industries including and beyond the finance and healthcare sectors.

III. FEDERAL GOVERNMENT AND AGENCIES REGULATING INDIVIDUAL CRITICAL INFRASTRUCTURE INDUSTRY CYBERSECURITY PRACTICES

The Department of Homeland Security ("DHS") is the agency in charge of safeguarding the federal government's IT systems from cyberattacks.[79] But Congress has been hesitant to pass legislation requiring the whole private sector to adopt certain cybersecurity standards and best practices.[80] The government's power to affect large-scale change in the private sector goes only so far as attempting to create partnerships and improving information sharing between businesses and the federal government.[81] As a result of President Obama's Executive Order 13636, however, Congress has promulgated a voluntary cybersecurity framework aimed at better managing and reducing cybersecurity risks in lieu of mandating specific standards.[82] There are several possible reasons for the lack of government regulation. One is that lobbying efforts have successfully reduced the effectiveness of proposed private sector cybersecurity bills.[83] Another is that extensive

79. Thad A. Davis, et al., *The Data Security Governance Conundrum: Practical Solutions and Best Practices for the Boardroom and the C-Suite*, 2015 COLUM. BUS. L. REV. 613, 637 (2015) ("DHS is now the lead enforcement agency in the federal government's internal fight against data breaches").

80. Wooten, *supra* note 19, at 230 ("[T]here is no general data-security statute in the United States").

81. *Cyber Security Division*, U.S. DEP'T OF HOMELAND SECURITY, https://www.dhs.gov/science-and-technology/cyber-security-division (last visited May 20, 2016); *Office of Cybersecurity and Communications*, U.S. DEP'T OF HOMELAND SECURITY, https://www.dhs.gov/office-cybersecurity-and-communications (last visited May 20, 2016).

82. *Cybersecurity Framework Frequently Asked Questions*, NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, http://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-basics.cfm (last visited May 20, 2016).

83. Gerry Smith, *Cybersecurity Bill Faces Uncertain Future in Fight over Regulation*, HUFFINGTON POST (Mar. 19, 2012, 4:51 PM), http://www.huffingtonpost.com/2012/03/19/cybersecurity-bill-regulation_n_1362529.html ("When senators introduced the Cybersecurity Act of 2012, which gives DHS new powers to set cybersecurity standards for private companies operating the nation's critical infrastructure . . . business lobbyists . . . pressured the bill's authors to include so many exceptions that the latest version 'really just papers over the problem.'"); Kayla Morency, *Cybersecurity Finally Takes Center Stage in the U.S.*, 15 J. HIGH TECH. L. 192, 228 (2014) ("[C]orporate constituents wield immense power over the legislative agenda.").

regulations would be too expensive for the government to create and too hard to enforce because the vast number of industries and businesses have differing needs. Although there is no one industry-wide regulation, government agencies have stepped in to create rules and regulations that compel specific industries to adopt data security safeguards.

In the financial sector, the Gramm-Leach-Bliley Act requires particular agencies, including the FTC, to establish safeguards for financial institutions:

> "(1) [T]o ensure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[84]

Under this act, the FTC created the "Safeguard Rule."[85] The Safeguard Rule requires financial institutions to "develop, implement, and maintain a comprehensive information security program that . . . contains administrative, technical, and physical safeguards."[86] The FTC has filed several complaints against businesses, alleging that they had violated the Safeguard Rule by failing to "implement reasonable policies and procedures to protect the security and confidentiality of the information it collects."[87] Defendants opted to settle the majority of these cases pursuant to consent orders requiring businesses to comply with the Safeguard Rule by implementing "reasonable" cybersecurity defenses to protect customer data.[88] While the FTC has successfully made

---

84. 15 U.S.C. § 6801(b) (2010); *See also* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 248 (3rd Cir. 2015).

85. Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 312–22 (2015).

86. Kristin Shields, *Cybersecurity: Recognizing the Risk and Protecting Against Attacks*, 19 N.C. BANKING INST. 345, 358 (2015).

87. Sunbelt Lending Services, F.T.C. No. C-4129 (Jan. 3, 2005), https://www.ftc.gov/sites/default/files/documents/cases/2005/01/050107comp0423153.pdf; *See also* Superior Mortgage Corp., F.T.C. No. C-4153 (Dec. 14, 2005), https://www.ftc.gov/sites/default/files/documents/cases/2005/12/051216comp0523136.pdf.

88. *See* Trendnet, Inc., F.T.C. No. C-4426 (Jan. 16, 2014), https://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf; *see also*

organizations within its authority take cybersecurity more seriously, its efforts are restricted to financial institutions and are not applicable to other CI industries.[89]

In the healthcare sector, the Health Insurance Portability and Accountability Act ("HIPAA") requires the Department of Health and Human Services ("DHHS") to publish the "HIPAA Security Rule," which compels "health plans, health care clearinghouses, and certain health care providers" to adopt "standards for the security of electronic protected health information."[90] While the DHHS has prosecuted several hospitals for losing patient health information to cyber breaches, cyber aggressors could carry out cyberattacks against a hospital network without accessing patient health information, letting hospitals escaping violation of the HIPAA Security Rule.[91]

The FTC Safeguard Rule and HIPAA Security Rule are representative of the rules government agencies typically use to push important U.S. CI businesses to improve their cybersecurity.[92] And while the agencies' goals are to protect people's data, the practices that the FTC and DHHS rules require also support the government's aim of improving homeland security on the

---

Shima Baradaran-Robison, *Kaleidoscopic Consent Decrees: School Desegregation and Prison Reform Consent Decrees After the Prison Litigation Reform Act and Freeman-Dowell*, 2003 B.Y.U. L. REV. 1333, 1337–42 (2003) (explaining that a consent order is an enforceable agreement the FTC and the business enter into where the business does not admit to any wrongdoing, but agrees to satisfy several requirements to avoid further prosecution).

89. Shields, *supra* note 86, at n.122 ("'Financial institutions' under the GLBA include national banks, Federal branches and Federal agencies of foreign banks, member banks of the Federal Reserve System, and banks insured by the Federal Deposit Insurance Corporation.").

90. Health Insurance Reform: Security Standards, 68 Fed. Reg. 8333 (U.S. Dep't of Health & Human Services Feb. 20, 2003) (to be codified at 45 C.F.R. pts. 160, 162 & 164), http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf.

91. Katherine Booth Wellington, *Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions*, 30 SANTA CLARA HIGH TECH. L. J. 139, 161 (2014).

92. Another industry-specific regulation includes the North American Electric Reliability Corporation's "Reliability Standards," which is "authorized to set mandatory standards in the operation of U.S. power system." Shackelford, *supra* note 85, at 322. The Reliability Standards "include nine critical infrastructure protection standards that mandate a variety of cybersecurity reporting, security identification, security implementation, and recovery requirements that are overseen by the Federal Energy Regulatory Commission." *Id.*

cybersecurity front by implementing reasonable data security measures. But these rules are narrow in the scope of the prosecutable offenses and the industries they can reach. As such, the measures still leave much of the U.S. CI without comprehensive or reasonable cybersecurity standards. However, two recent developments indicate that the legislative branch and government agencies are working to reach larger areas of the CI without passing all-encompassing cybersecurity regulations.

The first development is the FTC's prosecution of businesses for poor or non-existent cyber defenses as unfair practices under the pre-existing Federal Trade Commission Act ("FTC Act").[93] This section will then discuss a case before an administrative law judge ("ALJ"), *In re LabMD*, that may have limited the FTC's ability to bring unfairness claims against businesses for unfair data security practices.[94] After the FTC heard the case on appeal from the ALJ's holding however, the Commission held that the ALJ applied the wrong standard when dismissing *In re LabMD*, and that no such restriction was placed on the FTC's ability to prosecute businesses for unfair cybersecurity practices.[95] The second development is the Cybersecurity Act of 2015, which facilitates information-sharing between the private sector and federal government.[96] This section will now examine the effectiveness of these methods in improving CI cybersecurity and homeland security.

IV. CONGRESSIONAL AND FEDERAL AGENCY ATTEMPTS TO AFFECT WIDESPREAD CYBERSECURITY IMPROVEMENTS THROUGHOUT U.S. CRITICAL INFRASTRUCTURE

Although the FTC and DHHS have had success in regulating the financial and healthcare industries, their reach into other industries is statutorily limited under the Safeguard Rule and HIPAA Security Rule. The FTC may, however, have more success regulating industry cybersecurity practices via adjudication under

93. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3rd Cir. 2015); 15 U.S.C. § 45(a) (2012).

94. Initial Decision, LabMD, F.T.C. No. 9357 (Nov. 13, 2015), https://www.ftc.gov/system/files/documents/cases/151113labmd_decision.pdf [hereinafter "Initial Decision"].

95. Commission Opinion, LabMD, F.T.C. No. 9357, at 1 (July 29, 2016), https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf [hereinafter "Commission Opinion"].

96. Consolidated Appropriations Act, 2016, Pub. L. No. 114–113, 129 Stat. 2242, 2935-85 (codified at 6 U.S.C. §§ 1501–1532 (2017)).

the FTC Act. Congress may also be able to influence the private sector as a whole toward improved cybersecurity procedures through the Cybersecurity Act of 2015.

A. Overview: The FTC's Prosecution of Private Sector Businesses for Deficient Cybersecurity as Unfair Practices Under the FTC Act

The statutory source of FTC's broadest data security authority is § 45(a) of the FTC Act.[97] It empowers the FTC to "prevent persons, partnerships, or corporations . . . from using . . . unfair or deceptive acts or practices in or affecting commerce."[98] In contrast to the Security Rule, the FTC Act allows the FTC to reach essentially any business in any industry that deals with commerce.[99]

In order for the FTC to successfully prosecute a business for unfair data security practices under § 45(a), the FTC must satisfy subsection § 45(n) of the FTC Act and show that the business's act: (1) causes or is likely to cause substantial injury to consumers, which (2) consumers cannot reasonably avoid, and (3) the act is "not outweighed by countervailing benefits to consumers or to competition."[100] In deciding the "substantial injury" prong, the FTC engages in a cost-benefit analysis and balancing of various factors, including "the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity."[101] Although the FTC Act does not grant the FTC "explicit statutory authority to regulate

---

97. 15 U.S.C. § 45(a) (2012).

98. *See id.* § 45(a)(2) (2012); *see also* Am. Fin. Servs. Ass'n. v. Fed. Trade Comm'n, 767 F.2d 957, 979–988 (D.C. Cir. 1985). The distinction between *unfair* and *deceptive* acts often becomes nebulous during litigation. However, one court has distinguished between the two by holding that that "[a] practice is deceptive when the consumer is forced to bear a larger risk than expected (e.g., the consumer is misled) whereas a practice is unfair when the consumer is forced to bear a larger risk than an efficient market would require." *Id.* As such, in the cybersecurity world, businesses advertising to customers that they have a certain level of IT security that they do not have would be "deceptive," whereas simply having deficient cyber defenses and leaving the customer's information open to hackers would be an unfair practice. *Id.* This paper will concentrate on *unfair* acts as opposed to *deceptive* acts.

99. 15 U.S.C. § 45(a)(2) (2012). The FTC Act, however, does not apply to "banks, savings and loan institutions," which the FTC can reach through its Security Rules. *Id.*

100. *Id.* at § 45(n).

101. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 255 (3rd Cir. 2015).

data security" under their unfairness authority, the FTC has prosecuted many businesses under the FTC Act, alleging that failure to provide adequate data security constitutes unfair practices.[102]

Since 2002, the FTC has used consent orders to settle with over fifty businesses that the FTC alleged had "engaged in unfair or deceptive practices that put consumers' personal data at unreasonable risk."[103] In most unfair practices consent orders, the FTC orders businesses to create a "comprehensive security program that is reasonably designed to:

> (1) [A]ddress security risks related to the development and management of new and existing products and services for consumers, and (2) protect the security, integrity, and confidentiality of covered information, whether collected by respondent or input into, stored on, captured with, or accessed through a computer using respondent's products or services."[104]

For the past fourteen years, the FTC's cybersecurity enforcement actions have gone unchallenged with "[t]he vast majority of these cases . . . end[ing] in settlement."[105] However, in *Federal Trade Commission v. Wyndham* ("Wyndham case"), Wyndham Worldwide ("Wyndham") became the first business to challenge the FTC's "authority to regulate data security as an 'unfair' practice."[106]

1. Challenging the FTC's Cybersecurity Policing Authority: Wyndham Case Overview

---

102. Greg Dickenson, *Wyndham Worldwide v. Federal Trade Commission: The Developing Parameters of the FTC's Data Security Requirements*, 19 J. OF INTERNET L., no. 6, 2015, at 9, 10.

103. FED. TRADE COMM'N, FEDERAL TRADE COMMISSION 2014 PRIVACY AND DATA SECURITY UPDATE 5 (2014), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.

104. *See* Trendnet, Inc., F.T.C. No. C-4426 (Jan. 16, 2014), https://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf; *see* Fandango, LLC., F.T.C. No. C-4481 (Aug. 13, 2014), https://www.ftc.gov/system/files/documents/cases/140819fandangodo.pdf.

105. *Wyndham*, 799 F.3d at 240.

106. Gregory James Evans, *Regulating Data Practices: How State Laws Can Shore up the FTC's Authority to Regulate Data Breaches, Privacy, and More,* 67 ADMIN. L. REV. 187, 188 (2015).

Wyndham is a hospitality company that manages and franchises hotels.[107] Between 2008 and 2009, hackers broke into Wyndham's IT network three times and accessed "unencrypted information" including "card information from over 619,000 consumers, which . . . resulted in at least $10.6 million in fraud loss."[108] In 2012, the FTC filed charges against Wyndham in federal district court, alleging that Wyndham had "engaged in unfair cybersecurity practices that, 'taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft.'"[109] Instead of settling, Wyndham filed a motion to dismiss the claims against them.[110]

Although the district court denied Wyndham's motion to dismiss and ruled in the FTC's favor, the court certified two issues for interlocutory appeal.[111] The first was whether the FTC could "bring an unfairness claim involving data security under Section 5" of the FTC Act (codified as 15 U.S.C. § 45(a)).[112] The second issue was whether the FTC must "formally promulgate regulations before bringing its unfairness claim under Section 5" of the FTC Act to satisfy fair notice principles.[113] The United States Third Circuit Court of Appeals ("Circuit Court") issued a ruling on these issues.[114]

(1) First Issue: Could the FTC "Bring an Unfairness Claim Involving Data Security under Section 5" of the FTC Act Against Wyndham?

Wyndham made two lines of arguments for why the FTC did not have authority to prosecute businesses under their unfairness authority for cybersecurity practices. First, it maintained, Wyndham's inadequate data security practices fell outside the plain meaning of "unfair" within the FTC Act.[115] In its interpretation, "conduct is only unfair when it injures consumers 'through unscrupulous or unethical behavior.'"[116] The Supreme

107. *Wyndham*, 799 F.3d at 240.
108. *Id.* at 242.
109. *Id.* at 240.
110. *Id.* at 242.
111. FTC v. Wyndham Worldwide Corp., 10 F.Supp.3d 602, 636 (D.N.J. 2014).
112. *Id.*
113. *Id.*
114. *Wyndham*, 799 F.3d at 236.
115. *Id.*
116. *Id.* at 244.

Court precluded this contention when interpreting the FTC Act in a prior case, leaving the argument without merit.[117] Wyndham also maintained that "a business 'does not treat its customers in an 'unfair' manner when the business itself is victimized by criminals."[118] However, the Circuit Court rejected this argument because Wyndham cited no authority for its assertion.[119] Last, Wyndham made a "slippery slope" argument, claiming that extending the FTC's unfairness authority to data security would mean the FTC has authority to "regulate the locks on hotel room doors . . . to require every store in the land to post an armed guard at the door," and to prosecute supermarkets that are "sloppy about sweeping up banana peels."[120] The Circuit Court responded by saying "were Wyndham a supermarket, leaving so many banana peels all over the place that 619,000 customers fall hardly suggests it should be immune from liability under § 45(a)."[121]

In its second argument, Wyndham maintained that even if the plain meaning of "unfairness" included data security prosecution, subsequent Congressional legislative actions removed cybersecurity from the FTC's jurisdiction.[122] In particular, Wyndham contended that because the Gramm–Leach–Bliley Act required the FTC to create "standards for financial institutions to protect consumers' personal information," Congress had implicitly limited the FTC's authority to financial institutions.[123] Further, Wyndham argued that Congress had no other reason for passing legislation like the Gramm–Leach–Bliley Act if the FTC had general jurisdiction under their unfairness authority to prosecute all businesses for unfair data security practices.[124]

Neither argument persuaded the Circuit Court, and it held that Congress required the FTC to promulgate regulations for specific industries to lessen "some of the burdensome § 45(n) requirements for declaring acts unfair."[125] In rejecting Wyndham's arguments, the Circuit Court affirmed the district court's holding that data security falls within the FTC's unfairness authority.[126]

---

117. *Id.* at 244–45.
118. *Id.* at 246.
119. *Id.*
120. *Id.*
121. *Id.* at 247.
122. *Id.*
123. *Id.*
124. *Id.* at 247–48.
125. *Id.* at 248.
126. *Id.* at 249.

(2) Second Issue: Did the FTC Provide Wyndham with Fair Notice That Their Actions Could Fall Within 15 U.S.C. § 45(a)(2) of the FTC Act?

The Circuit Court held that finding a data security practice unfair under Subsection 45(n) requires a cost-benefit analysis.[127] The Circuit Court did not find this legal standard "so vague as to be 'no rule or standard at all.'"[128] From this, the Circuit Court concluded that "[f]air notice is satisfied here as long as the company can reasonably foresee that a court could construe its conduct as falling within the meaning of the statute" by examining § 45(n).[129] Wyndham noticed that its actions could fall within the FTC Act because the FTC had published "consent decrees in administrative cases raising unfairness claims based on inadequate corporate cybersecurity," as well as materials like *Protecting Personal Information: A Guide for Business*, on their website.[130] But the court noted that neither the consent orders nor other publications "state that any particular practice is required by § 45(a);" rather, it requires that they generally put businesses on notice.[131] The fact that Wyndham was hacked three times also should have made it clear that a court might find their conduct would fall into the § 45(n) cost-benefit analysis.[132] Taken together, the Circuit Court held that the FTC's past actions in data security prosecution put Wyndham on notice.[133] Further, the Circuit Court held that Wyndham was only entitled to know whether it "had fair notice that its conduct could fall within the meaning of the statute," and it was not entitled to know with "ascertainable certainty" the specific cybersecurity practices the FTC read the FTC Act as requiring under their unfairness authority.[134]

In conclusion, there are three lessons that the private sector should take away from the Wyndham case: (1) the FTC has authority to prosecute businesses for not engaging in reasonable data security practices under the FTC Act as outlined by the §

---

127. *Id.* at 255.

128. *Id.*

129. *Id.* at 256.

130. *Id.* at 256–57; s*ee also* FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (2007) (describing practices that form "sound data security plan[s]" and counseling against many of the specific practices Wyndham allegedly participated in).

131. *Wyndham*, 799 F.3d at 256.

132. *Id.*

133. *Id.* at 258.

134. *Id.* at 255.

45(n) cost-benefit analysis balancing factors, (2) the FTC is not currently required to publish specific reasonable cybersecurity practices it expects businesses to maintain, and (3) future businesses will now be on notice as to the FTC's unfairness authority because of the number of prior businesses the FTC has prosecuted and data security materials it published on its website.

2. A Subsequent Judicial Development in the FTC's Authority Over Private Sector Data Security Practices: *In re LabMD* Overview, Decision, and Appeal

Tiversa Holding Company ("Tiversa"), a data security company, approached LabMD, a clinical testing laboratory, claiming they found on a public peer-to-peer file sharing network a LabMD document containing personal information for approximately 9,300 consumers, including customer names, addresses, social security numbers, and health insurance information.[135] After LabMD declined to pay for Tiversa's data security services, Tiversa reported LabMD to the FTC.[136] In August 2013, the FTC filed an administrative complaint against LabMD alleging they had engaged in unfair data security practices.[137] After hearing the case, the administrative law judge ("ALJ") ruled that under § 45(n) the FTC needed to prove that LadMD's "practice causes or is likely to cause substantial injury to consumers."[138] The FTC, however, had failed to provide evidence that the file's mere existence on a public network had caused any consumer a substantial injury.[139] The ALJ reasoned that, although there may be proof of a "possible" harm, the ALJ did not equate "possible harm" with "probable" harm, or "likely" injury as required under § 45(n).[140] The ALJ reasoned that allowing the FTC to base unfair conduct liability "on a mere 'risk' of harm alone, without regard to the probability that such harm will occur, would effectively allow unfair conduct liability to be imposed upon proof of unreasonable data security alone."[141] Based on the above reasoning, the ALJ dismissed the Commission's suit against LabMD.[142]

---

135. Initial Opinion, *supra* note 94, at 24.
136. *Id.* at 30.
137. *Id.* at 1.
138. *Id.* at 88.
139. *Id.*
140. *Id.* at 87.
141. *Id.* at 81.
142. *Id.* at 88.

The FTC's Complaint Counsel appealed the ALJ's decision to the Commission, and in an opinion written by Chairwoman Edith Ramirez, the Commission overturned the ALJ's dismissal holding that the ALJ applied the incorrect legal standard for unfairness.[143] The Commission examined how "likely" a harm had to be to satisfy Section 5(n)'s first prong.[144] Contrary to the ALJ opinion, the Commission held that "a practice may be unfair if the magnitude of the potential injury is large, even if the likelihood of the injury occurring is low."[145] After this general conclusion, the Commission went on to apply Section 5(n)'s three prongs to LabMD's data security practices to see whether LabMD failed to provide reasonable security for the sensitive information on its servers, and whether LabMD's failure "caused or was likely to cause substantial injury that consumers could not have reasonably avoided and that was not outweighed by benefits to consumers or competition."[146] The Commission provided a thorough analysis of the meaning of "likely to cause."[147] The ALJ relied on the Merriam-Webster dictionary's definition that "likely" means that Section 5(n) requires a showing that it is "probable that something will occur," not merely "possible," and concluded that "at best, Complaint Counsel has proven the 'possibility' of harm."[148] However, the Commission disagreed with the ALJ for several reasons.

First, various dictionaries defined "likely" differently, and as such, when interpreting an important statutory term, dictionaries may not be useful.[149] Second, for prior Commission cases applying Section 5(n), "likely" evaluated the magnitude of the harm involved combined with the likelihood of the harm occurring. In those cases, it was found that a practice could be unfair if the severity of the harm is large, even if the likelihood of injury is low.[150] The Commission thus concluded that Congress intended to "incorporate the concept of risk when it authorized the Commission to pursue practices 'likely to cause substantial injury.'"[151] Based on the Commission's reversal, the Commission issued a Final Order similar to those it had issued in the past,

143. Commission Opinion, *supra* note 95, at 1.
144. *Id.* at 10.
145. *Id.*
146. *Id.* at 11.
147. *Id.* at 20–25.
148. *Id.* at 20.
149. *Id.*
150. *Id.* at 21.
151. *Id.*

ordering LabMD to institute reasonable cybersecurity safeguards for its information.[152] LabMD is expected to file an appeal with the Court of Appeals appealing the FTC's decision.[153]

3. The Eleventh Circuit Examines the FTC's Cybersecurity Prosecutorial Powers Under the FTC Act

After the FTC issued its Final Order in 2016, LabMD appealed the case to the Eleventh Circuit Court of Appeals ("Circuit Court") and requested that the FTC stay their final order while the Circuit Court reviewed the appeal.[154] The FTC denied the stay, but the Circuit Court granted it.[155] The first factor the Circuit Court analyzed when deciding whether to grant LabMD's stay was "whether the stay applicant has made a strong showing that he is likely to succeed on the merits," and this is where the Circuit Court examined whether the FTC's interpretation of 45(n) was "reasonable."[156] Although the Circuit Court recognized the FTC's interpretation is typically entitled to *Chevron* deference if reasonable, LabMD had identified compelling reasons why the FTC's interpretation might not be reasonable.[157]

The Circuit Court first addressed whether "a reasonable interpretation of § 45(n) included intangible harms like those that the FTC found in this case."[158] The "intangible harms" the FTC alleged consumers suffered included the sole unauthorized disclosure of their personal information, and "'privacy harm' that may have affected their reputations or emotions."[159] However, the legislative history of § 45(n) said that "[e]motional impact and more subjective types of harm alone are not intended to make an injury unfair."[160] Further, LabMD argued that the harm the FTC had found was "not even 'intangible,'" as a true data breach of

---

152. Final Order, *LabMD*, F.T.C. No. 9357 (July 29, 2016) https://www.ftc.gov/system/files/documents/cases/160729labmdorder.pdf [hereinafter "Final Order"].

153. Cara Salvatore, *LabMD Taps 4 from Ropes & Gray for FTC Cyber Appeal*, LAW360 (Aug. 19, 2016), http://www.law360.com/articles/830507/labmd-taps-4-from-ropes-gray-for-ftc-cyber-appeal.

154. LabMD, Inc. v. Fed. Trade Comm'n, No. 16-16270-D, 2016 WL 8116800, at *2 (11th Cir. 2016).

155. *Id.*

156. *Id.* at *2–3.

157. *Id.* at *3.

158. *Id.*

159. *Id.*

160. *Id.* (quoting S. REP. NO. 103-130, at *13 (1993)).

personal information to the public might be, "but rather is purely conceptual" because this harm is only speculative."[161] Thus the court held the LabMD had shown the FTC's interpretations and factual findings may not be reasonable.[162]

The Circuit Court then addressed whether the FTC had reasonably interpreted "likely to cause" in § 45(n).[163] The FTC originally held that § 45(n)'s "likely to cause" language meant "significant risk," where "a practice may be unfair if the magnitude of the potential injury is large, even if likelihood of the injury occurring is low."[164] The Circuit Court differed with the FTC's interpretation of "likely to cause," and held that the word "likely" does not include something that has a low likelihood. The Circuit Court differed and did not read "likely" to include something that has a low likelihood of occurring.[165] Thus the Circuit Court held the FTC's interpretation was not reasonable.[166] The Circuit Court concluded that LabMD could make a "substantial case on the merits and present a serious legal question" as to its claims that the FTC had misapplied and misinterpreted §45(n).[167] And after examining the other three factors for a stay pending appeal, the Circuit Court granted LabMD's stay.[168]

4. Wyndham and LabMD Case Analyses: Their Implications for the FTC's Ability to Affect Cybersecurity Changes Throughout the U.S. Critical Infrastructure

After the Circuit Court held in the FTC's favor, Wyndham settled with the FTC.[169] The Wyndham case shows that the FTC is becoming a powerful player in private sector data security enforcement. It is clear that the FTC is attempting to create and improve cybersecurity standards in the private sector where Congress has declined to do so through blanket regulation.[170]

---

161. *Id.*
162. *Id.*
163. *Id.*
164. *Id.*
165. *Id.*
166. *Id.*
167. *Id.* at *4.
168. *Id.* at *5.
169. Stipulated Order for Injunction, FTC v. Wyndham World Wide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014) (No. 13-CV-1887), https://www.ftc.gov/system/files/documents/cases/151209wyndhamstipulated.pdf.
170. Stacey Higginbotham, *The FTC's Wyndham Victory is Good for Privacy but Confusing for Businesses*, FORTUNE (Aug. 28, 2015), http://fortune.com/2015/08/28/ftc-wyndham-privacy-courts/.

What many companies in the private sector may find troubling is that, although the § 45(n) cost-benefit balancing test pushes them to evaluate their practices, the FTC has not published clear standards for what exactly constitutes unreasonable cybersecurity and data security measures.[171] This places the FTC in an odd position where it can prosecute businesses for not maintaining reasonable data security practices without telling businesses what exactly they consider reasonable practices.

Some commentators have argued that the FTC should publish "very detailed, specific, rigorous list of the most effective data security practices for companies."[172] But the FTC will likely not set such practices in stone. First, businesses throughout the CI house and protect different types of data, and as such, the FTC recognizes that imposing "a one-size-fits-all set of security requirements" would be impractical.[173] This is similar to why Congress has declined to pass such legislation. Second, cyber aggressors are becoming more sophisticated every day, which means that any practices the FTC mandates would be outdated within a few months. Nevertheless, the specter of FTC prosecution will likely persuade businesses to adopt reasonable cybersecurity initiatives detailed in past FTC consent orders. Business that are concerned with whether the FTC could file a suit against them for unfair cybersecurity practices would be best served by examining past suits the FTC has brought under their unfairness authority in the business's industry, and to create a playbook of practices to avoid or institute in order to bolster their defenses should the FTC file suit.

In the most recent LabMD development, the Eleventh Circuit may be the first court to limit the FTC's ability to prosecute businesses for insufficient data security practices under their unfairness authority despite *Chevron* deference and Congress intentionally leaving the development of the term "unfair" to the FTC.[174] Although the Eleventh Circuit did not bar the FTC from pursuing suits where there is an "intangible harm," the Circuit Court nevertheless limited "intangible harm" to not include

---

171. *Id.*

172. Josephine Wolff, *What Exactly Does Reasonable Mean*?, SLATE, (Aug. 26, 2015, 4:33 PM), http://www.slate.com/articles/technology/future_tense/2015/08/the_ftc_punishes_wyndham_for_failing_to_protect_customer_data.html.

173. *Id.*

174. LabMD, Inc. v. FTC, No. 16-16270-D, 2016 WL 8116800 at *3 (11th Cir. Nov. 10, 2016).

"emotional impact." The Circuit Court's holding has also brought into question and made unclear the amount of harm consumers must sustain before the FTC can intercede under their unfairness authority.

Although the FTC has mainly prosecuted technology and retail businesses when their data security practices have harmed customers, the FTC could potentially begin prosecuting businesses in other CI industries as long as those businesses retain customer data and are in commerce.[175] Although the FTC's goal is consumer data protection, putting other CI industries on notice that their data protection practices could fall within the FTC's unfairness authority would have the positive effect of indirectly improving homeland security because businesses would examine whether they had reasonable cybersecurity practices so as to avoid an FTC probe.

B. The Cybersecurity Act of 2015's Effect on Critical Infrastructure Cybersecurity Practices

1. Cybersecurity Act of 2015 Overview

At the end of 2015, Obama signed the "Consolidated Appropriations Act, 2016" into law containing a provision called the "Cybersecurity Act of 2015" ("Cybersecurity Act").[176] One of the Cybersecurity Act's goals is to increase the sharing of "cyber threat indicators, defensive measures, and information relating to cybersecurity threats" among the private sector and between the private sector and the federal government.[177] In passing the Cybersecurity Act, Congress had hoped that promoting voluntary information sharing between the private sector and government would help both parties improve their respective cybersecurity systems to protect America's CI, and by extension, homeland security.[178]

---

175. *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority (last visited May 20, 2016) ("The Commission may 'prosecute any inquiry necessary to its duties in any part of the United States' (FTC Act Sec. 3, 15 U.S.C. Sec. 43) and may 'gather and compile information concerning, and to investigate from time to time the organization, business, conduct, practices, and management of any person, partnership, or corporation engaged in or whose business affects commerce . . . .'").

176. Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2242, 2935-85 (codified at 6 U.S.C. §§ 1501-1532 (2017)).

177. 6 U.S.C. § 1502(a)(2) (2017).

178. *Id.*

Three aspects of the Cybersecurity Act impact the movement of information between the government and the private sector. A private entity may (1) monitor an information system for cybersecurity purposes, (2) operate defensive measures on the network to protect against a cyberattack, and (3) provide or receive cyber threat indicators.[179] Although much of the news surrounding the Cybersecurity Act has focused on data privacy concerns, the third aspect, information sharing, is the crux of the Cybersecurity Act in context of national security. If a private entity chooses to share a potential cyber threat, it must remove any "personal information of a specific individual or information that identifies a specific individual . . . not directly related to a cybersecurity threat" contained in the cyber threat indicator.[180] To encourage information-sharing among the private sector and with the federal government, the Cybersecurity Act has several private sector liability shields. First, private entities sharing cybersecurity information with one another will not be considered a violation of any antitrust laws.[181] Second, there can be no cause of action in any court for information sharing as long as the private entity submits the cyber threat information to the DHS.[182] This has the effect of putting the DHS in charge of implementing the Cybersecurity Act.

2. Evaluating the Cybersecurity Act's Effectiveness in Improving Private Sector Cybersecurity and Homeland Security

a. The Cybersecurity Act Misunderstands the Main Threat Facing Information Systems

While the Cybersecurity Act is a step in the right direction, emphasizing information-sharing as an effective means of improving CI cybersecurity and homeland security may be "too little, too late."[183] The imagined scenario where information-sharing would be beneficial is a business in the private sector receiving an e-mail containing malware. The business discovers and intercepts the malware and sends it to DHS, who then

179. *Id.* § 1501(15)(A) (defining a private entity as "any person or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity"); *id.* at § 1503(d)(1).

180. *Id.* § 1503(d)(2).

181. *Id.* § 1503(e)(1).

182. *Id.* § 1505(b).

183. Paul Rosenzweig, *The Cybersecurity Act of 2015*, LAWFARE (Dec. 16, 2015, 2:59 PM), https://www.lawfareblog.com/cybersecurity-act-2015.

examines the malware and forwards a summary of the email and malware to other government agencies and private sector business as a means of warning them about the threat.[184] There is one central problem with the Cybersecurity Act: it misunderstands the cyber threats currently facing the private sector and offers a solution that will likely prove ineffective on its own.

As one commentator put it, "cybersecurity through information sharing is like driving a car by looking in the rearview mirror."[185] The scenario detailed above assumes that there will be a finite number of unique "zero-day attacks," and that if enough of these attacks are shared among the private sector and government, they will be able to create blanket defenses against the threats in the event that cyber aggressors use the same malware in the future.[186] But in the current cyberspace climate, the majority of malware that target businesses *are* zero-day attacks in the form of advanced persistent threats ("APTs"), and there is not a finite number of threats.[187] APTs are "characterized by more sophisticated and concentrated efforts by coordinated attackers focused on a single target."[188] APTs are tailored to specific weaknesses in the target's IT system and can go undetected for months because they do not seek to cause damage to the system.[189] Instead, the hacker's goal is to siphon out sensitive information using APTs without leaving traces in the IT system.[190] This means that many businesses do not know they have been hacked until months after the fact.[191] If the threat is discovered, sharing the threat information with others in

184. Rodin, *supra* note 32, at 520.

185. DB Networks, *Cybersecurity Act of 2015 is Ineffective, Warns DB Networks*, PR NEWSWIRE (Dec. 29, 2015, 8:30 AM), http://www.prnewswire.com/news-releases/cybersecurity-act-of-2015-is-ineffective-warns-db-networks-300197479.html.

186. *Id.* (defining "zero-day attacks" as malware of first impression, the code for which no one has seen before).

187. *Id.*; Virginia Harrison & Jose Pagliery, *Nearly 1 Million New Malware Threats Released Every Day*, CNN MONEY (Apr. 14, 2015, 11:54 AM), http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/.

188. Ahmad Mukaram, *Cyber Threat Landscape: Basic Overview and Attack Methods*, RECORDED FUTURE (June 3, 2014), https://www.recordedfuture.com/cyber-threat-landscape-basics/.

189. Nate Lord, *What is an Advanced Persistent Threat? APT Definition*, DIGITAL GUARDIAN (Jan. 26, 2017), https://digitalguardian.com/blog/what-advanced-persistent-threat-apt-definition.

190. Mukaram, *supra* note 189.

191. *See* Rodin, *supra* note 32, at 520–21 ("According to an annual data-breach survey . . . an external party, such as the government, informed companies that they had been breached in seven out of ten cases.").

order to develop counter measures has been ineffective because of the continuous onslaught of unique APTs and the lag time between APT infection and discovery.[192] With hundreds of millions of new malware viruses being created each year, knowing about unique APTs will likely not offer any guidance to other businesses or agencies on future attacks, leaving the Cybersecurity Act as a drop in the water in fixing lagging CI cybersecurity and homeland security.[193]

b. Implementing the Cybersecurity Act is Clunky and Few Businesses Have Used It

The substantive portions of the Cybersecurity Act aside, implementing the Cybersecurity Act has so far proven difficult, and few companies have begun sharing information via the portal the DHS created. An analysis of the DHS's implementation of the Cybersecurity Act showed that the DHS has taken steps to implement certain provisions of the Cybersecurity Act.[194] The DHS, however, has a long way to go in rolling out a fully functional means of allowing businesses to share cyber threat information with the DHS with sufficient security measures to protect information flowing through its own channels.[195]

Statistics about the number of organizations taking part in the information-sharing initiative are also discouraging. Of approximately the 140 organizations connected to the DHS's Automated Indicator Sharing system, only one company has shared any information with the DHS.[196] There are several reasons why organizations are reluctant to share information with the DHS. First, some organizations, such as AT&T, have over a hundred petabytes of data flow through there IT systems, and so there is a challenging amount of data to look through to find the type of

192. DB Networks, *supra* note 186.

193. Harrison & Pagliery, *supra* note 188.

194. DEP'T OF HOMELAND SEC., OFFICE OF THE INSPECTOR GEN., REVIEW OF THE DEPARTMENT OF HOMELAND SECURITY'S IMPLEMENTATION OF THE CYBERSECURITY ACT OF 2015 (2016), https://www.oig.dhs.gov/assets/Mgmt/2016/OIG-16-142-Sep16.pdf.

195. *Id.* at 3 ("[N]ot all DHS components used data exfiltration protection capabilities to support data loss prevention, forensics and visibility, and digital rights management. Further, the Department had not developed policies and procedures to ensure that contractors implement data protection solutions.").

196. Robert Lemos, *Cyber-Threat Data Sharing Off to Slow Start Despite U.S. Legislation*, EWEEK (Oct. 2, 2016), http://www.eweek.com/security/cyber-threat-data-sharing-off-to-slow-start-despite-u.s.-legislation.html.

threat indicators to share with the DHS.[197] Second, as mentioned, organizations are still calculating what they hope to gain by spending resources on sharing information with the DHS to avoid a "free rider" situation.[198] And last, despite the liability shields that the Cybersecurity Act provides, cybersecurity information sharing is still in its infancy, which leaves organizations feeling uncertain about any liability issues might play out.[199] Overall, the DHS will need to assuage organizations' fears regarding information sharing, as well as discuss the benefits of information sharing with businesses that resist spending resources on scrubbing information of personal information and sharing it with the DHS.

V. BOARD OF DIRECTOR, C-SUIT, AND EMPLOYEE CYBER THREAT EDUCATION AS A MEANS OF IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

Instead of focusing solely on information sharing, the government should offer incentives to encourage the private sector to provide their employees with cyber threat education and training, and not to rely solely on technology or cybersecurity experts to bolster their cyber defenses.[200] In a 2014 interview, Michael Daniel, the White House cybersecurity coordinator and cybersecurity czar said that "[b]eing too down in the weeds at the technical level could actually be a bit of a distraction" in fighting cyberattacks.[201] Although his remark drew fire from online critics, he was right in the sense that concentrating on hyper-technical

197. Giuseppe Macri, *Only One Company is Using DHS's Automated Cyber Threat Sharing Portal*, INSIDE SOURCES (Sept. 26, 2016), http://www.insidesources.com/only-one-company-using-dhss-automated-cyber-threat-sharing-portal/.

198. *See* Dourado & Brito, *supra* note 72; *see also* Sales, *supra* note 15, at 1520 ("A company that secures itself against intruders makes it harder for assailants to commandeer its systems to attack others. Investments in cyber-defense thus effectively subsidize other firms. Because the investing company doesn't capture the full benefit of its expenditures, it has weaker incentives to secure its systems. And because other companies are able to free ride on the investing firm's expenditures, they have weaker incentives to adopt defenses of their own.").

199. Lemos, *supra* note 197.

200. Robert Gyenes, *A Voluntary Cybersecurity Framework is Unworkable—Government Must Crack the Whip*, 14 U. PITT. J. TECH. L. & POL'Y 293, 311 (2014).

201. Eric Chabrow, *Michael Daniel's Path to the White House*, GOVINFOSECURITY (Aug. 21, 2014), http://www.govinfosecurity.com/interviews/michael-daniels-path-to-white-house-i-2422.

cyber defenses actually misses the main cause of cyber breaches in America. CI named "human error" as a contributing factor in the breach in ninety-five percent of all cyber breach investigations throughout the U.S., with an estimated 91% of hacking attacks beginning with a phishing or spear-phishing email as opposed to SQL injection or other complex brute force hacking methods.[202] Whereas phishing "involves malicious emails sent to any random email account," spear-phishing is when a hacker targets a specific person and disguises a malicious email as coming from a legitimate or trusted source such as the recipient's bank.[203] In spear-phishing, the email often contains personal information about the recipient and other methods for gaining the recipient's trust, such as business logos or partial account numbers.[204] The email tricks the recipient into clicking a URL or downloading an attachment falsely named as something relevant to the recipient's job or personal life, allowing malware to penetrate the IT system.[205] Hackers use tactics such as spear-phishing to circumvent the technological defenses that many private sector businesses employ in favor of exploiting employees who are not trained in spotting such cyberattacks.[206] Although other forms of human error include "system misconfiguration, poor patch management, use of default usernames and passwords or easy-to-guess passwords," double-

202. Kim Zetter, *Hacker Lexicon: What Are Phishing and Spear Phishing?*, WIRED (Apr. 7, 2015, 6:09 PM), http://www.wired.com/2015/04/hacker-lexicon-spear-phishing/ (defining "spear phishing."); IBM GLOB. TECH. SERVICES, IBM SECURITY SERVICES 2014 CYBER SECURITY INTELLIGENCE INDEX: ANALYSIS OF CYBER ATTACK AND INCIDENT DATA FROM IBM'S WORLDWIDE SECURITY OPERATIONS 3 (2014), http://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf [hereinafter IBM CYBER ATTACK ANALYSIS]; *SQL Injection*, TECHOPEDIA, https://www.techopedia.com/definition/4126/sql-injection (last visited Mar. 7, 2017) ("An SQL injection is a computer attack in which malicious code is embedded in a poorly-designed application and then passed to the backend database. The malicious data then produces database query results or actions that should never have been executed.").

203. Trevor Hawthorn, *Why Spear Phishing is Your Biggest Cyber Security Threat*, WOMBAT SEC. (Dec. 9, 2015, 11:23 AM), https://info.wombatsecurity.com/blog/why-spear-phishing-is-the-biggest-cyber-security-threat-facing-companies-today; Zetter, *supra* note 203.

204. Hawthorn, *supra* note 204.

205. Zetter, *supra* note 203.

206. RANDY ABRAMS, NSS LABS, ANALYST BRIEF: USER EDUCATION EFFECTIVENESS CAN BE MEASURED 3 (2013), https://www.nsslabs.com/index.cfm/_api/render/file/?method=inline&fileID=147F2419-5056-9046-931A7C5CBB527A90.

clicking on an unsafe URL or email attachment remains the most prevalent cause of cyber breaches in the private sector.[207]

Governmental emphasis on private sector cyber threat education and training in conjunction with information-sharing would benefit CI cyber defenses in three ways. First, improved cyber threat education would increase the chance of employees recognizing emails containing malware so that they can report them to the DHS under the Cybersecurity Act. The Cybersecurity Act assumes that businesses are able to recognize and intercept malware before an employee downloads a malicious attachment or clicks a URL. However, this may not be the case. Through educating employees about hackers using social engineering to learn personal details about employees to tailor spear-phishing emails, businesses can improve their abilities to share cyber threat information with the government.[208] Second, cyber threat education would bridge the gap between lapses in technological cyber defenses and human error, which is where the bulk of hackers concentrate their efforts.[209] And last, the government could couch their efforts in language that would avoid the "free rider" issue that many businesses perceive when deciding to spend resources on information sharing pursuant to the Cybersecurity Act. The government could sell the cybersecurity education idea to the private sector as a means of helping avoid civil liability should a cyber breach occur and litigants file suit against the business for allegedly insufficient cybersecurity practices.

VI. CONCLUSION

Defending against a cyberattack that could shut down a U.S. nuclear reactor or power grid should be a priority in America's homeland security strategy.[210] The tension between competing private sector and federal government interests is a significant obstacle to homeland cybersecurity. The Cybersecurity Act could

---

207. IBM CYBER ATTACK ANALYSIS, *supra* note 203, at 3.

208. *Social Engineering—Definition*, KASPERSKY LAB, https://usa.kaspersky.com/internet-security-center/definitions/social-engineering#WKiUehIrLBI (last visited Mar. 7, 2017) ("Social engineering is a form of techniques employed by cybercriminals designed to lure unsuspecting users into sending them their confidential data, infecting their computers with malware or opening links to infected sites.").

209. Fran Howarth, *The Role of Human Error in Successful Security Attacks*, SEC. INTELLIGENCE (Sept. 2, 2014), https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/.

210. Gyenes, *supra* note 201, at 313–14.

be an effective tool in partially overcoming this difficulty if enough private sector businesses across the U.S. CI submit cyber threat information. But it remains to be seen whether information-sharing will be enough for the government to improve homeland cybersecurity without extensive non-voluntary legislation. The FTC's efforts under the FTC Act seem to be more effective. The FTC, however, has been reluctant to step outside of the technology and retail industries to prosecute businesses in other CI industries for unfair data security practices. Further, the *Wyndham* and *LabMD* cases may indicate the start of businesses declining to settle with the FTC, and instead challenging the FTC's prosecution authority for failing to provide reasonable data security standards that the FTC expects businesses to maintain.

When it comes to homeland security and safeguarding the U.S. CI, the government needs to be more assertive in aligning private sector's profit maximization aims with the government's goal of avoiding a 9/11-like cyber event.[211] Perhaps as the private sector begins to lose significant amounts of money to cyber breach litigation and increasing cyber insurance premiums and audits, the market will align private industry interests with the government's homeland security interests where the government has failed to do so.[212] Until such a time as the private sector takes the initiative to improve its cybersecurity, the onus is on the government to influence the private sector toward taking cybersecurity seriously in the name of national security.

211. Stockton & Golabek-Goldman, *supra* note 36, at 212–13.

212. Jim Finkle & Leigh Thomas, *Insurers in Dash for Expertise to Master Cyber Risk Insurance*, INS. J. (July 14, 2014), http://www.insurancejournal.com/news/national/2014/07/14/334442.htm.