## *VIII. Cybersecurity and the Struggle to Regulate the Financial Industry and Defend Against Cybercriminals*

### A. Introduction

On January 23, 2019, TechCrunch reported more than twenty-four million banking and financial documents had been compromised from some of the biggest banks in the United States including Citigroup, HSBC Life Insurance, Wells Fargo, CapitalOne, and several U.S. federal departments.[1] Reports of cyberattacks and data breaches have become an all-too familiar narrative in recent years, but this latest attack on financial records invites renewed concern regarding how financial data is protected. In fact, just one day later TechCrunch reported the same set of financial documents had been exposed again, compromising sensitive data such as "names, addresses, birth dates, Social Security numbers," as well as bank account numbers, bankruptcy filings, and tax documents.[2] This particular breach was the result of inadequate cybersecurity controls, not a malicious hack.[3] Although individual data privacy concerns are at stake when a breach involving financial information occurs, the consequences of an intentional, adversarial cyberattack on the financial sector implicate more problematic national security concerns.[4]

---

[1] Zack Whittaker, *Millions of Bank Loan and Mortgage Documents Have Leaked Online*, TECHCRUNCH (Jan. 23, 2019), https://techcrunch.com/2019/01/23/financial-files/ [https://perma.cc/765J-6SLS].

[2] Zack Whittaker, *Massive Mortgage and Loan Data Leak Gets Worse as Original Documents Also Exposed*, TECHCRUNCH (Jan. 24, 2019), https://techcrunch.com/2019/01/24/mortgage-loan-leak-gets-worse/ [https://perma.cc/L9FK-DSM9] (discussing the original breach, and reporting that "[i]t turns out that data was exposed again—but this time, it was the original documents.").

[3] Whittaker, *supra* note 1 (stating that the data was not "protected with a password, allowing anyone to access and read the massive cache of documents").

[4] *See* JASON HEALEY ET AL., BROOKINGS INSTITUTION, THE FUTURE OF FINANCIAL STABILITY AND CYBER RISK 1 (2018), https://www.brookings.edu/wp-content/uploads/2018/10/Healey-et-al_Financial-Stability-and-Cyber-Risk.pdf. [https://perma.cc/7JGC-W925] ("Some of the most direct initiatives on these questions began in 2013, after a White House Executive Order instructed the Department of Homeland Security, in consultation with the Department of Treasury, to identify those financial institutions for which 'a cyber incident would have far reaching impact on regional or national economic security.'").

Banks in the United States are particularly vulnerable to cyberattacks and breaches due to their significance in the global economy and their international presence.[5] In fact, the complexity and "'unacknowledged correlated risk of cyberspace is why cyberspace is capable of black swan behavior,' of very unpredictable, extremely high-consequence events."[6] In other words, because there is little data publicly available regarding cyberattacks on financial institutions, the threat posed by a cyberattack on the financial sector is unknown.[7] Correspondingly, as it is unknown how the consequences of cyber-attack on the financial industry would cascade, the threat to economic stability is difficult to predict.[8] Further, "[t]hese risks are compounded by the international and interdependent nature of the global financial system,"[9] and by the largely unregulated use of third-party vendors in the financial industry.[10] In addition to economic stability implications, the malicious use of cyberspace poses serious national security risks. With increasing frequency and sophistication, state and nonstate actors are using cyberspace to target the United States' financial institutions because "after over two decades of global military leadership, cyberspace is the only domain of warfare in which the United States faces near-peer, or even peer, competitors."[11] Thus, the only way that many of the United States' adversaries can directly challenge the U.S. is through cyberattacks. Nation-states are enlisting the help of cyber criminals to target "core financial infrastructure."[12] In fact, North

---

[5] Erica D. Borghard, *Protecting Financial Institutions Against Cyber Threats: A National Security Issue* 1, 5 (Carnegie Endowment for Int'l Peace, Cybersecurity and the Financial System Working Paper No. 2, 2018), https://carnegieendowment.org/files/WP_Borghard_Financial_Cyber_formatted_complete.pdf [https://perma.cc/JL49-TEBJ].

[6] *Id*. at 4–5 (citing Dan Geer Jr., *A Rubicon* 1 (Hoover Institution: Aegis Series Paper No. 1801, 2018), https://www.hoover.org/sites/default/files/research/docs/geer_webreadypdfupdated2.pdf [https://perma.cc/KHB9-K8T3]).

[7] Antoine Bouveret, *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment* 2, 2 (Int'l Monetary Fund, Working Paper No. WP/18/143, 2018), http://www.complinet.com/net_file_store/new_editorial/i/m/IMF-2018.pdf [https://perma.cc/Y7LC-RZ8M].

[8] Borghard *supra* note 5, at 5.

[9] *Id.* at 6.

[10] *See* Kevin L. Petrasic et al., *A Cybersecurity Catch-22 for Banks*, LAW360 (May 13, 2015, 10:25 AM), https://www.law360.com/articles/654392/a-cybersecurity-catch-22-for-banks.

[11] Borghard, *supra* note 5, at 6.

[12] *See* HEALEY ET AL., *supra* note 4, at 6.

Korea attempted to steal $951 million from the Bangladesh central bank by attacking the Society for Worldwide Interbank Financial Telecommunications (SWIFT) global payment messaging system.[13]

This is an issue because the infrastructure of storing and sharing information and communications was not designed with security as a priority, and, consequently, developing cybersecurity programs to protect such information *ex post* is increasingly difficult.[14] Further, the regulatory landscape in the United States remains uncertain, leaving banks, financial firms, and third-party vendors with inadequate supervision over their cybersecurity programs charged with protecting consumer data.[15] However, recent legislation and government involvement suggests this trend could be changing. For example, President Trump signed the Cybersecurity and Infrastructure Security Agency Act of 2018, which created a new Department of Homeland Security (DHS) agency to act as the top cyber police force.[16] Although there are conflicting ideas about how the United States should address cybersecurity in the financial industry, it is clear that given the advances in sophistication and frequency of attack, more must be done to adequately defend the financial system against such attack. The remainder of this article will discuss each of these issues regarding cybersecurity in the financial industry, in greater detail.

Section B provides an introduction to cybersecurity and define the term as it relates to the financial industry. Next, Section C elaborates on the evolution of cyber threat landscape, and how the response by the United States government has grown proportionately with the increased sophistication of cyberattacks. Section D discusses the current regulatory climate in the United States for cyber risk, and the

---

[13] *Id.* at 7 ("Other examples include North Korean intrusions into the Bangladesh central bank to attempt to steal USD 951 million through the SWIFT global payment messaging system . . . .").

[14] *See* Borghard, *supra* note 5, at 6.

[15] *See* Greg Baer & Rob Hunter, *A Tower of Babel: Cyber Regulation for Financial Services*, CLEARING HOUSE (2017), https://www.theclearinghouse.org/banking-perspectives/2017/2017-q2-banking-perspectives/articles/cyber-regulation-for-financial-services [https://perma.cc/UDY7-PNTB] (discussing the "core problems" of cybersecurity bank regulations).

[16] Cat Zakrzewski, *The Cybersecurity 202: Trump Set to Make a New DHS Agency the Top Federal Cyber Cop*, WASH. POST (Nov. 16, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/11/16/the-cybersecurity-202-trump-set-to-make-a-new-dhs-agency-the-top-federal-cyber-cop/5bedb9a71b326b3929054867/?utm_term=.410ecebdbfb2.

problems with reactive regulation in a rapidly evolving environment. Finally, Section E concludes by discussing regulatory developments and trends when it comes to cybersecurity in the financial sector, and includes different proposals and ideas about the best way to handle this risk.

### B. Background on Cybersecurity and Banking

Historically, banks focused their security efforts primarily on protecting physical assets such as money, promissory notes, and other valuable assets stored inside their vaults.[17] However, as the banking industry grew in complexity, financial institutions began relying on new services and providers, which ultimately had the effect of increasing the number of access points to a bank's assets.[18] By exploiting the weakest of those access points, cybercriminals can access the data, systems, as well as networks of financial institutions.[19] Moreover, the past decade has given way to the rapid digitization of the global economy,[20] which consequently has meant increasingly sophisticated cyberattacks on banks.[21]

---

[17] *See* Kim Loy, *5 Emerging Risk Management and Security Trends in Banking*, SECURITYMAGAZINE (Oct. 20, 2018), https://www.securitymagazine.com/articles/89528-emerging-risk-management-and-security-trends-in-banking [https://perma.cc/97KP-HSED].

[18] *See* Nick Ismail, *Securing the Future: The Evolution of Cyber Security in the Wake of Digitalisation*, BONHILL GROUP PLC: INFORMATIONAGE (Feb. 13, 2018), https://www.information-age.com/evolution-cyber-security-wake-digitalisation-123470747/ [https://perma.cc/6YC4-V2XB] ("Today, with the sharp increase in in use of digital technologies in the workplace . . . there has been a surge in the number of endpoints and potential ways for cybercriminals to gain access to enterprise networks.").

[19] Petrasic et al., *supra* note 10.

[20] *See generally* JAMES MANYIKA ET AL., MCKINSEY GLOBAL INST., DIGITAL GLOBALIZATION: THE NEW ERA OF GLOBAL FLOWS (Feb. 2016), https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx [https://perma.cc/E5AE-F4FN].

[21] Petrasic et al., *supra* note 10.

### *1. What Is Cybersecurity?*

Broadly speaking, cybersecurity seeks to promote the security of systems, networks, and information.[22] Although information/data security is included in cybersecurity, it is but one part of a bigger picture. Cybersecurity professionals explain the goals of cybersecurity as three-fold: (i) confidentiality, (ii) integrity, and (iii) availability.[23] Therefore, when thinking about the financial industry, it is important to consider the broader set of harms, including "financial, operational, legal, and reputational impact."[24]

The potential for intentional attacks is a unique feature of the cybersecurity landscape. Specifically, a cyber event can be either unintentional, such as the breach reported by TechCrunch on January 23, 2019, or intentional.[25] As illustrated by the January 23 breach, many of the data breaches in the financial industry result from inadequate cybersecurity controls of third-party providers.[26] However, the source of an intentional cyberattack is not always as clear. Cyberattacks can take on many different forms and are increasingly tailored to inflict harm on a particular institution.[27] The White House Council of Economic Advisors estimates that these malicious cyber-attacks account for losses between $57 billion and $109 billion per

---

[22] Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 996 (2018) ("A focus on the security of systems and networks—and not just information—is necessary as physical devices are increasingly connected to the Internet.").

[23] *Id*. at 997 ("Cybersecurity professionals commonly think about security as covering three general categories of goals: (1) confidentiality; (2) integrity; and (3) availability . . . .").

[24] FED. FIN. INSTS. EXAMINATION COUNCIL CYBERSECURITY ASSESSMENT TOOL, USER'S GUIDE 1, 2 (2017), https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017_Users_Guide_June2.pdf [https://perma.cc/CHM7-S4MH].

[25] *See* Whittaker, *supra* note 1.

[26] *See, e.g.,* Alex Campanelli, *Lessons Learned from 3 Major Financial Services Data Breaches*, BITSIGHT (July 24, 2018), https://www.bitsight.com/blog/lessons-learned-from-3-major-financial-services-data-breaches [https://perma.cc/C7KP-QWXC].

[27] Petrasic et al., *supra* note 10 ("[I]ncluding through spear phishing (sending emails with malicious software attached to individuals at the bank), launching distributed denial of service attacks (shutting off Internet access to bank services . . . ), and subverting the supply chain (attacking the [bank's] equipment or software . . . ).").

year to the U.S. economy.[28] Consequently, as banks develop cyber-security programs, they must account for data breaches—a task which requires enhanced oversight of third-party vendors, as well as increasingly sophisticated cyberattacks.[29]

### *2. The Financial Industry's Vulnerabilities*

The United States' financial industry is vulnerable to cyber-attacks for several reasons. First, the financial industry is increasingly global, and "U.S.-based firms that are essential to U.S. financial stability have interests and operations that span the world, creating an exceptionally large surface area of attack."[30] The vulnerabilities are further compounded by the industry's increasing reliance on financial technology, and reenforce the concern that any "significant disruptive or destructive attacks against the financial sector could have catastrophic effects on the economy and threaten financial stability."[31] For instance, the attack on the SWIFT network exposed this weakness in the industry, notably, that a lack of substitutes that perform vital financial functions can have serious financial consequences.[32] Despite the estimated $1 billion financial impact from that attack, the industry still lacks adequate substitutes. Thus, because U.S. financial institutions rely on the same systems to perform vital functions, there are financial and reputational implications of these attacks. Finally, cyberspace exposes the United States to "near-peer, or even peer, competitors" that have not traditionally been able to challenge the

---

[28] COUNCIL OF ECON. ADVISERS, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY 36 ("[W]e estimate that malicious cyber activity costs the U.S. economy between $57 billion and $109 billion in 2016 . . . .").

[29] Campanelli, *supra* note 26. (discussing key takeaways from three recent financial services data breaches and emphasizing the need for increased oversight of third-party and fourth-party vendors as well as the increasingly sophisticated nature of cyberattacks).

[30] Borghard, *supra* note 5, at 6.

[31] *Id*. at 5.

[32] Joshua Hammer, *The Billion Dollar Bank Job*, N.Y. TIMES (May 3, 2018), https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html (discussing how hackers turned SWIFT's defining feature—its global reach—into a vulnerability); Jack Stubbs, *Hackers Stole $6 Million From Russian Bank via SWIFT System: Central Bank*, REUTERS (Feb. 16, 2018, 1:07 AM), https://www.reuters.com/article/us-russia-cyber-swift/hackers-stole-6-million-from-russian-bank-via-swift-system-central-bank-idUSKCN1G00DV [https://perma.cc/586F-E73W].

United States' global military position.[33] Thus, "targeting the financial sector in cyberspace is one of the few ways adversaries can directly challenge the United States, through significant and potentially catastrophic effects on the U.S economy."[34]

### C. Evolution of Cyberattacks

By 2001 federal regulators were expressing concerns about the risks associated with the increasing digitization of various banking services.[35] However, cyberattacks would continue to increase in sophistication and frequency. In 2013, a significant shift in cybercrime methodology could be seen through the unprecedented attack on more than one hundred banking entities around the world.[36] This attack represented a emerging trend in which cybercriminals did not target banking customers, but instead directly targeted banks' networks.[37] This shift in strategy was significant because it revealed the vulnerabilities of the banking sector, and ultimately resulted in one billion dollars in losses to the targeted banks.[38]

In 2014, Tim Johnson, then-Chairman of the Banking Committee addressed the significance of the issue, explaining to Congress that "[n]ot only are financial institutions frequent targets of cybercrime, they are uniquely interconnected with major sectors of the

---

[33] Borghard, *supra* note 5, at 6.
[34] *Id.*
[35] *See, e.g.,* Letter from Michael J. Zamorski, Acting Dir., Fed. Deposit Ins. Corp., to Chief Exec. Officer & Chief. Info. Officer (Aug. 24, 2001), https://www.fdic.gov/news/news/financial/2001/fil0169.html [https://perma.cc/K67M-SUCD] ("Customer interaction with financial institutions is migrating from in-person, paper-based transactions to [] electronic access and transaction initiation . . . [thereby] increas[ing] the risk of doing business with unauthorized or incorrectly identified parties that could result in financial loss or reputation damage to the financial institution.").
[36] Ariana L. Johnson, *Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation*, 20 N.C. BANKING INST. 277, 277–78 (2016) (describing the elements of a "Carbanak" attack).
[37] *Id*.
[38] *Id.* ("[Financial institutions] must continue to strengthen their cybersecurity infrastructure by investing resources in gathering, analyzing, and sharing cyber threat intelligence data to better understand the evolving nature of complex security risks.").

economy."[39] Underscoring the significance of the interconnected position of financial institutions, Chairman Johnson warned that cyberattacks could "cause damage to the financial system without directly attacking a bank," identifying attacks on third-party providers as an example.[40] In other words, Johnson feared that traditional regulation of banks was not enough to protect the greater economy from a cyberattack, and in 2015 President Obama strongly agreed.[41]

On April 1, 2015, President Obama declared cyberattacks a national emergency.[42] Additionally Obama imposed targeted sanctions through executive order "to deal with the unusual and extraordinary threat to the national security, foreign policy, and economy of the United States constituted by the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States."[43] Obama's concerns were supported by research from IBM Security, whose research revealed that in 2016, financial services institutions were attacked sixty-five percent more than the average organization across all industries.[44] Moreover, state and non-state

---

[39] *Cybersecurity: Enhancing Coordination to Protect the Financial Sector: Hearing Before the S. Comm. on Banking, Hous., & Urban Affairs*, 113th Cong. 1–2 (2014) (statement of Sen. Tim Johnson, Chairman, S. Banking Comm.) (encouraging witnesses to take action to address cybersecurity).

[40] *Id.* (stressing the need to "ensure that consumers have confidence in the financial system").

[41] President Barack Obama, Remarks by the President at the Cybersecurity and Consumer Protection Summit (Feb. 13, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit [https://perma.cc/HW8B-DR89] ("There's only one way to defend America from these cyber threats, and that is through government and industry working together, sharing appropriate information as true partners.").

[42] Cory Bennett & Elise Viebeck, *Obama Declares Cyberattacks a 'National Emergency'*, HILL (Apr. 1, 2015, 9:13 AM), https://thehill.com/policy/cybersecurity/237581-obama-declares-cyberattacks-a-national-emergency [https://perma.cc/TE6E-UAUU].

[43] OFFICE OF FOREIGN ASSETS CONTROL, CYBER-RELATED SANCTIONS PROGRAM 2, 3 (2017), https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber.pdf [https://perma.cc/JEE8-F7UW] (authorizing sanctions against those involved in "certain malicious cyber-enabled activities").

[44] Press Release, IBM, IBM X-Force: Financial Services Most Targeted by Cybercriminals in 2016 (Apr. 27, 2017), https://www-03.ibm.com/press/us/en/pressrelease/52210.wss [https://perma.cc/6TG5-DRJ6] ("[T]he number

actors have multiplied the cybersecurity threat landscape by using cyberspace to target U.S. financial institutions.[45]

### D. Current Regulation

The United States currently does not have a unified approach to cybersecurity. Rather, the regulatory framework in place "stems from century-old privacy norms, torts, and criminal laws that bear little relation" to the protections needed today.[46] Further, the focus of many of the regulations is limited to confidentiality and protecting consumer data and sensitive information. For example, at the federal level for financial institutions, the Gramm-Leach-Bliley Act (GLBA) is the principal statutory authority that requires banks to safeguard customer information.[47] However, the GBLA was passed in 1999 and primarily addresses consumer privacy; its coverage is not responsive to full scope of banks' present-day cybersecurity needs.[48] Financial regulators from the states as well as the federal government have subsequently promulgated various standards that address discrete aspects of cybersecurity. However, standards promulgated by the prudential regulators face criticism that they "run counter to best practices and would increase cyberrisk," suggesting that regulators lack sufficient cybersecurity expertise.[49]

At the federal level, there are also several cooperative and voluntary measures in place. One such measure is the Financial Services Information Sharing and Analysis Center, an information sharing partnership between the public and private sectors that is

---

of financial services records breached skyrocketed 937 percent in 2016 to more than 200 million.").

[45] Borghard, *supra* note 5, at 5–6.

[46] Kosseff, *supra* note 22, at 988.

[47] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 15 U.S.C.).

[48] *See* Christopher D. Pham & N. Chethana Perera, *The Effects of New York's New Cyber Security Law*, FREDRIKSON & BYRON, P.A. (Sept. 1, 2017), https://www.fredlaw.com/news__media/2017/09/01/1610/the_effects_of_new_yorks_new_cyber_security_law?utm_source=fredlawemail&utm_medium=fredlawemail [https://perma.cc/2BBA-M4HD] (comparing the scope of GLBA and New York's more recent regulation to combat "ever-increasing and sophisticated cyber intrusions").

[49] Baer & Hunter, *supra* note 15.

specific to the financial industry.[50] Another example is the National Institute of Standards and Technology (NIST) Framework, which was developed through public and private sector collaboration in response to an executive order signed in 2013.[51] The executive order directed the NIST to create "a risk-based cybersecurity framework to serve as a set of voluntary consensus standards and industry best practices to help organizations manage cybersecurity risks."[52] The NIST Framework has been very successful and is considered to be an industry best practice.[53] In 2015, the Cybersecurity Act of 2015 provided an information sharing mechanism that was not limited to the financial industry.[54] Specifically, Article I of the legislation gives DHS the authority to facilitate information sharing, and the ability to provide safe harbor protections.[55] On November 14, 2018, President Trump signed the Cybersecurity and Infrastructure Security Agency (CISA) Act of 2018 into law, which created CISA, a new DHS agency.[56] The stated mission of the agency is to "partner[] with industry and government to understand and manage risk to our Nation's critical infrastructure."[57] Alluding to the importance of the financial industry, DHS cybersecurity chief Chris Krebs said that CISA "serves as a

---

[50] *A Framework for Cybersecurity*, FED. DEPOSIT INS. CORP.: SUPERVISORY INSIGHTS 3–4 (Winter 2015), https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin15/si_winter2015-article01.pdf [https://perma.cc/K3NA-JKKD].

[51] *Id*. at 4–5 ("The first version of the cybersecurity framework . . . consisted of five core areas: Identify, Protect, Detect, Respond, and Recover.").

[52] *Id*. at 4 (describing the intent of the executive order).

[53] Shin-yi Peng, *Private Cybersecurity Standards: Cyberspace Governance, Multistakeholderism, and the (Ir)Relevance of the TBT Regime*, 51 CORNELL INT'L L.J. 445, 458–59 (2018) (arguing that the NIST Framework "has the potential to become a de facto international cybersecurity standard").

[54] Cybersecurity Act of 2015, Pub. L. No. 114-113, Div. N, § 1(a), 129 Stat. 2935; Memorandum from Sullivan & Cromwell LLP, The Cybersecurity Act of 2015 5–6 (Dec. 22, 2015), https://www.sullcrom.com /siteFiles/Publications/SC_Publication_The_Cybersecurity_Act_of_2015.pdf [https://perma.cc/5WJQ-5HYM].

[55] Memorandum from Sullivan & Cromwell, *supra* note 54, at 3.

[56] Press Release, The White House, President Donald J. Trump Signed H.R. 3359 into Law (Nov. 16, 2018), https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-signed-h-r-3359-law/ [https://perma.cc/TT6W-8ZZS].

[57] *About CISA*, DEPT. HOMELAND SECURITY, https://www.dhs.gov/cisa/about-cisa [https://perma.cc/4JDT-CLLP] (last visited Mar. 5, 2019) ("Our partners in this mission span the public and private sectors.").

model for how we're going to partner to protect the grid, to protect the banks."[58]

In addition to federal laws and regulations, banks must also comply with the various state laws that address cybersecurity. For example, every state, as well as the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have passed data breach laws.[59] That said, these laws apply based on customer residency and are not uniform with respect to when an institution must notify an individual, nor with the format and content of the notification.[60] Further, individual states like New York have passed comprehensive cybersecurity legislation aimed at financial services firms.[61]

### E. Conclusion: Development, Reform and Trends

Despite years of recognition, regulators and legislators have failed to establish a unified federal cybersecurity framework, and consequently, tremendous regulatory uncertainty exists for U.S. financial institutions.[62] The Office of Inspector General (OIG) continues to name cybersecurity as the primary risk threatening "safety and soundness of financial institutions."[63] The most recent OIG report reiterates the fear that "a cybersecurity incident could disrupt services at a bank, resulting in the exploitation of personal information in fraudulent or other illicit schemes, and an incident could start a contagion that spreads through established interconnected banking relationships."[64] Cybersecurity regulations for banks continue to grow

---

[58] Zakrzewski, *supra* note 16.

[59] *Security Breach Notification Laws*, NAT'L CONF. STATE LEGISLATURES (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/N24L-9XFE].

[60] Kosseff, *supra* note 22, at 1014–15.

[61] Brian Neil Hoffman et al., *Federal and State Cybersecurity Regulation of Financial Services Firms*, CORP. COUNSELOR 5–6 (June 2017).

[62] OFFICE OF THE INSPECTOR GEN., FED. DEPOSIT INS. CORP., TOP MANAGEMENT AND PERFORMANCE CHALLENGES FACING THE FEDERAL DEPOSIT INSURANCE CORPORATION 2–3 (2019) [hereinafter OIG 2019 REPORT], https://www.fdicoig.gov/sites/default/files/attachments/OIG-TMPC-Publish-Final-2-14-19.pdf [https://perma.cc/DV7W-YW5A] (stressing the mutually-agreed need for greater cybersecurity protection).

[63] *Id*. at 2.

[64] *Id*.

in volume, and lack consistency in their objectives and requirements.[65] In fact, it is estimated that large banks are forced to spend forty percent of cybersecurity resources on regulatory compliance.[66] This might help explain a second observation made in the OIG report, that "[d]espite increased spending on cybersecurity, banks are encountering difficulties in getting ahead of the increased frequency and sophistication of cyberattacks."[67]

However, the future of cybersecurity in the financial industry is unclear. The differences in approach to regulation are wide-ranging and fraught with disagreement over fundamental points including determining the relevant regulatory agency, jurisdiction, and level of public-private cooperation. One argument holds that the lack of harmonization in the current cybersecurity framework for banks is ineffective, as it increasingly diverts resources from "actual cyber protection to compliance, actively hindering the security of the nation's financial infrastructure."[68] Further, the inefficiency argument points out that federal financial regulators lack expertise in cybersecurity, and consequently, their regulations suffer from an overly-simplistic, "one-size-fits-all" model despite different risks and capabilities that firms face.[69] A second argument is that in order to properly address the cybersecurity threats that are currently being posed, the government must allocate adequate funds in order to properly address and remediate the inadequacies of the current framework. Bruce Schneier, a security guru and proponent of government investment in cybersecurity explains that, in addition, he "would like to see policies that both give companies incentives to increase security and make them liable for security failures," and stresses the "need to focus on resilience," explaining that "[i]f we can't provide the level of security we need, we must ensure that small failures don't cascade into major

---

[65] Baer & Hunter, *supra* note 15.
[66] *Id.* ("One firm told us it receives a new cybersecurity standard once a week on average.").
[67] OIG 2019 REPORT, *supra* note 62, at 3 ("Cyberattacks—such as distributed denial of service and ransomware—may be global in nature and have disrupted financial services in several countries around the world.").
[68] Baer & Hunter, *supra* note 15.
[69] *Id*. (clarifying, however, that the evolving nature of cybersecurity threats renders a "one-size-fits-all" approach insufficient, "regardless of the expertise of the agency writing them").

ones."[70] Still others believe that cybersecurity regulation is unnecessary because "banks understand the threats posed by cybersecurity attacks and have every incentive to mount robust defenses to such threats."[71]

Thus, although each recognizes that a change to the current framework is necessary, the precise change to achieve an optimal cybersecurity regulatory framework remains an open question.

Parker Conway[72]

[70] Interview by Journal of Int'l Affairs with Bruce Schneier, 71 J. INT'L AFF. 121, 121 (2018) (stressing the need for governments to invest necessary resources in cybersecurity).
[71] Baer & Hunger, *supra* note 15.
[72] Student, Boston University School of Law (J.D. 2020).