Vanderbilt Journal of Entertainment & Technology Law

Volume 21
Issue 1 *Issue 1 - Fall 2018*

Article 6

2018

Corporate Cybersecurity: The International Threat to Private Networks and How Regulations Can Mitigate It

Eric J. Hyla

Corporate Cybersecurity: The International Threat to Private Networks and How Regulations Can Mitigate It

ABSTRACT

Cyberattacks are occurring at an accelerating pace. Foreign nations are increasingly utilizing hacking as a tool for economic gain, acts of aggression, or international political expression. At risk are US consumers' personal data, private firms' bottom line, and the economies' integrity. In response, federal and state lawmakers have issued a series of disparate, uncoordinated policies seeking to strengthen cybersecurity practices. However, recent events indicate that these policies are less than ideal. This Note suggests that a unified response to cybersecurity is required and calls for the establishment of a single, central federal agency with authority over all cybersecurity regulations. Such an agency would promulgate adequate and appropriate regulations to best protect sensitive data.

TABLE OF CONTENTS

On July 29, 2017, consumer credit reporter Equifax discovered it had been hacked by cybercriminals who obtained Social Security numbers, addresses, birth dates, and some credit card information of around 143 million Americans—nearly half the population of the

United States.[1] When Equifax announced the hack on September 7, 2017,[2] Americans were understandably angry—their most sensitive financial data was exposed and could potentially cause harm for years to come.[3] Though still incomplete, both internal investigations and US government probes have uncovered evidence that suggests the breach was conducted by foreign state-sponsored hackers.[4]

If the Equifax hack was indeed state sponsored, Equifax will not have been the first company targeted. Former FBI Director James Comey showcased the prolific nature of state-sponsored attacks, stating that "[t]here are two kinds of big companies in the United States[,] . . . those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese."[5] State actors[6]—including the United States[7]—have increasingly been behind major cyber-breaches, corporate or otherwise.[8] For example, in May 2017, a strain of ransomware dubbed "WannaCry" infected tens of thousands of entities across 150 countries.[9] Afflicted entities included healthcare

1. *See* Craig Timberg et al., *Data of 143 Million Americans – Nearly Half the Country – Exposed in Equifax Hack*, CHI. TRIB. (Sept. 8, 2017), http://www.chicagotribune.com/business/national/ct-equifax-data-breach-20170907-story.html [https://perma.cc/35ZU-33X2]; *U.S. and World Population Clock*, U.S. CENSUS BUREAU, https://www.census.gov/popclock/ [https://perma.cc/876P-7PZ5?type=image] (last visited Oct. 4, 2018) (projecting the US resident population to be 328,732,057).

2. *Equifax Announces Cybersecurity Incident Involving Consumer Information*, EQUIFAX (Sept. 7, 2017), https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628 [https://perma.cc/R32N-XG55].

3. *See* Ben Popken, *Equifax Fallout: FTC Launches Probe, Websites, and Phones Jammed with Angry Consumers*, NBC News (Sept. 13, 2017, 2:39 PM), https://www.nbcnews.com/business/consumer/equifax-melts-down-under-surge-angry-consumers-n800991 [https://perma.cc/W7KP-LK5P]; Michael Riley et al., *The Equifax Hack Has the Hallmarks of State-Sponsored Pros*, BLOOMBERG BUSINESSWEEK (Sept. 29, 2017), https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros [https://perma.cc/9KCP-GEAK];.

4. *See* Riley et al., *supra* note 3.

5. *See* James Cook, *FBI Director: China Has Hacked Every Big US Company*, BUS. INSIDER (Oct. 6, 2014, 6:24 AM), http://www.businessinsider.com/fbi-director-china-has-hacked-every-big-us-company-2014-10 [https://perma.cc/QP4K-9SAN]; *accord* Scott Pelley, *FBI Director on Threat of ISIS, Cybercrime*, CBS NEWS: 60 MINUTES (Oct. 5, 2014), https://www.cbsnews.com/news/fbi-director-james-comey-on-threat-of-isis-cybercrime/ [https://perma.cc/H3NS-HJN4].

6. For the purposes of this Note, the term "state actors" is defined to mean national governments, their agencies, or individuals acting on behalf of a government.

7. *See* Barton Gellman & Ellen Nakashima, *U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show*, WASH. POST (Aug. 30, 2013), https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html?utm_term=.e538bcbf8a74 [https://perma.cc/DCG8-BG28].

8. *See* Chris Colvin et al., *Cyber Warfare and the Corporate Environment*, 2 J.L. & CYBER WARFARE 1, 3–4 (2013).

9. *See* Ellen Nakashima, *The NSA Has Linked the WannaCry Computer Worm to North Korea*, WASH. POST (June 14, 2017), https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-

institutions, public utilities, and large corporations.[10] The virus worked by locking users out of infected systems, then ransoming off the key to regain control.[11] Following investigations, the National Security Agency (NSA) linked the creation of WannaCry to the North Korean government, claiming the ransomware was an attempt to raise revenue for the regime.[12]

As the proliferation of the internet connects more of the world, state-sponsored cyberattacks are on the rise[13]—a trend experts predict will not change.[14] Despite the increased incidence of state-sponsored cybercrime, the US government's response has been underwhelming. State legislatures have enacted laws enforcing cybersecurity measures; however, their efforts are not coordinated with other states, creating laws that lack parity with one another.[15] The federal response suffered the same issues due to various administrative agencies promulgating a patchwork of "sometimes redundant and often conflicting regulations."[16] The lackluster government response to cyberattacks has left cyber defense largely to the private sector, and the lack of a unified legal framework signals to the private sector a sense of regulatory ambivalence on the issue. Further, the lack of a unified framework unnecessarily increases difficulty and cost to comply with cybersecurity regulations, which could potentially cause some companies to cut corners on their security compliance.

Although legal frameworks are a necessary part of protecting sensitive data from cybercrimes, this alone is not enough. The

---

be25-3a519335381c_story.html?utm_term=.764a4a7ef88c [https://perma.cc/S3WW-VBZZ]; Lily Hay Newman, *The Ransomware Meltdown Experts Warned About is Here*, WIRED (May 12, 2017, 2:03 PM), https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/ [https://perma.cc/UV29-FN42].

10. *See* Lily Hay Newman, *The Biggest Cybersecurity Disasters of 2017 So Far*, WIRED (July 1, 2017, 10:00 AM), https://www.wired.com/story/2017-biggest-hacks-so-far/ [https://perma.cc/UV29-FN42].

11. *See* Newman, *supra* note 9.

12. *See* Nakashima, *supra* note 9.

13. *See* Mark Testoni, *License to Hack: State-Sponsored Hackers Are Upping the Ante*, HILL (Mar. 6, 2018, 9:00 AM), http://thehill.com/opinion/cybersecurity/376807-license-to-hack-state-sponsored-hackers-are-upping-the-ante [https://perma.cc/6RCF-7Q69].

14. *See* Warwick Ashford, *Infosec Pros Expect Increase in Nation State Cyber Attacks*, COMPUTER WKLY. (June 21, 2018, 2:57 PM), https://www.computerweekly.com/news/252443475/Infosec-pros-expect-increase-in-nation-state-cyber-attacks [https://perma.cc/WB4Y-LZZR].

15. *See* David Forscey et al., *Cybersecurity is the Next Frontier of State Regulation*, LAW360 (May 11, 2017, 1:26 PM), https://www.law360.com/articles/922786/cybersecurity-is-the-next-frontier-of-state-regulation [https://perma.cc/DS99-KEU3].

16. Jessie Bur, *Federal Cybersecurity Regulations Called Inconsistent, Redundant*, MERITALK (June 23, 2017, 2:11 PM) (quoting Senator Claire McCaskill), https://www.meritalk.com/articles/federal-cybersecurity-regulations-called-inconsistent-redundant-senate/ [https://perma.cc/VNL3-4Y65]; *accord* Forscey et al., *supra* note 15.

increasing complexity and frequency of foreign state-sponsored data breaches suggests that corporations alone are not doing enough to protect data from malicious actions by state actors, especially when companies could have prevented the two attacks described above by simply applying software patches when they became available.[17] This Note argues that nuanced federal regulation promulgated via a single administrative agency is required to best guarantee the safety of sensitive consumer data. Part I discusses the motives behind state-sponsored hacking, its potential impact on citizens, and current regulations. Part II examines strategy suggestions posed by the existing literature and politicians. Part III argues why the creation of an administrative agency, which can regulate and monitor corporate cybersecurity provides the best protection for citizens, corporations, and the US economy. Part IV offers concluding remarks, reiterating that a central administrative agency could improve protections for corporations and their customers.

I. BACKGROUND

A. Foreign State Motives to Hack Businesses

Perhaps the most obvious motivation of a state-sponsored cyberattack is economic gain. As previously discussed, the NSA believes North Korea launched WannaCry to directly fund their Reconnaissance General Bureau, the agency that conducts North Korea's cyber operations.[18] North Korea has also been linked to various cyber heists throughout Asia, including an $81 million heist from a Bangladeshi bank, achieved by altering the bank's online payment messaging system.[19]

Hard currency is not the only economic benefit to be obtained from cyber activities. China, for example, has expended significant efforts to obtain an enormous amount of intellectual property from US

17. *See* Matt Burgess, *Everything You Need to Know About EternalBlue – the NSA Exploit Linked to Petya*, WIRED (June 28, 2017), http://www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch [https://perma.cc/V8AE-RZ8E]; Lily Hay Newman, *Equifax Officially Has No Excuse*, WIRED (Sept. 14, 2017, 1:27 PM), https://www.wired.com/story/equifax-breach-no-excuse/ [https://perma.cc/5X2P-GUXP]. Equifax was initially hacked in May via a vulnerability in a web-application software that a software developer identified and patched in March. *See* Newman, *supra*. Equifax had over two months to fix the vulnerability but failed to do so. *See id.* Similarly, the WannaCry ransomware relied on exploiting a known Microsoft Operating System vulnerability named "EternalBlue," which was patched in a "critical" security update released on March 14, before WannaCry started to spread. *See* Burgess, *supra*.

18. *See* Nakashima, *supra* note 9 ("WannaCry was apparently an attempt to raise revenue for the regime . . . . [T]hough the hackers raised $140,000 in bitcoin . . . so far they have not cashed it in . . . .").

19. *See id.*

businesses.[20] Through intellectual property theft, the Chinese government is able to give its economy a competitive advantage by distributing US firms' research to Chinese businesses.[21] In an interview with NPR, James Lewis of the Center for Strategic and International Studies reported that "[y]ou can see the immediate economic benefit: You don't have to pay for the design, you can build it cheaper, and you can offer the same product at a lower price."[22] Indeed, the US Trade Representative estimates that "Chinese theft of American IP currently costs between $225 billion and $600 billion annually."[23]

The United States responded to China's unlawful cyber activity by publicly shaming the Chinese government and, in 2014, criminally indicting Chinese citizens for hacking US businesses.[24] Though the United States charged five Chinese military hackers with thirty-one counts each—including conspiring to commit computer fraud, computer hacking, economic espionage, and other offenses[25]—the move was "almost certainly symbolic since there is virtually no chance that the Chinese would turn over the five People's Liberation Army members named in the indictment."[26] The United States' use of public shaming and symbolic indictments is a testament to both the importance the

---

20. *See China's Cyber Threat a High-Stakes Spy Game*, NPR (Nov. 27, 2011, 6:03 PM), http://www.npr.org/2011/11/27/142828055/chinas-cyber-threat-a-high-stakes-spy-game?sc=tw [https://perma.cc/R7RJ-FHGS].

21. *See id.*

22. *Id.*

23. Scott J. Shackelford, *On Climate Change and Cyber Attacks: Leveraging Polycentric Governance to Mitigate Global Collective Action Problems*, 18 VAND. J. ENT. & TECH. L. 653, 655 (2016) ("[E]stimates on the [global] cost of cyber attacks range from approximately $400 billion in 2014 to more than $3 trillion by 2020."); Sherisse Pham, *How Much Has the US Lost from China's IP Theft?*, CNN (Mar. 23, 2018, 5:35 AM) (quoting the US Trade Representative), http://money.cnn.com/2018/03/23/technology/china-us-trump-tariffs-ip-theft/index.html [https://perma.cc/8TAQ-GFMH].

24. *See U.S. Charges Five Chinese Military Hackers for Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, U.S. DEP'T JUST. (May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor [https://perma.cc/X6DK-E4GH]; *China's Cyber Threat a High-Stakes Spy Game*, *supra* note 20.

25. *See* Indictment at 1–2, United States v. Wang Dong, No. 14-118 (W.D. Pa. May 1, 2014), https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf [https://perma.cc/4UT3-CSL4] ("From at least in or about 2006 up to and including at least in or about April 2014, members of the People's Liberation Army ('PLA'), the military of the People's Republic of China ('China'), conspired together and with each other to hack into the computers of commercial entities located in the Western District of Pennsylvania and elsewhere in the United States, to maintain unauthorized access to those computers, and to steal information from those entities that would be useful to their competitors in China, including state-owned enterprises ('SOEs')."); *U.S. Charges Five Chinese Military Hackers for Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, *supra* note 24.

26. Michael S. Schmidt & David E. Sanger, *5 in China Army Face U.S. Charges of Cyberattacks*, N.Y. TIMES (May 19, 2014), https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html [https://perma.cc/UT6T-5SAW].

government places on protecting its citizens from cybercrime and the difficulty of the task.

Foreign states may also be motivated to target businesses in order to conduct acts of terrorism or aggression. Due to increasing network interconnectivity, state-sponsored hackers and non-state-affiliated groups have committed cyberattacks of critical infrastructure—such as US financial institutions—as acts of "Postmodern Terrorism."[27] John Michael McConnell, former Director of National Intelligence, posited that "a successful attack on a large American financial institution 'would have an order-of-magnitude greater impact on the global economy than the Sept. 11, 2001, attacks.'"[28]

Other nations have clearly recognized the potential damage of cyberattacks.[29] Colonels of the Chinese People's Liberation Army included strategies for conducting cyberattacks against US financial institutions in a book about war tactics.[30] Additionally, in 2010, a hacker in Russia, who may or may not have been related to the Russian government,[31] breached the Nasdaq Stock Market and implanted malware designed to spy, steal data, and, if activated, cause "digital destruction."[32] Fortunately, the implanted malware never fulfilled its

---

27. Colvin et al., *supra* note 8, at 3. As an extreme example, Estonia's government was nearly crippled by cyberattacks traced to Russian officials working for Vladimir Putin after Estonia removed a World War II-era Soviet soldier statue from a park. *See* Mark Landler & John Markoff, *Digital Fears Emerge After Data Siege in Estonia*, N.Y. TIMES (May 29, 2007), http://www.nytimes.com/2007/05/29/technology/29estonia.html [https://perma.cc/V8KF-PFBD]. The attacks were particularly debilitating due to the high reliance Estonian citizens placed on the internet; vital government functions such as voting or paying taxes were impossible. *See id.* The Estonian defense minister compared the attacks to the country's "ports [being] shut to the sea." *Id.*

28. Tom C.W. Lin, *Financial Weapons of War*, 100 MINN. L. REV. 1377, 1388 (2016) (quoting John Michael McConnell).

29. *See id.* at 1396–97.

30. *See id.* at 1391 (citing QIAO LIANG & WANG XIANGSUI, UNRESTRICTED WARFARE: CHINA'S MASTER PLAN TO DESTROY AMERICA 120–23 (2002)).

31. *Compare* Stephanie Yang & Elena Holodny, *The Massive Hack of the Nasdaq That Has Wall Street Terrified of Cyber Attacks*, BUS. INSIDER (July 17, 2014, 3:37 PM), http://www.businessinsider.com/nasdaq-attacked-by-hackers-2014-7 [https://perma.cc/XS4Q-FK8R] ("By 2011, [the officials] had concluded that Russia wanted to imitate the Nasdaq exchange, and used the hack to collect information for their own stock exchanges."), *with* Jose Pagliery, *Russian Hackers Placed 'Digital Bomb' in Nasdaq – Report*, CNN (July 17, 2014, 3: 49 PM), http://money.cnn.com/2014/07/17/technology/security/nasdaq-hack/index.html [https://perma.cc/H4N2-2JQC] ("[T]hose familiar with the investigation say the more likely attacker is an independent Russian hacker from the city of St. Petersburg named Aleksandr Kalinin.").

32. Pagliery, *supra* note 31; *accord* Yang & Holodny, *supra* note 31.

destructive purpose,[33] but the fear of another Nasdaq breach lingers today.[34]

Russia is not the only foreign nation to target the US financial sector. In 2012, Iran carried out a cyberattack that resulted in major service disruptions to the online banking sites of many of the United States' largest banks.[35] Rather than attempt to steal money from the banks, the Iranian hackers employed use of a "botnet"[36] to conduct a Distributed Denial of Service[37] (DDoS) attack on the banks in retaliation for Western economic sanctions and the United States' involvement with a virus used to destroy Iranian Nuclear centrifuges.[38] Causing disruption or destruction when hacking financial institutions in lieu of stealing money is a hallmark of state-sponsored cybercrime.[39]

---

33. *See* Pagliery, *supra* note 31.

34. *See* Cameron Colquhoun, *Was the Nasdaq 'Glitch' Really Stock Market Warfare?*, WIRED (July 21, 2017), http://www.wired.co.uk/article/nasdaq-hack-july [https://perma.cc/3XT6-PSRJ] ("[A]s New York's financial community left their offices and headed for the beaches of the Hamptons or the cooler forests of Upstate, shock waves rippled through the markets. Just before 12.30 p.m. local time, the world's biggest stock exchange, Nasdaq, was displaying the stock prices of Amazon, Microsoft, Apple, and more than a dozen other companies at same price; $123.47. . . . The cause? Nasdaq claimed that 'erroneous third party test data' was behind the wild swings in stock prices. Whilst we should take Nasdaq at its word–that this was a simple error–it is vital to remember that Nasdaq had no other choice. Communicating any kind of hack or security breach would trigger a major market incident and, potentially, a financial crash similar to that of 2008. It is, nevertheless, incumbent to consider the alternatives, and explore the possibility that the 3 July resetting of share prices was a deliberate act.").

35. *See* Nicole Perlroth & Quentin Hardy, *Bank Hacking Was the Work of Iranians, Officials Say*, N.Y. TIMES (Jan. 8, 2013), http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html [https://perma.cc/5SZ8-6YST].

36. *See* Perlroth & Hardy, *supra* note 35. A botnet is a network of computers infected by "bots," or "web robots," which stealthily take control of infected machines. *See What is a Botnet?*, NORTON, https://us.norton.com/botnet/ [https://perma.cc/4WWW-H6P9] (last visited Sept. 22, 2018). The network can contain up to hundreds of thousands of machines, most infected without their owner's knowledge. *See id.* With the network at their disposal, the bot's master can use vast, global computing power to conduct various cybercriminal activities. *See id.*

37. Perlroth & Hardy, *supra* note 35; *see also* Swathi Padmanabhan, Note, *Hacking for Lulz: Employing Expert Hackers to Combat Cyber Terrorism*, 15 VAND. J. ENT. & TECH. L. 191, 197–98 (2012) (explaining the mechanics of a DDoS attack); *Understanding Denial-of-Service Attacks*, U.S. COMPUTER EMERGENCY READINESS TEAM (Feb. 6, 2013), https://web.archive.org/web/20180117112517/https://www.us-cert.gov/ncas/tips/ST04-015 [https://perma.cc/LW4G-VKXC] ("In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. . . . The most common and obvious type of DoS attack occurs when an attacker 'floods' a network with information. When you type a URL for a particular website into your browser, you are sending a request to that site's computer server to view the page. The server can only process a certain number of requests at once, so if an attacker overloads the server with requests, it can't process your request. . . . In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a website or send spam to particular email addresses.").

38. *See* Perlroth & Hardy, *supra* note 35.

39. *See id.*

The final motive considered behind foreign state hacking is to make a statement for political gain. A particularly salient example is the alleged Russian interference with the 2016 US presidential campaign. Here, Russian hackers targeted the Department of Homeland Security's election infrastructure before the November election, among other activities.[40] Though this Note does not posit the exact motives behind Russia's activities, its actions neither sought to destroy infrastructure nor achieve financial gain.[41]

A similar motive is evident in North Korea's 2014 hack of Sony Pictures Entertainment in response to the production of *The Interview*—a film in which James Franco and Seth Rogan play characters who attempt to assassinate a highly parodied Kim Jong Un.[42] In response, a North Korean-backed group, which called themselves "the Guardians of Peace," stole and leaked unreleased movies, personal employee information, and emails.[43] Moreover, the group threatened "9/11-type attacks on theaters that screen *The Interview*" and consequently disrupted the film's release through its threats.[44] The frequency and ease with which nations are utilizing cybercrime as a relatively effective means of international political expression suggests that those nations are unlikely to stop hacking any time soon.

B. Why Protections Are Vital

There are two primary arguments for why preventing cyber breaches against private-sector networks is vital: national security and consumer protection. First, businesses must shield themselves from hackers to ensure the physical and economic safety of the nation and its citizens. Nuclear power plants—which have already been targeted[45]—are a prime example of a private network that must be defended due to the physical devastation that could result from sabotage or other

40. *See 2016 Presidential Campaign Hacking Fast Facts*, CNN (July 18, 2018, 11:43 AM), http://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html [https://perma.cc/B82Y-V4WT].

41. *See id.* ("While the CIA assessment shows that the Russians may have sought to damage Clinton and help Trump, the FBI has yet to find proof that the attacks were orchestrated to elect the Republican candidate . . . .").

42. *See* Lori Grisham, *Timeline: North Korea and the Sony Pictures Hack*, USA TODAY (Jan. 5, 2015, 12:36 PM), https://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/ [https://perma.cc/VTP9-AJBV].

43. *See id.*

44. *Id.*

45. *See* Nicole Perlroth, *Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say*, N.Y. TIMES (July 6, 2017), https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html [https://perma.cc/S4YQ-FC5V].

cyberattacks. For example, hundreds of thousands of Ukrainians have twice lost power when Russian-backed hackers shut down their electrical grid.[46] In 2017, hackers with suspected Russian affiliations gained direct access to US power grid controls.[47] The hackers did not cut power to US citizens, but they could have.[48] The financial institutions discussed above are a less obvious but equally important example of a vulnerable network. If targeted, cyber attackers have the capacity to cripple the domestic and global economy.[49] As such, some scholars argue that "[f]inance may be the most powerful weapon of war."[50]

Due to the size, interconnectivity, and speed that transactions are conducted, modern financial institutions represent critical points to protect.[51] Should a foreign state cause one or multiple of those institutions to collapse, the financial harm to the United States could be more ruinous than the harms caused by the Great Recession.[52] The increased interconnectivity of other financial institutions, like venture capital firms, might create institutions which are "too linked to fail," in that the institutions are related to so many others that the failure of one could ripple across the system regardless of size.[53] Finally, transactions in the modern financial infrastructure occur in milliseconds, creating risks that failures in financial institutions might produce repercussions which are "too fast to save."[54] "Flash crashes" exemplify the concept of "too fast to save,"[55] the largest of which

46. *See* Andy Greenberg, *How an Entire Nation Became Russia's Test Lab for Cyberwar*, WIRED (June 20, 2017, 6:00 AM), https://www.wired.com/story/russian-hackers-attack-ukraine/ [https://perma.cc/J5L7-C6V8].

47. *See* Andy Greenberg, *Hackers Gain Direct Access to US Power Grid Controls*, WIRED (Sept. 6, 2017, 6:00 AM), https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/ [https://perma.cc/WB9H-4GBU].

48. *See id.* Experts believe that the hackers did not cut power to US consumers because they wanted to wait for a strategically opportune time to do so, such as in response to an armed conflict or as part of a threat to deter the United States from hacking into other countries' critical infrastructure. *See, e.g., id.*

49. *See supra* notes 20–23 and accompanying text.

50. *See, e.g.*, Lin, *supra* note 28, at 1377.

51. *See id.* at 1388 ("The modern financial infrastructure is subject to critical systemic risks and vulnerabilities due to its size, links, and speed.").

52. *See id.* at 1389.

53. *Id.* at 1389–90; *see also id.* at 1390 ("For instance, in 1998, the Federal Reserve initiated a $3.6 billion private bailout for Long-Term Capital Management, a hedge fund with fewer than two hundred employees, because its demise would have generated significant losses for many investment banks and caused widespread panic in the international financial markets. Since then, hedge funds and other financial intermediaries have only grown larger in size, volume, and importance, further exacerbating the risks of 'too linked to fail.'").

54. *Id.* at 1391–92.

55. *See id.*; Kimberly Amadeo, *Flash Crash Explained with Examples: Recent Examples and What Caused Them*, BALANCE (Feb. 23, 2018), https://www.thebalance.com/what-is-a-flash-crash-3306184 [https://perma.cc/V4TJ-FKF6]. A "flash crash" occurs when "a market . . . plummets

occurred May 6, 2010.[56] During the May 6th crash, the Dow Jones briefly lost a trillion dollars of market value in under an hour.[57] The market recovered shortly thereafter,[58] but the crash and others like it serve as a warning for the speed at which the financial sector might experience harms.

Second, it is vital to protect businesses from cyberattacks to safeguard consumer data. Financial harms to consumers from corporate hacks can be devastating partly because many large companies hold treasure troves of financial information. As of this writing, one woman has already had her identity stolen fifteen times as a result of the Equifax breach.[59] If a consumer's personal and financial information is compromised by a foreign state trying to generate revenue for its cyber activities, US consumers would bear the financial burden.[60]

Hacks can also violate consumer privacy as easily as they violate a consumer's bank account. Although some businesses allow consumers to volunteer the sensitive personal data they gather, like dating websites or social media,[61] some large businesses unilaterally obtain sensitive consumer data and profit by selling that data to companies.[62] Even when businesses only obtain consumer-volunteered data, consumers are so accustomed to providing their data to obtain products

---

within minutes, then rebounds. Different things can set it off, but computer trading programs make any crash worse." *Id.*

56. *See* Ben Rooney, *Trading Program Sparked May 'Flash Crash'*, CNN MONEY (Oct. 1, 2010, 2:56 PM), http://money.cnn.com/2010/10/01/markets/SEC_CFTC_flash_crash/index.htm [https://perma.cc/9MHG-YHSH]; Jill Treanor, *The 2010 'Flash Crash': How it Unfolded*, GUARDIAN (Apr. 22, 2015, 1:43 PM), https://www.theguardian.com/business/2015/apr/22/2010-flash-crash-new-york-stock-exchange-unfolded [https://perma.cc/MFD9-NHLH].

57. *See* Rooney, *supra* note 56; Treanor, *supra* note 56.

58. *See* Treanor, *supra* note 56.

59. *See Woman's ID Stolen 15 Times After Equifax Breach*, CNN (Oct. 29, 2017, 12:24 AM), https://web.archive.org/web/20171029110447/http://www.wafb.com/story/36709925/womans-id-stolen-15-times-after-equifax-breach [https://perma.cc/M7FR-7T27].

60. Such information could either be sold to a criminal or held for ransom back to the original owner, such as in WannaCry. *See supra* notes 9, 11 and accompanying text.

61. *See* Michael Zimmer, *OkCupid Study Reveals the Perils of Big-Data Science*, WIRED (May 14, 2016, 7:00 AM), https://www.wired.com/2016/05/okcupid-study-reveals-perils-big-data-science/ [https://perma.cc/2R27-SCRQ].

62. *See* Brian Naylor, *Firms Are Buying, Sharing Your Online Info. What Can You Do About It?*, NPR (July 11, 2016, 4:51 PM), http://www.npr.org/sections/alltechconsidered/2016/07/11/485571291/firms-are-buying-sharing-your-online-info-what-can-you-do-about-it [https://perma.cc/J3LE-66KK] ("They're called data brokers, and they collect all sorts of information — names, addresses, income, where you go on the Internet and who you connect with online. That information is then sold to other companies. There are few regulations governing these brokers. Some of the categories are innocuous — pet owner, or winter sports enthusiast. But . . . others were more problematic, like 'single mom struggling in an urban setting' or 'people who did not speak English and felt more comfortable speaking in Spanish' or 'gamblers.'").

or services that many do so willingly.[63] This is especially true with brands consumers trust.[64] As previous Ashley Madison users are aware, stolen social data can be as harmful as stolen financial data.[65] Exposed consumer data, whether financial or otherwise, harms individuals due to a corporation's failure to keep their data safe—creating a powerful incentive to ensure corporations employ the highest practicable standard of cybersecurity.

C. Review of Current Regulations

The federal government has issued several statutes that criminalize behaviors generally associated with cybercrime[66] but has passed nothing by way of overarching private sector cybersecurity regulation.[67] Various pieces of legislation, which may create or unify security standards, have been introduced in Congress but none have become law.[68] Congress is likely unable or unwilling to pass sweeping

---

63. *See* Steve Olenski, *For Consumers, Data Is a Matter of Trust*, FORBES (Apr. 18, 2016, 9:35 AM), https://www.forbes.com/sites/steveolenski/2016/04/18/for-consumers-data-is-a-matter-of-trust/ [https://perma.cc/P5GS-ACRF].

64. *See id.* ("Although the consumers who participated clearly understood which data was the most sensitive, including address, mobile phone number, name and date of birth, they were still willing (75%) to share it with companies in exchange for a product or service they value and a brand they trust. Even more consumers (80%) were positively influenced into sharing personal data with companies when they received special offers or data-enabled benefits.").

65. *See* Jose Pagliery, *Now You Can Search the Ashley Madison Cheaters List*, CNN (Aug. 19, 2015, 1:06 PM), http://money.cnn.com/2015/08/19/technology/ashley-madison-search/index.html [https://perma.cc/V69Q-DHA7] ("The stolen database of 32 million people who used cheating website Ashley Madison has made its way to the Web. And it's easily searchable on several websites. . . . Many of the cheaters exposed in this hack serve in the U.S. military, evident because they used email addresses that end in the .mil domain. Adultery does, in fact, violate Uniform Code of Military Justice. It's a prosecutable offense that can land you a year in confinement and a dishonorable discharge. What about people who used Ashley Madison to engage in gay affairs? The website's users were worldwide, and there are 79 countries where homosexuality is illegal. In Afghanistan, Iran, Mauritania, Nigeria, Qatar, Saudi Arabia and the United Arab Emirates, the punishment is death.").

66. *See* Identity Theft and Assumption Deterrence Act, Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified as amended at 18 U.S.C. § 1029); Computer Fraud and Abuse Act, Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified as amended at 18 U.S.C. § 1030); Wiretap Act, Pub. L. No. 90-351, 82 Stat. 197 (1968) (codified as amended at 18 U.S.C. § 2511; Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. § 2701); Stephanie Balitzer, Note, *What Common Law and Common Sense Teach Us About Corporate Cybersecurity*, 49 U. MICH. J.L. REFORM 891, 901–04 (2016).

67. *See* Michael Hooker & Jason Pill, *You've Been Hacked and Now You're Being Sued: The Developing World of Cybersecurity Litigation*, 90 FLA. B.J. 31, 37 (2016) ("A few of these regulatory initiatives have encountered stiff resistance due, in part, to the absence of any overarching federal legislation to regulate cyber-security liability and the lack of a uniform standard for private-sector cybersecurity programs."); Evan M. Wooten, *The State of Data-Breach Litigation and Enforcement: Before the 2013 Mega Breaches and Beyond*, 24 J. ANTITRUST & UNFAIR COMPETITION L. SEC. ST. B. CAL. 229, 239 (2015) ("Congress has yet to address data security in the private sector or to set (or authorize) mandatory standards . . . .").

68. *See* Hooker & Pill, *supra* note 67, at 40 n.53.

legislation because a one-size-fits-all approach to cybersecurity would be impractical and incapable of adjusting to increasingly sophisticated attacks.[69]

Federal agencies have implemented scattered regulations, all of which possess unmistakable drawbacks. For example, the Cybersecurity Enhancement Act[70] authorizes the National Institute of Standards and Technology (NIST) to develop data security standards. However, adherence to those standards is entirely voluntary for members of the private sector.[71] Similarly, the Department of Homeland Security has implemented an information-sharing program pursuant to the Cybersecurity Act of 2015.[72] This program is also voluntary, was slow to initiate, and has garnered few participants.[73]

The Federal Trade Commission (FTC) has enacted seemingly mandatory standards, but they are loosely defined.[74] Nevertheless, the FTC has successfully settled with over fifty companies for having "unfair data security practices" and required them to (1) create a comprehensive security program designed to address security risks related to developing and managing services for consumers and (2) protect the security and confidentiality of consumer information.[75] While the FTC's authority related to unfair practices expands to almost

---

69. *See* James Eastman, Note, *Avoiding Cyber-Pearl Harbor: Evaluating Government Efforts to Encourage Private Sector Critical Infrastructure Cybersecurity Improvements*, 18 COLUM. SCI. & TECH. L. REV. 515, 545 (2017).

70. *See* Cybersecurity Enhancement Act, Pub. L. No. 113-274, § 201, 128 Stat. 2971, 2974 (2014) (codified as amended 15 U.S.C. § 7431 (2012)).

71. *See* Wooten, *supra* note 67, at 239 ("The new data-security bills only affect federal agencies and any critical infrastructure standards promulgated by NIST will be voluntary.").

72. *See* Cybersecurity Act of 2015, Pub. L. No. 114-113, div. N, 129 Stat. 2242, 2936–80 (2015) (codified as amended 6 U.S.C. §§ 1501–1532 (2017)); U.S. DEP'T. OF HOMELAND SEC., CRITICAL INFRASTRUCTURE THREAT INFORMATION SHARING FRAMEWORK: A REFERENCE GUIDE FOR THE CRITICAL INFRASTRUCTURE COMMUNITY 1 (2016), https://www.dhs.gov/sites/default/files/publications/ci-threat-information-sharing-framework-508.pdf [https://perma.cc/NU43-AYXS]; *Cyber Information Sharing and Collaboration Program (CISCP)*, U.S. DEP'T HOMELAND SECURITY (Aug. 31, 2018), https://www.dhs.gov/ciscp [https://perma.cc/N6Q9-U8QW].

73. *See* Eastman, *supra* note 69, at 546, 549.

74. *See* Andrea Arias, *The NIST Cybersecurity Framework and the FTC*, FED. TRADE COMMISSION (Aug. 31, 2016, 2:34 PM), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc [https://perma.cc/W62J-229F]. The FTC suggests that complying with the NIST Cybersecurity framework is consistent with the FTC's process-based approach the FTC employs to determine whether a firm has met their minimal security requirements but maintains that the true is that of "reasonableness." *Id.* ("[T]he touchstone of the FTC's approach to data security has been reasonableness . . . in light of the volume and sensitivity of information the company holds, the size and complexity of the company's operations, the cost of the tools that are available to address vulnerabilities, and other factors.").

75. *See* Eastman, *supra* note 69, at 535, 537.

any industry,[76] 15 U.S.C. § 45(n) prohibits the FTC from prosecuting unless the security measures are "likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[77] The US Court of Appeals for the Eleventh Circuit recently questioned the FTC's expansive interpretation of § 45(n), suggesting the agency's oversight may be further curtailed in the future.[78] It is unsurprising that the FTC faces increased difficulties promulgating regulations relative to other administrative agencies, given the FTC's history of being disciplined for agency overreach.[79]

While Congress has failed to pass legislation regarding cybersecurity standards, states are enacting their own.[80] The statutes generally focus exclusively on consumer data security and utilize some type of reasonableness standard.[81] The statutes vary, however, in both the type of data requiring protections and what qualifies as a "reasonable" level of protection—thereby creating a patchwork of incongruous regulations, which may prove too burdensome for some businesses to navigate.[82] Most of the statutes also fail to address operational security procedures,[83] an unfortunate oversight when "over 95 percent of all incidents investigated [by IBM's Managed Security Services] recognize 'human error' as a contributing factor."[84]

II. ANALYSIS

Recent breaches have proven that consumer data is vulnerable and privacy concerns are valid.[85] In a landscape featuring few

---

76. *See* 15 U.S.C. § 45(a)(2) (2018) ("The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.").

77. 15 U.S.C. § 45(n).

78. *See* LabMD, Inc. v. FTC, 678 F. App'x 816, 820–21 (11th Cir. 2016).

79. *See* J. Howard Beales, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, FED. TRADE COMMISSION (May 30, 2003), https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection [https://perma.cc/LT98-6ZFA]. After a striking example of agency overreach, Congress shut down the FTC for several days and introduced legislation limiting the FTC's ability to promulgate unfairness rulemakings. *See id.*

80. *See* Forscey et al., *supra* note 15.

81. *See id.*

82. *See id.*

83. *See id.* Operational cybersecurity consists of actions of people, purposeful or mistaken; systems and technology failures; failed internal processes; and external events, such as natural disasters, legal issues, or service provider dependencies. *See* JAMES J. CEBULA & LISA R. YOUNG, SOFTWARE ENG'G INST., A TAXONOMY OF OPERATIONAL CYBER SECURITY RISKS 2 (2010).

84. IBM GLOB. TECH. SERVS., IBM SECURITY SERVICES 2014 CYBER SECURITY INTELLIGENCE INDEX 1, 3 (2014) [hereinafter IBM REPORT].

85. *See supra* Section I.B.

comprehensive regulations[86] and hitherto inefficient consumer protections, one question remains: What, if anything, should be done to improve consumer safety regarding cybersecurity vulnerabilities? This Part provides an analysis of three potential solutions. Section A discusses an elective partnership between the private sector and the federal government. Section B considers the military assuming total responsibility and control of private sector cybersecurity. Section C analyzes a system in which the federal government mandates rigorous minimum cybersecurity standards for the private sector.

A. Public-Private Cybersecurity

The first possible solution is to leave the responsibility to protect consumer data in the hands of the private sector, who would be motivated by economic pressures or government encouragement. "Public-private cybersecurity" is the de facto system of cyber defense, which is "characterized by the surprisingly important, quasi-governmental role of the private sector on many important cybersecurity issues, and correspondingly, by instances in which the federal government acts more like a market participant than a traditional regulator."[87] The theory is wildly popular with government officials,[88] private sector representatives, and the media.[89] In fact, the strategy even received endorsement by President Obama during his remarks at the National Cybersecurity Communications Integration Center.[90]

The partnership has been one of convenience for the government for two key reasons. First, cooperation with private firms makes sense for the government because the United States' critical national cyber infrastructure is owned, operated, and protected by the private sector.[91]

---

86. *See supra* Section I.C.

87. Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 470–71 (2017).

88. *See id.* at 469–70. Navy Adm. Mike Rogers, director of the NSA and the commander of the US Cyber Command, stated it was unrealistic for either the private sector or the government alone to withstand against cyberattacks; cooperation is needed. *See* Cheryl Pellerin, *Cybercom Commander: Public-Private Partnerships Needed for Cybersecurity*, U.S. DEP'T DEF. (Nov. 16, 2016), https://www.defense.gov/News/Article/Article/1006807/cybercom-commander-public-private-partnerships-needed-for-cybersecurity/ [https://perma.cc/LGU2-EAMS].

89. Eichensehr, *supra* note 87, at 469–70.

90. *See* President Barack Obama, Remarks by the President at the National Cybersecurity Communications Integration Center (Jan. 13, 2015) ("Most of [our critical] infrastructure is owned and operated by the private sector. So neither government, nor the private sector can defend the nation alone. It's going to have to be a shared mission—government and industry working hand in hand, as partners.").

91. *See* Justin S. Daniels & Joe D. Whitley, *Cybersecurity Public Private Partnerships: Challenges and Opportunities*, L.J. NEWSL. (Feb. 2017), http://www.lawjournalnewsletters.com/

Receiving cooperation from targeted firms is vital because the government needs full access to a firm's network and data to investigate attacks and strengthen defenses.[92] Cooperation and information sharing is important because it is both prohibitively expensive and currently against the law for the NSA to monitor privately owned critical infrastructure.[93] With appropriate private participation, the government need not spend the resources or create new laws to monitor critical infrastructure.

The second point of convenience for the government is that the private sector is able to perform tasks that would be difficult—either structurally or politically—for the government to perform itself. For example, in recent years, the private sector has been quick to publicly attribute cyber intrusions to state-sponsored actors—often based on data provided to the firm by the US government[94]—when the US government would have otherwise been reluctant to do so.[95] The process is useful because the government can circumvent political issues involving accusations and avoid relying upon classified information, but still open dialogue with the offending country.[96] As another example, the private sector can help the government monitor compliance to agreements struck between nations.[97] Cybersecurity companies were instrumental in monitoring China's compliance with a 2015 agreement between China and the United States regarding cyber theft of trade secrets.[98]

The private sector has enjoyed some success in protecting itself. Some of the most successful examples of private and public sector cooperation have been botnet takedowns.[99] Microsoft pioneered the technique in 2010 when it took down the Waldec botnet.[100] It was not until over a year later that the US government, using tactics similar to

---

sites/lawjournalnewsletters/2017/02/01/cybersecurity-public-private-partnerships-challenges-and-opportunities/ [https://perma.cc/48QH-R6GC].

92. *See* Pellerin, *supra* note 88.

93. *See id.*

94. *See* Eichensehr, *supra* note 87, at 490–91.

95. *See id.* at 489.

96. *See id.* at 489 n.108.

97. *See id.* at 492.

98. *See id.*

99. *See* GEORGE WASHINGTON UNIV., CTR. FOR CYBER & HOMELAND SEC., INTO THE GRAY ZONE: THE PRIVATE SECTOR AND ACTIVE DEFENSE AGAINST CYBER THREATS 12 (2016), https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL.pdf [https://perma.cc/8GGZ-8KBT] [hereinafter GRAY ZONE REPORT].

100. *See* Nick Wingfield & Ben Worthen, *Microsoft Battles Cyber Criminals*, WALL ST. J. (Feb. 26, 2010, 12:45 PM), https://www.wsj.com/articles/SB10001424052748704240004575086523786147014 [https://perma.cc/8QS6-3KLK].

Microsoft's, took down its first botnet.[101] Since then, Microsoft has collaborated with the FBI and federal police forces[102] in other countries to take down many other nets.[103] Microsoft has received criticism for its participation in the operations;[104] nevertheless, companies and the government have embraced collaboration while taking down botnets, creating a "new normal" for botnet removal.[105]

Another space in which governments and firms have been teaming up, though not always in good moral conscience,[106] is in the acquisition of zero-day vulnerabilities.[107] Zero-day vulnerabilities are vulnerabilities in a system that are unknown to the software vendor and are therefore available for exploitation by whoever might know of its existence.[108] Because the developers are unaware of the vulnerability, they have yet to create a patch for it and all systems running the software are targetable.[109] When seeking to acquire zero-

101. *See* Eichensehr, *supra* note 87, at 480.

102. *See, e.g.*, Cory Bennett, *Officials Break Up Global Ring of 1m Infected Computers*, HILL (Dec. 4, 2015), http://thehill.com/policy/cybersecurity/262087-officials-break-up-global-ring-of-infected-computers [https://perma.cc/FD8L-UEVJ] ("The FBI said Microsoft assisted the Dorkbot takedown, which also included help from the European Cybercrime Center and the Interpol Digital Crime Center.").

103. *See* Microsoft Corp. v. John Does 1-8, No. 1:14cv811 LOG/TCB, 2014 WL 12575722, at *4–5 (E.D. Va. June 27, 2014) (enjoining defendants from operating the Shylock botnet); Microsoft Corp. v. John Does 1-18, No. 1:13cv139 (LMB/TCB), 2014 WL 1338677, at *11 (E.D. Va. Apr. 2, 2014) (permanently enjoining defendants from operating the Bamital botnet); Microsoft Corp. v. John Does 1-82, No. 3:13-cv-319, 2013 WL 2632612, at *5–6 (W.D.N.C. June 10, 2013) (enjoining the defendants from operating the Citadel botnet); Bennett, *supra* note 102 (reporting that Microsoft helped take down the "Dorkbot" botnet, which infected over one million computers in 190 countries); Jonathan Camhi, *How Microsoft & FS-ISAC Are Attacking Malware Threats*, INFORMATIONWEEK: BANK SYS. & TECH. (Oct. 6, 2014), http://www.banktech.com/security/how-microsoft-and-fs-isac-are-attacking-malware-threats/d/d-id/1316382.html [https://perma.cc/5KFX-HR8A]; *FBI and Microsoft Take Down $500m-Theft Botnet Citadel*, BBC (June 6, 2013), http://www.bbc.com/news/technology-22795074 [https://perma.cc/TUV2-SY9H] (reporting that Microsoft helped take down the "Citadel" botnet, which was responsible from stealing more than $500 million from bank accounts and infected around five million machines).

104. *See* Antone Gonsalves, *Microsoft Criticized for Botnet Takedown Tactics*, CSO ONLINE (June 13, 2013), https://www.csoonline.com/article/2133617/malware-cybercrime/microsoft-criticized-for-botnet-takedown-tactics.html [https://perma.cc/FD2J-XLUD].

105. *See* Eichensehr, *supra* note 87, at 481; Leslie R. Caldwell, *Assistant Attorney General Leslie R. Caldwell Delivers Remarks at the Georgetown Cybersecurity Law Institute*, U.S. DEP'T JUST. (May 20, 2015), https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-georgetown-cybersecurity [https://perma.cc/F2KL-T5TY].

106. *See* Eichensehr, *supra* note 87, at 483 ("[C]ompanies have built business models selling not just to the U.S. government but also to other companies and governments around the world, including governments with poor human rights records."). Even when obtained by the NSA, the purpose of the acquisition is morally dubious. The agency is known to pay off software and hardware companies to not disclose known vulnerabilities or backdoors so the NSA can continue to exploit them. *Id.* at 485.

107. *See id.* at 482–83.

108. *See id.* at 482.

109. *See id.*

day vulnerabilities, the NSA either browses the black market[110] to buy vulnerabilities themselves, or pays other companies like defense contractors to obtain vulnerabilities as an intermediary.[111] The Department of Defense has also placed a "bug bounty"[112] on itself called "Hack the Pentagon," a $150,000 program in which the government paid private hackers to find and report over one hundred vulnerabilities.[113]

The public-private cybersecurity strategy is not without its flaws, the first of which is the private sector's loose commitment to sharing information with the government. While corporations have been generally willing to share information *after* a breach has occurred,[114] their willingness to share information *before* consumer data has been compromised is questionable.[115] Illustrative of this issue is the abysmal corporate participation rate with the Department of Homeland Security's Cyber Information Sharing and Collaboration Program.[116] Namely, as of October 2016, only one of the 140 organizations connected to the system shared any significant amount of information.[117] An ideal system would prevent firms' systems from being compromised in the first instance. It is of little comfort to the consumer when corporations seek government assistance only after the consumer's sensitive information has been stolen. Similarly, intuition suggests that it would be less efficient to remedy an economic crash caused by the loss of a major financial institution than it would be to prevent that loss initially.

---

110. *See id.* Sometimes the vulnerabilities market is labeled as the "gray market" since buyers and sellers are presumptively conscionable actors, though that is not always the case. *Id.* at 483.

111. *See id.* at 482–83.

112. *Id.* at 488. A bug bounty is a program through which entities invite white-hat hackers to attempt to breach the firm's systems in hopes that the hackers will find and report the bugs to the firm in exchange for a cash reward. *See Bug Bounty*, TECHOPEDIA, https://www.techopedia.com/definition/28637/bug-bounty [https://perma.cc/K59J-X69R] (last visited Oct. 5, 2018).

113. *See* Lisa Ferdinando, *Carter Announces 'Hack the Pentagon' Program Results*, U.S. DEP'T DEF. (June 17, 2016), https://www.defense.gov/News/Article/Article/802828/carter-announces-hack-the-pentagon-program-results/ [https://perma.cc/AB2M-HDVN].

114. *See* Pellerin, *supra* note 88. For example, Sony "had no issue at all" in providing the NSA access to their networks after they were hacked in 2014 by North Korea. *Id.*

115. *See id.* During his talk at the Wall Street Journal's CEO Council annual meeting, then-Navy Admiral Michael S. Rogers took a poll as to whether the CEOs in attendance trusted the government enough to work with them during a cyberattack; 34 percent said 'only if their company was attacked' and 9 percent said 'never.' *Id.* The survey, admittedly with sample size and selection issues, demonstrates that at least a noninsignificant number of corporate CEOs would not proactively volunteer to work with the government to prevent breaches.

116. *See* Eastman, *supra* note 69, at 549.

117. 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 [https://perma.cc/4NSH-VCVN].

The second flaw in the public-private cybersecurity system concerns consumer safety more than critical infrastructure. It is one of tangled public law values—chiefly, the lack of accountability and transparency.[118] The private sector is not beholden to the same transparency standards by which the government carries out its cybersecurity policies.[119] Without such mechanisms, private cybersecurity policies are entirely opaque—preventing concurrent public oversight and eliminating the possibility of ongoing accountability.[120]

One could argue that while the public-private strategy lacks ongoing accountability, private actors face accountability via retroactive means such as market reactions or private lawsuits.[121] However, the efficacy of such retroactive accountability is dubious. A 2016 study by RAND Corporation found that after a firm has been breached, only 11 percent of respondents stopped shopping with that firm.[122] The RAND study contends "[t]hat the overwhelming majority of consumers (89 percent) continue to do business with the breached company appears to provide little incentive for the company to change its behavior, especially with regard to cybersecurity protection or defenses."[123] Because private actors have largely escaped currently available accountability mechanisms,[124] consumer data is at risk. While it would be extreme to require private firms to publicly disclose all information on their security measures, an improved accountability system would need to be implemented to adequately protect consumer information in the first instance.

B. Militarized Cybersecurity

The second possible solution is for the military to assume responsibility for defending all US cyberspace. Unlike the widespread support for a public-private cybersecurity partnership scheme, support for militarized cybersecurity has been almost non-existent in academic

---

118. *See* Eichensehr, *supra* note 87, at 511–12.

119. *See id.* at 515.

120. *See id.* at 512–14.

121. *See id.* at 513–14.

122. LILLIAN ABLON ET AL., RAND CORP., CONSUMER ATTITUDES TOWARD DATA BREACH NOTIFICATIONS AND LOSS OF PERSONAL INFORMATION 26 (2016).

123. *Id.* at 27. A counterargument is that the apathetic consumer response suggests that a change in cyber regime is not needed since consumers do not care that their information was breached. This argument ignores the fact that, in practice, switching firms might be prohibitively costly. *See id.* at 26.

124. *See* Eichensehr, *supra* note 87, at 514.

legal literature and lackluster at best among government officials.[125] That is not to say that this approach has been entirely unsupported. In early 2017, then President-elect Donald Trump "called for stepped-up efforts to combat cyber-crime and protect critical infrastructure, including greater involvement by the Defense Department."[126]

There are conceptual reasons as to why some might call for a militarized approach—the vulnerabilities and increased importance of critical infrastructure[127] are often cited as the next frontier in the evolution of warfare[128]—but no argument in favor of militarized cybersecurity for the private sector serves to alleviate the many flaws this approach presents. First, it is currently structurally impossible to implement a completely militarized approach to corporate cybersecurity. Although the US government implemented rigorous defenses for its own systems and seeks to disrupt criminal activity in cyberspace,[129] "no element of the U.S. Government, including the military, has adequate organization or resources to meet the challenge of defending American economic interests in cyberspace."[130]

Second, the US public is uncomfortable with the idea that the government monitors too much personal information.[131] A national

125. *See* Sean Lawson, *Is the United States Militarizing Cyberspace?*, FORBES (Nov. 2, 2012, 6:00 AM), https://www.forbes.com/sites/seanlawson/2012/11/02/is-the-united-states-militarizing-cyberspace/#261f7263798d [https://perma.cc/RBV4-LWBY]. In 2010, for example, Senator John McCain called for the Department of Defense to assume a greater role in national cybersecurity, but his call was resisted by General Keith Alexander, then-Commander of the United States Cyber Command. *See id.*

126. Paul Merrion, *McCaul Says Pentagon Role in Civilian Cybersecurity Would Be a 'Mistake'*, CQ ROLL CALL (Jan. 12, 2017) (2017 WL 115625). House Homeland Security Chairman Michael McCaul was quick to dismiss the idea as a mistake. *See id.*

127. *See supra* notes 27–44 and accompanying text.

128. *See, e.g.*, Lin, *supra* note 28, at 1381 ("[Critical infrastructure] presents an extremely valuable battle space for our adversaries because they may be able to plunder funds for their efforts and cause widespread financial panic and crisis simultaneously. Unlike Wartime theaters, the financial theater of war is less defined by geography and more by its critical functions, assets, and liabilities.") (footnote omitted).

129. *See* U.S. DEP'T OF HOMELAND SEC., CYBERSECURITY STRATEGY 3 (2018), https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf [https://perma.cc/43U8-E967].

130. Matteo G. Martemucci, *Unpunished Insults—The Looming Cyber Barbary Wars*, 47 CASE W. RES. J. INT'L L. 53, 60 (2015).

131. *See* Mary Madden, *Americans' Views on Government Surveillance Programs*, PEW RES. CTR.: INTERNET & TECH. (Mar. 16, 2015), http://www.pewinternet.org/2015/03/16/americans-views-on-government-surveillance-programs/ [https://perma.cc/JXL8-ZAZY]. Fifty-two percent of Americans were either "very concerned" or "somewhat concerned" about the government's surveillance of Americans' data and electronic communications. *Id.* Further, while Americans are comfortable with surveilling others, only 40 percent of the people polled thought it was acceptable to monitor ordinary US citizens. *Id.* Moreover, individuals maintain a strong expectation of privacy against government intrusions in personal records, as well as information stored "into a corporation's computer." *See* Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society"*, 42 DUKE L.J. 727, 762 (1993).

debate regarding the acceptable amount of personal data collected by the government ensued after Edward Snowden leaked the quantity and type of data collected by the NSA's PRISM program.[132] As a military support agency and part of the Department of Defense,[133] the NSA's collection of data for PRISM is analogous to military collection of data for cybersecurity, as both would be by the military for the sake of national defense. Because the government needs full access to a firm's networks and data to monitor its cybersecurity,[134] the public would likely raise privacy concerns similar to those raised regarding the government's PRISM program.[135]

Finally, the militarization of cyber defense could raise international law concerns, especially if the government engaged in "hacking back"[136] or other more aggressive active defenses when the aggressor is a foreign nation.[137] In a worst-case scenario, the government's potential mismanagement of private sector cybersecurity could justify a physical armed response from another nation.[138] Though

---

132. Edward Snowden revealed that the NSA could directly access the systems of "internet giants" to obtain data on consumers. *See* Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google, and Others*, GUARDIAN (June 7, 2013, 3:23 PM), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [https://perma.cc/68NN-WTJU]; T.C. Sottek & Janus Kopfstein, *Everything You Need to Know About PRISM: A Cheat Sheet for the NSA's Unprecedented Surveillance Programs*, VERGE (July 17, 2013, 1:36 PM), https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet [https://perma.cc/47S8-J7ZX]. As a result of the revelations, debate engulfed Congress about the legality of the data collections, private parties challenged the program in courts, and "Restore the Fourth" rallies were held in over one hundred cities on July 4, 2013. *See* Sottek & Kopfstein, *supra*.

133. *See Support to the Military*, U.S. NAT'L SECURITY AGENCY (May 3, 2016), https://www.nsa.gov/what-we-do/support-the-military/ [https://perma.cc/YZ4B-7B8Z] ("The National Security Agency is part of the U.S. Department of Defense, serving as a combat support agency. Supporting our military service members around the world is one of the most important things that we do.").

134. *See* Pellerin, *supra* note 88.

135. *See* Martemucci, *supra* note 130, at 60 (stating that "deep concern" by the public over perceptions of the NSA in the wake of Snowden leaks would further complicate military control of private-sector cybersecurity); *President Obama's Dragnet*, N.Y. TIMES (June 6, 2013), http://www.nytimes.com/2013/06/07/opinion/president-obamas-dragnet.html [https://perma.cc/FS7R-X3ME] ("Mr. Obama is proving the truism that the executive branch will use any power it is given and very likely to abuse it.").

136. "Hacking back" is defined as conducting operations intended to destroy external networks or information. GRAY ZONE REPORT, *supra* note 99, at 10.

137. *See* U.N. Charter art. 2, ¶ 4. Hacking back is likely permissible as self-defense if the first breach counts as an "armed attack," but no standard of practical use exists that defines when a cyber operation rises to that level. *See* Michael N. Schmitt, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum*, 8 HARV. NAT'L SECURITY J. 239, 244, 246 (2017) ("[T]he answer lies in the 'scale and effects' of the operation, a standard drawn from the *Nicaragua* judgment. Unfortunately, the standard is, albeit accurate as a matter of law, of little practical use.") (footnote omitted).

138. *See* Schmitt, *supra* note 137, at 245 ("[W]hen a state is the target of harmful cyber operations that rise to the level of an armed attack, it may respond with kinetic or cyber operations that would otherwise constitute prohibited uses of force in violation of article 2(4) of the UN

cybersecurity is important to defend, a militarized approach is structurally and politically inefficient to a degree that fatally undermines any argument in its favor.

C. Regulated Cybersecurity

Rather than act as partner to facilitate cybersecurity in the public-private partnership model, or usurp total control of cybersecurity measures in the militarized system, the third solution is for the government to pass legislation requiring adequate cybersecurity measures from firms. Legislatures have called for and passed such statutes, in at least a minor form, in nearly all states,[139] but similar statutes have gained little ground in the federal government.[140] Specifically, New York[141] and California[142] state legislatures have taken the lead to enact more comprehensive legislation.

The legislative landscape concerning cybersecurity regulation is a patchwork of rules enacted mostly by states.[143] Many federal agencies also seek to regulate cyber defenses in some capacity for industries within their fields. Section I.C discusses the FTC's attempts under 15 U.S.C. §45(n).[144] Other regulatory agencies that have promulgated regulations in this realm include the Department of Health and Human Services,[145] the Federal Communications Commission,[146] the Federal

---

Charter and its customary international law counterpart."). For more information on when and how a cyberattack might rise to the level of an "armed attack," see *id.* at 245–46.

139. *See* Brian Neil Hoffman et al., *Federal and State Cybersecurity Regulation of Financial Services Firms*, L.J. NEWSLS. (June 2017), http://www.lawjournalnewsletters.com/sites/lawjournalnewsletters/2017/06/01/federal-and-state-cybersecurity-regulation-of-financial-services-firms/?slreturn=20180118161409 [https://perma.cc/YE5N-V9AD] ("46 other states, Washington, DC, and three U.S. territories have enacted similar laws [to California's general breach notification law].").

140. *See* Wooten, *supra* note 67, at 239.

141. *See* Cybersecurity Requirements for Financial Services Companies, N.Y. COMP. CODES R. & REGS. tit. 23, § 500 (2017).

142. CAL. CIV. CODE § 1798.81.5(b) (West 2016). California law requires any "business that owns, licenses, or maintains personal information about a California resident [to] implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information" from disclosure. *Id.* In February 2016, then-California Attorney General Kamala Harris issued a report that stated that "reasonable security procedures" for *all* organizations that collect or maintain personal information requires adherence to the twenty controls in the Center for Internet Security's Critical Security Controls. KAMALA D. HARRIS, CAL. DEP'T OF JUSTICE, CALIFORNIA DATA BREACH REPORT 30 (2016).

143. *See* Forscey et al., *supra* note 15.

144. *See supra* notes 74–79 and accompanying text.

145. *See* Health Insurance Reform: Security Standards, 68 Fed. Reg. 8,334, 8,334 (Feb. 20, 2003) (to be codified at 45 C.F.R. pts. 160, 162, 164).

146. *See* Federal Communications Act, Pub. L. No. 73-416, 48 Stat. 1064 (1934) (codified as amended at 47 U.S.C. § 151 et seq.).

Energy Regulatory Commission,[147] and the Securities and Exchange Commission.[148] A benefit to comprehensive, federally promulgated cybersecurity rules is that they would bring much needed clarity to the current landscape, called for by both states[149] and businesses.[150] A comprehensive rule would also help solve the oversight issue identified within the public-private partnership model; though businesses have not been reactive to market pressures, the government could write procedures which would facilitate oversight into the rule.

An unfortunate reality—and a major flaw for regulating cybersecurity—is that because organizations vary in threats faced and data held, "[there is] no one-size-fits-all approach to managing cybersecurity risk."[151] To mandate that all companies use certain systems or firewalls with specific requirements would be both over and underinclusive; overinclusive because mandatory minimum requirements might be prohibitively expensive for small businesses with relatively no risk for breaches, and underinclusive because it is highly unlikely the standards promulgated would cover all types of breaches or defenses.

Assuming that a universal approach was even practical, cybersecurity is a fast-moving, readily evolving industry, whereas Congress is decidedly neither fast-moving nor readily evolving.[152] Even when a single party controls the House, Senate, and Presidency—such as the legal landscape as of the time of writing—laws are passed at tectonic speed.[153] Further complicating matters, Congress lacks the

147. *See* Federal Power Act, Pub. L. No. 333, 49 Stat. 847 (1935) (codified as amended at 16 U.S.C. § 824).

148. Companies must disclose cybersecurity risks to comply with the Securities Act of 1933 and '34. *See CF Disclosure Guidance: Topic No. 2*, U.S. SEC. & EXCHANGE COMMISSION (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm [https://perma.cc/P2A8-D3C6].

149. *See* Colin Wood, *States Push Feds to 'Harmonize' Cybersecurity Regulations in 2018*, STATESCOOP (Jan. 19, 2018, 6:06 PM), http://statescoop.com/states-push-feds-to-harmonize-cybersecurity-regulations-in-2018 [https://perma.cc/5PFV-MBFL].

150. *See* Catalina E. Azuero, *CyberSecurity Regulation Back on Center Stage after Data Breach*, GOODWIN (Sept. 21, 2017), https://www.lenderlawwatch.com/2017/09/21/cybersecurity-regulation-back-on-center-stage-after-data-breach/ [https://perma.cc/6XQJ-HP6W]. A letter to Congress by various industry trade groups argued for a national law on data breach notification, which would preempt the existing patchwork. *See id.*

151. *See* Arias, *supra* note 74.

152. *See* Adrien Seybert, *Net 'Paradigm Shift' for Slow-Moving Congress*, WIRED (Mar. 7, 1997, 7:30 PM), https://www.wired.com/1997/03/net-paradigm-shift-for-slow-moving-congress [https://perma.cc/PY76-ZWUP].

153. *See* Scott Simon, *Conservative Donors Grow Frustrated with Congress Over Slow Legislative Progress*, NPR (Oct. 21, 2017, 8:12 AM), https://www.npr.org/2017/10/21/559215243/conservative-donors-grow-frustrated-with-congress-over-slow-legislative-progress [https://perma.cc/K8H3-3WPT].

expertise[154] required to understand cybersecurity policies comprehensively enough to appropriately legislate. Said structural deficiencies partially explain why Congress has yet to pass even statutes that seem widely supported, such as a data breach notification requirement.[155]

III. SOLUTION

The strategies discussed in Part II outline the goals for a better cybersecurity landscape. First, the ideal security landscape would be standardized and centralized to reduce the costs of compliance and eliminate confusion for firms and states attempting to navigate regulations. Second, private firms should be in charge of their own systems and concurrently held accountable for their security practices. Third, select information pertaining to cybersecurity should be readily shared with the government, but the firms and consumers should monitor which data is released to reduce the chance of government abuse or misuse. Finally, the system must be flexible enough to avoid forcing a one-size-fits-all framework while being rigorous enough to place consumer protection above other considerations.

Repeated failure by private firms to protect consumer data demands change. Because firms elect to acquire and maintain vast deposits of consumer data,[156] the cost for its protection ought to reside primarily with the firm, rather than the public. For that reason, the ideal solution would be one that imposes mandatory compliance upon firms rather than attempting to incentivize increased cooperation with the government.[157] With mandatory compliance in mind, the best

154. *See* James M. Curry, *To Be Effective Legislators, Members of Congress Need Expert Resources of Their Own*, SCHOLARS STRATEGY NETWORK (May 1, 2015), http://www.scholarsstrategynetwork.org/brief/be-effective-legislators-members-congress-need-expert-resources-their-own [https://perma.cc/8VLP-LUDQ]. Expert resources available to Congress for members to learn about the legislations they are debating have declined since the 1970s. *See id.*

155. All fifty states passed legislation requiring entities to notify individuals of security breaches of information involving personally identifiable information. *See Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Oct. 7, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/3THD-M85R]. Congress is considering a similar provision, the "Data Security and Breach Notification Act," but, as of writing, little progress has been made. *See* Data Security and Breach Notification Act, S. 2179, 115th Cong. § 3(a) (2017); Ted Knutson, *Congress Ratcheting Up Pressure on Companies to Notify Consumers of Data Breaches Sooner*, FORBES (Feb. 14, 2018, 1:16 PM), https://www.forbes.com/sites/tedknutson/2018/02/14/congress-ratcheting-up-pressure-on-companies-to-notify-consumers-of-data-breaches-sooner/#4f72f22558df [https://perma.cc/7TRD-7BAF].

156. *See supra* note 59 and accompanying text.

157. *But see* Lin, *supra* note 28, at 1427–31 (suggesting that policymakers can use tax policy to provide corporate tax incentives that encourage companies to invest in better security—

method by which the United States can achieve a system that meets the four requirements outlined above is the creation of a single administrative agency, which would assume all authority regarding cybersecurity regulation.[158] For simplicity's sake, this proposed agency will be referred to as the "Cyber Agency" throughout the remainder of this Note.

A single central agency, as opposed to the current regulatory landscape in which multiple agencies have unclear, piecemeal authority over cybersecurity regulations, is vital for three reasons. First, an agency dedicated solely to cybersecurity regulations would be more assured about its authority to regulate and could avoid concerns of mission overreach held by other regulatory agencies.[159] This is especially important given that the FTC is currently heavily involved in cybersecurity regulations based on preventing "unfairness"[160] but has faced unfairness-related overreach criticisms in the past.[161] With a congressional grant of authority, the Cyber Agency would be more likely to receive *Chevron* deference for its cybersecurity rulings and remove concerns regarding other agencies overstepping its authority.[162]

A single agency would also address concerns regarding a lack of adaptability or expertise present for laws passed through the legislative process. Agencies promulgate regulations much faster and with higher frequency than Congress can legislate,[163] and a singular agency can

---

preferring government contract offers to firms that meet security standards and subsidizing white-hat firm expenditures to purchase zero-day exploits). *See id.* The main distinction between Lin's argument and the one presented here is that Lin's argument is focused on the government's duty to protect the nation from other states' warlike efforts, whereas this Note is focused on firms' duty to protect those people off of whom firms profit. *See id.* at 1378 ("This Article descriptively and normatively explores the new financial theater of war . . . and proposes key recommendations for current and future financial warfare.").

158. For a similar argument, see Balitzer, *supra* note 66, at 917–18. The arguments presented here differ chiefly from Balitzer's in that this Note's argument is predicated on a *single* agency, rather than a joint effort by the FCC and Cyber Threat Intelligence Integration Center. This Note calls for flexible, nuanced applications of security standards instead of Balitzer's "extensive minimum-security standards." *See id.* at 916–18.

159. *See* 5 U.S.C. §§ 706(2)(A), (C) (2018) ("The reviewing court shall hold unlawful and set aside agency action . . . found to be . . . an abuse of discretion, . . . in excess of statutory jurisdiction, authority, or limitations, or short of statutory right . . . ."); Jody Freeman & Jim Rossi, *Agency Coordination in Shared Regulatory Space*, 125 HARV. L. REV. 1131, 1134 (2012).

160. *See* Eastman, *supra* note 69, at 536–37.

161. *See* Beales, *supra* note 79.

162. *See* 5 U.S.C. §§ 706(2)(A), (C); JARED P. COLE, CONG. RESEARCH SERV., AN INTRODUCTION TO JUDICIAL REVIEW OF FEDERAL AGENCY ACTION 2 (2016).

163. *See* Clyde Wayne Crews Jr., *How Many Rules and Regulations Do Federal Agencies Issue?*, FORBES (Aug. 15, 2017, 12:48 PM), https://www.forbes.com/sites/waynecrews/2017/08/15/how-many-rules-and-regulations-do-federal-agencies-issue/#1ebcbc791e64 [https://perma.cc/C6AL-JCCG]. From 1995 through 2016, agencies promulgated almost ninety thousand total rules, whereas Congress enacted 4,312 laws. *Id.*

specialize in cybersecurity, allowing it to obtain the expertise necessary to promulgate satisfactory regulations. The ideas of expertise and efficiency similarly support the proposition of creating a new agency to regulate cybersecurity rather than granting an existing agency, say the FTC, the authority to regulate. The FTC could tackle cybersecurity regulation, but then it would have to either hire more people or use its current staff. If the FTC hired more people, the agency would bloat, take more to manage, and could possibly slow from bureaucratic inefficiencies. If the FTC instead worked with people already in the agency, it risks sacrificing the benefits gained from expertise in cybersecurity. The FTC regulates a broad field of issues, potentially preventing it from obtaining the high level of expertise necessary to create properly nuanced and evolving rules.

Finally, leaving cybersecurity regulations to multiple agencies would fail to reduce the costs of compliance associated with following laws and regulations by multiple governing bodies—one of the core concerns of an optimal security landscape. When creating the Cyber Agency, Congress could grant the Cyber Agency exclusive control over cybersecurity regulations. In this way, the Cyber Agency could act as a repository for all cybersecurity-related rules, untangling the patchwork of regulations promulgated by other agencies. The Cyber Agency's rules would also help to partially alleviate the state patchwork of regulations by preempting state regulations in conflict with those promulgated by the Cyber Agency.[164] Should Congress establish an express or field preemption over state cybersecurity regulations,[165] businesses will incur lower costs for compliance when needing to satisfy only one agency's regulations rather than looking to multiple agencies' and states' rules.

The second goal for an ideal cybersecurity landscape is that private firms oversee their own systems but are concurrently held accountable for their security practices. The Cyber Agency satisfies this requirement by acting as a vehicle for public oversight[166] through

164. *See* U.S. CONST. art. VI, cl. 2.

165. Preemption is express when "Congress states clearly in a federal law that it intends to supersede related state laws." Stephen Wermiel, *SCOTUS for Law Students (Sponsored by Bloomberg Law): Preemption Again*, SCOTUSBLOG (Mar. 11, 2013, 11:05 AM), http://www.scotusblog.com/2013/03/scotus-for-law-students-sponsored-by-bloomberg-law-preemption-again/ [https://perma.cc/A9LV-3S2U]. Field preemption applies when Congress legislates in a way that is so comprehensive that it occupies the entire field of an issue. *Id.*

166. Public oversight would be achieved partially through the notice and comment rulemaking procedures, mandated by the Administrative Procedures Act before an administrative agency passes any binding rules. *See* Brian Wolfman & Bradley Girard, *Argument Preview: The Administrative Procedure Act, Notice-and-Comment Rule Making, and "Interpretive" Rules*, SCOTUSBLOG (Nov. 26, 2014, 10:13 AM), http://www.scotusblog.com/2014/11/argument-previewthe-administrative-procedure-act-notice-and-comment-rule-making-and-interpretive-

regulations without usurping network control. Possible regulations could require firms to maintain audit trails of their responses to potential risks,[167] conduct regular penetration testing,[168] or provide regular reports to the agency about security updates.

This system of accountability is not without its flaws. Critics might argue that the stringency of the agency's monitoring rules would largely depend upon executive branch policies, or that the agency could face issues of regulatory capture in the likely event that interested firms participate more extensively than the public in the Cyber Agency's notice and comment proceedings.[169] The public's control over the executive branch and the public's history of notice and comment participation when motivated partially alleviate these misgivings.[170] The agency would additionally be subject to Congressional and judicial oversight. Despite potential flaws, monitoring by the Cyber Agency is the most workable option for concurrent monitoring when the alternative systems, as discussed in Part II, are ineffective as a whole or provide virtually no concurrent oversight.[171]

The third goal for an ideal system calls for maximizing security-related information sharing—both between corporations and between

---

rules/ [https://perma.cc/CDJ4-MWRY]. The procedures require any agency seeking to promulgate a binding rule to submit the proposed rule to the public and consider publicly submitted comments on the rule. *Id.*

167. *See* Cybersecurity Requirements for Financial Services Companies, N.Y. COMP. CODES R. & REGS. tit. 23, § 500.006 (2017).

168. The tests could be administered by the Cyber Agency or other external companies, similar to an external audit. *See* Lin, *supra* note 28, at 1431–32. The Department of Homeland Security's National Cybersecurity and Communications Integration Center provides a precedent for agency-administered testing. *See* Jason Miller, *How DHS Hacks Agency Networks to Make Them Stronger, More Resilient*, FED. NEWS RADIO (Dec. 6, 2017, 8:07 AM), https://federalnewsradio.com/cybersecurity/2017/12/how-dhs-hacks-agency-networks-to-make-them-stronger-more-resilient/ [https://perma.cc/52S3-NJUD]. Penetration testing has the further benefit of already being standard practice for the government and some financial institutions. *See* Lin, *supra* note 28, at 1432.

169. *See* Lawrence G. Baxter, *Understanding Regulatory Capture: An Academic Perspective from the United States*, *in* THE MAKING OF GOOD FINANCIAL REGULATION: TOWARDS A POLICY RESPONSE TO REGULATORY CAPTURE 31, 31–32 (2012); HENRIQUE SCHNEIDER, UBER: INNOVATION IN SOCIETY 65 (2017) ("[R]egulatory capture . . . is the process by which regulatory agencies eventually come to be dominated by the very industries they were charged with regulating.").

170. Although the most recent fight over net neutrality was clouded by controversy concerning the true extent of the public's comments, the FCC's consideration of net neutrality rules in 2014 fueled millions of scandal-free comments by consumers interested in making themselves heard. *See* Brian Naylor, *As FCC Prepares Net-Neutrality Vote, Study Finds Millions of Fake Comments*, NPR (Dec. 14, 2017, 5:00 AM), https://www.npr.org/2017/12/14/570262688/as-fcc-prepares-net-neutrality-vote-study-finds-millions-of-fake-comments [https://perma.cc/AT6H-TWTY] ("Some 22 million public comments have been filed with the Federal Communications Commission . . . . But, it turns out, much of that public input is not what it appears."); Marguerite Reardon, *Net Neutrality: How We Got from There to Here*, CNET (Feb. 24, 2015, 4:00 AM), https://www.cnet.com/news/net-neutrality-from-there-to-here/ [https://perma.cc/6GD4-AC84] ("In total, more than 4 million public comments were filed on the [2014] Net neutrality proposal.").

171. *See supra* Part II.

the private sector and the government—while minimizing risk of governmental abuse. This is important because the accountability the second goal calls for requires a metric reflecting data-sharing activity and cooperation by the firms. To achieve this, the Cyber Agency could borrow from the Department of Homeland Security and implement an information-sharing program,[172] but simply make active participation mandatory.[173] Mandatory disclosure of data might make the public uneasy, but—just as the Cyber Agency can act as the public's vehicle to monitor private sector cybersecurity—so, too, can firms act as the public's vehicle to monitor the Cyber Agency for appropriate data usage and application. The Cyber Agency could limit the type of information it requires from businesses. For example, the information shared could be limited to information about the corporation's cyber infrastructure, such as vulnerabilities discovered and methods used to patch them, or the attacks detected and any identifying marks gleaned from the hackers. To ensure these limitations are respected, private firms could publish reports about the type of data they give to the Cyber Agency. The Cyber Agency could simultaneously file public reports on the types of metrics the agency requires from the private sector. If citizens notice that the Cyber Agency is mandating disclosure of personal information rather than just cybersecurity statistics, they can lobby the agency or Congress for change. Transparencies about and limitations on the data collected from firms ought to help ease misgivings about data abuse by the government.

Finally, a single agency is the best method by which a nuanced structure of regulations can be enacted to ensure consumer data are protected while avoiding blanket regulations. As previously discussed, a one-size-fits-all approach to cybersecurity is realistically impracticable.[174] The Cyber Agency's expertise and dedication to cybersecurity regulation would enable it to create metrics ensuring *appropriate* minimum security standards, not simply sufficient ones. Single-store mom and pop shops who collect credit card information from their customers ought not be subjected to the same minimum requirements as national financial institutions or power plants whose networks qualify as critical infrastructure. Small businesses are far from exempt from cyberattacks, but they can take relatively straightforward steps to protect themselves, like watching out for

172. *See Cyber Information Sharing and Collaboration Program (CISCP)*, *supra* note 72.

173. Enforcing such a program would be admittedly difficult, but possible, if combined with the proposed audit trails and regular reports.

174. *See* Arias, *supra* note 74; *supra* Section II.C.

phishing expeditions.[175] Critical infrastructure, which by its nature is largely interconnected,[176] might require more thorough and costly measures to protect its data. Similarly, as between two large companies, those which collect only credit card information should not be subject to the same standards as those who also collect addresses, driver's license numbers, and social security numbers since the potential damage caused by a breach of the former would be less than a breach of the latter. The Cyber Agency could use the information gleaned through the concurrent accountability reporting requirements to ensure the riskiest businesses are held to the strictest standards while relatively risk-free firms are not bogged down by unnecessary regulation. The assessment would focus on each firm's risk of being hacked and the potential damage a breach would cause to the public.

The Cyber Agency's flexibility while regulating also allows the public to consider who they think ought to bear the cost of protections. This Note argues that firms who collect and sell consumer data purely for profit ought to carry the burden to protect that information. The argument becomes less straightforward, however, when considering who should pay to protect the networks of public utility companies or financial institutions, like the New York Stock Exchange, which are considered critical infrastructure. Should the public decide the cost to defend critical infrastructure rightfully belongs to the government, the Cyber Agency could still mandate appropriate security requirements but offer incentives or subsidies in the event of compliance to offset the cost.

An example regulation is illustrative. If the Cyber Agency is created, it could require that companies disclose the type and quantity of information collected from their customers. The Cyber Agency might then decide to require penetration testing for companies whose stored information is of sufficient value or sensitivity (i.e., the credit card information of at least three hundred thousand customers or the credit card and social security information of at least one hundred thousand customers). The determination for the minimum information stored before penetration testing is required could be a cost-benefit analysis: balancing the cost of penetration testing compared to the expected damage from a breach, calculated as the potential damage of losing the

175. *See* Chris Morris, *14 Million US Businesses Are at Risk of a Hacker Threat*, CNBC (July 25, 2017, 10:02 AM), https://www.cnbc.com/2017/07/25/14-million-us-businesses-are-at-risk-of-a-hacker-threat.html [https://perma.cc/7WRP-H8Y5]; Steve Strauss, *Cyber Threat is Huge for Small Businesses*, USA TODAY (Oct. 20, 2017, 10:33 AM), https://www.usatoday.com/story/money/columnist/strauss/2017/10/20/cyber-threat-huge-small-businesses/782716001/ [https://perma.cc/BY7R-GRHD].

176. *See* Lin, *supra* note 28, at 1388.

stored information times the likelihood that the information would be lost. From the results of penetration testing, the Cyber Agency might find that for many corporations, security would be improved by updating their physical defenses. The Cyber Agency therefore might promulgate a rule that requires corporations to install gateways,[177] segmented system memory,[178] and hack-proof wireless routers.[179] To determine the extent to which hardware upgrades will be required, the Cyber Agency could conduct another cost-benefit analysis, this time comparing the cost of installing the hardware to the value of the information expected to be protected once the hardware is installed. The Cyber Agency could carve out exceptions to the requirement for companies whose security would see little benefit from installation—knowledge to be gleaned from the penetration tests—or for companies whose stored data is not valuable enough to warrant the additional cost for protections. If the public decides that the cost to defend critical infrastructure belongs to the federal government, the Cyber Agency might also include cost-shifting measures to assume some of the financial burden of installation for public utility companies who are required to upgrade their hardware. In this way, the Cyber Agency's dedication and expertise to cybersecurity allow them to promulgate a tailored and effective rule to ensure appropriate protections over consumer data.

It is important to note that the Cyber Agency's creation and promulgated regulations would supplement the current public-private partnership system. The public-private system became the de-facto cybersecurity strategy because it features some benefits.[180] The Cyber

177. *See* Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 24 n.152 (2009). Gateways serve to restrict all data flowing in and out of the server to one channel which can be monitored to ensure the traffic is for legitimate purposes and from trustworthy sources. *See id.* One could analogize a computer gateway to a single gated access road leading onto a campus from the highway.

178. *See id.* at 24. Segmented system memory works by storing privileged processes on one server drive and nonprivileged processes on others. *Id.* at 24 n.151.

179. *See* Alex Hern, *'All Wifi Networks' Are Vulnerable to Hacking, Security Expert Discovers*, GUARDIAN (Oct. 16, 2017, 4:33 PM), https://www.theguardian.com/technology/2017/oct/16/wpa2-wifi-security-vulnerable-hacking-us-government-warns [https://perma.cc/NPN5-35SN]. Researchers recently discovered that the WPA2 protocol, used to secure most WiFi connections, has been recently broken, "potentially exposing wireless internet traffic to malicious eavesdroppers and attacks." *Id.* Though the attacker utilizing the exploit, named "Krack," must be physically within range to access the targeted WiFi network—once the network has been breached—the attacker can decrypt all information transmitted over the network. *See id.* Companies were quick to release safer router designs. *See, e.g.*, Tom Warren, *Microsoft Has Already Fixed the Wi-Fi Attack Vulnerability*, VERGE (Oct. 16, 2017, 9:58 AM), https://www.theverge.com/2017/10/16/16481818/wi-fi-attack-response-security-patches [https://perma.cc/L69C-DGZS].

180. *See supra* Section II.A.

Agency is meant to address the flaws inherent in the public-private partnership—chiefly issues of accountability[181] and corporate apathy[182]—without completely supplanting it. Indeed, the increased information sharing between corporations and reduced confusion surrounding what measures are required by the Cyber Agency would likely *increase* the private sector's effectiveness in protecting itself.

IV. CONCLUSION

Deficiencies in cybersecurity are and will continue to be a problem, especially as nation-states ramp up their presence in cyberspace and increase their utilization of sponsored hacks as a tool to further their political agendas. Beyond government-owned networks, consumer data and critical infrastructure owned by private firms also face substantial risks. Data and critical networks are currently protected by a public-private partnership system which, though effective in some regards, features a lack of oversight and accountability by relying on ex ante private sector cooperation. It is this system which has allowed over half of the citizens in the United States to have compromised social security numbers and public utility systems to be held for ransom.

A single dedicated agency is the best solution to remedy these failings while avoiding concerns regarding privacy and data abuse, cost and practicality, and regulatory rigidity present in other cybersecurity strategies. The agency could centralize regulations to reduce costs of compliance incurred by firms to determine necessary security standards. Firms could retain control over their own networks, held concurrently accountable by the agency's oversight. A centralized agency could facilitate data sharing between firms and the government while avoiding fears of misuse. Finally, the regulations promulgated by the agency can be tailored in a way to avoid a one-size-fits-all approach. It is through this system that the current cybersecurity landscape can be shored up to give individual consumers peace of mind about the integrity of their data and the nation a sense of assurance that it will be protected from attacks against critical infrastructure.

Eric J. Hyla[*]

181. *See supra* notes 118–24 and accompanying text.

182. *See* Newman, *supra* notes 17.

* J.D. Candidate, 2019, Vanderbilt University Law School; B.A., Illinois Wesleyan University, 2016. I would like to thank the editors of the *Vanderbilt Journal of Entertainment & Technology Law* for all of their hard work through the publication process of this Note.