UNC SCHOOL OF LAW

NORTH CAROLINA BANKING INSTITUTE

Volume 20 | Issue 1 Article 15

3-1-2016

Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation

Ariana L. Johnson

Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation

I. INTRODUCTION

In late 2013, a multinational gang of cybercriminals began to execute a series of highly sophisticated attacks against more than 100 banking entities across the globe.[1] These incredibly complex and unprecedented cyber attacks, also known as Carbanak[2] attacks, resulted in cumulative losses of nearly $1 billion to banks.[3] An analysis of these incidents confirmed that Carbanak attacks primarily target financial networks that utilize money processing services such as deposit accounts and ATMs.[4] The financial losses resulting from these continuing attacks have been astronomical, as losses per bank have ranged from $2.5 million to $10 million per attack.[5]

The Carbanak attacks illustrate an alarming methodological shift in cybercrime, as cybercriminals are now directly targeting banks' networks, rather than targeting end-user banking customers.[6]

---

1. *See* Mike Lennon, *Hackers Hit 100 Banks in 'Unprecedented' $1 Billion Cyber Heist: Kaspersky Lab*, SEC. WEEK (Feb. 15, 2015), http://www.securityweek.com/hackers-hit-100-banks-unprecedented-1-billion-cyber-attack-kaspersky-lab (indicating that Carbanak attacks are still an active threat to banking entities); *see also* KASPERSKY LAB, CARBANAK APT THE GREAT BANK ROBBERY, VERSION 2.1 4 (2015), https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf ("Most of the victims based in the geolocation of infected IPs are located in Russia, USA, Germany, China and Ukraine.").

2. KASPERSKY LAB, *supra* note 1, at 7. A Carbanak attack goes through the "backdoor" of a system, they are designed to provide cybercriminals with remote access to infected networks for purposes of data exfiltration and espionage. *Id.*

3. Konstantin Goncharov, *The Great Bank Robbery: Carbanak APT*, KASPERSKY LAB BUS. (Feb. 17, 2015), https://business.kaspersky.com/the-great-bank-robbery-carbanak-apt/3598/.

4. KASPERSKY LAB, *supra* note 1, at 4. The ATM network was also used to dispense cash from certain ATMs at certain times where money mules were ready to collect it. *Id.*

5. For example, one bank lost approximately $7.3 million due to ATM fraud, and another lost $10 million due to a successful infiltration of their online banking platform. *Id.*

6. KASPERSKY LAB, *The Great Bank Robbery: Carbanak Cybergang Steals $1bn From 100 FIs Worldwide*, [hereinafter "The Great Bank Robbery"] (Feb. 16, 2015), http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide.

Cybercriminals employing Carbanak attacks send spear phishing e-mails to bank employees in order to infect systems with custom malware containing video files that capture bank employees' activities.[7] This surveillance feature provides attackers with an operational picture of the banks practices that the cybercriminals later mimic to create fake transactions to transfer money into their own accounts.[8] The intelligence gained from custom malware enables cybercriminals to remain versatile in meticulously tailoring their attacks based on a specific bank's operational practices and vulnerabilities.[9] Perhaps most alarming, no matter what software the banks were using, the cybercriminals got in, often undetected, even though all malware leaves a trace or "marker" when it successfully infiltrates a system.[10] Unfortunately, this marker often goes unnoticed because financial institutions ("FIs")[11] have not revamped their cybersecurity infrastructure to include monitoring changes to their networks.[12]

In the face of these persistent cyber attacks, FIs 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.[13] Utilizing

---

7. KASPERSKY LAB, *supra* note 1, at 3, 21. In one series of attacks, the email attachments exploited vulnerabilities in Microsoft Office and Microsoft Word, which decrypted and opened up the "backdoor" (remote access point) known as Carbanak. *Id.*

8. *Id.* at 21; *see also* The Great Bank Robbery, *supra* note 6 ("In other cases cybercriminals penetrated right into the very heart of the accounting systems, inflating account balances before pocketing the extra funds via a fraudulent transaction. For example: if an account has 1,000 dollars, the criminals change its value so it has 10,000 dollars and then transfer 9,000 to themselves. The account holder doesn't suspect a problem because the original 1,000 dollars are still there.").

9. *See* KASPERSKY LAB, *supra* note 1, at 21.

10. *Id.* On average, each bank robbery took between two and four months, from infecting the first computer at the bank's corporate network to making off with the stolen money. *Id.*

11. INVESTOPEDIA, Definition of a Financial Institution, http://www.investopedia.com/terms/f/financialinstitution.asp (last visited Jan. 26. 2016). A financial institution is "[a]n establishment that focuses on dealing with financial transactions, such as investments, loans and deposits. Conventionally, FIs are composed of organizations such as banks, trust companies, insurance companies and investment dealers." *Id.*

12. *See* Lennon, *supra* note 1 (quoting Chief Technology Officer of Tripwire, Dwayane Melancon in saying that the Carbanak attacks are a "jarring reminder of how easy it is for even sophisticated enterprises to overlook damaging changes to their cyber infrastructure").

13. John W. Carlson, Testimony on Behalf of the Fin. Servs. Information Sharing & Analysis Ctr. ("FS-ISAC") Before the U.S. House of Rep. Comm. on Fin. Servs. 12 (June 24, 2015),
https://www.fsisac.com/sites/default/files/news/JCarlson%20June%2024%20Testimony%20

cyber intelligence analytics may aid FIs in better monitoring network activity, resulting in more effective threat detection, mitigation, and enhanced response strategies.[14] However, on their own, FIs often lack the resources to efficiently detect, analyze, and mitigate cyber attacks.[15] Meanwhile, the federal government has a strong foreign intelligence apparatus coupled with the cybersecurity capability to determine where the threat or attack came from, and how to stop it.[16] Therefore, proactive collaboration may lead to better cybersecurity solutions capable of keeping pace with the evolving nature of attacks against FIs.[17]

On December 18, 2015, President Obama signed into law the Cybersecurity Act of 2015 (the "Act"), which is designed to serve as a powerful vehicle to facilitate a collaborative initiative premised on cyber threat information sharing.[18] The Act establishes a voluntary cybersecurity information sharing process, and most significantly, clearly delineates liability[19] protections to private entities such as FIs that wish to share cyber threat information with one another and the federal government.[20] Although controversial among civil liberties and privacy

---

FINAL.pdf.

14. FED. FIN. INSTS. EXAMINATION COUNCIL, FFIEC CYBERSECURITY ASSESSMENT GENERAL OBSERVATIONS 3 (last visited Jan. 19, 2016), https://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Assessment_Observations.pdf.

15. *See id*. at 2 (comparing the limited position of private sector entities with the government who is "uniquely positioned to investigate, arrest, and prosecute cybercriminals; [and] to collect foreign intelligence on cyber threats. . ."); *see also* Carlson, *supra* note 13, at 19 ("While the financial sector is an example of a strong and frequent cyber collaboration and investment, we cannot fight this battle alone.").

16. *See* Judith H. Germano, *Cybersecurity Partnerships: A New Era of Public-Private Collaboration*, THE CTR. ON L. & SEC.: NYU SCH. OF L. 2 (Oct. 2014) (concluding that "the government can provide a more complete perspective on the threat and on effective mitigation techniques, while taking steps to protect individual victims").

17. *See id.* at 11 (A well-structured cybersecurity program requires consistent collaboration with and information sharing between the financial sector and the federal government.); *see also* FIN. STABILITY OVERSIGHT COUNCIL, ANNUAL REPORT 4, 9 (2015).

18. Cybersecurity Act of 2015, H.R. 2029, 114th Cong. (2015).

19. *See* Germano, *supra* note 16, at 8 ("Theories of liability revolve around both the actual breach and the company's response to the breach, including regarding the content and timing of notice and disclosure. And exposure can be grounded in statutory, regulatory, and common law.").

20. ALSTON & BIRD, THE CYBERSECURITY INFORMATION SHARING ACT IS NOW LAW 1–2 (Dec. 23, 2015), http://www.alston.com/Files/Publication/994c3e4b-2220-4c54-b5ca-9699571d0c89/Presentation/PublicationAttachment/40260001-f03b-4c3f-a7dc-9884d39de8c9/15-443-CybersecurityInformationSharingAct.pdf; CADWALADER, PRESIDENT OBAMA SIGNS CYBERSECURITY ACT OF 2015 TO ENCOURAGE CYBERSECURITY INFORMATION SHARING (Dec. 24, 2015), http://www.cadwalader.com/resources/clients-friends-memos/president-obama-signs-cybersecurity-act-of-2015-to-encourage-cybersecurity-

advocates, the Act is a positive and much needed step in furtherance of a joint solution to modern cyber warfare.[21] President Obama further demonstrated the critical need to strengthen the nation's cybersecurity infrastructure through a $19 billion allocation for cybersecurity initiatives in the fiscal 2017 budget.[22] The budget follows with instruction from President Obama directing his administration to implement a Cybersecurity National Action Plan (CNAP).[23] CNAP's initiatives "place[] significant focus on the private sector's role in securing the nation's cyber borders," and also mirrors the voluntary nature of the Act.[24]

This Note proceeds in five parts. Part II details FIs' stake in cyber warfare.[25] Part III highlights the importance of cyber risk assessments and the critical role cyber intelligence and collaboration play in threat detection and response.[26] Part IV discusses the collaborative imperative between the financial sector and the federal government, and the significance of recently passed cyber legislation that addresses information sharing practices.[27] Finally, Part V concludes by reiterating the pressing need for FIs to take a larger role in cyber risk mitigation.[28]

---

information-sharing.

21. White House Office of the Press Secretary, *FACT SHEET: Cybersecurity National Action Plan* (Feb. 9, 2016), https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan; Russell Brandom, *Congress Passes Controversial Cybersecurity Bill Attached to Omnibus Budget*, THE VERGE (Dec. 18, 2015, 12:08 PM), http://www.theverge.com/2015/12/18/10582446/congress-passes-cisa-surveillance-cybersecurity.

22. Allison Grande, *Obama Budgets $19B To Take Action Against Cyberattacks*, LAW360 (Feb. 9, 2016, 8:44 PM), http://www.law360.com/articles/756881/obama-budgets-19b-to-take-action-against-cyberattacks (noting this budget is a 35% "increase over the $14 billion that the president requested from Congress for these efforts for the 2016 fiscal year").

23. White House Office of the Press Secretary, *supra* note 21.

24. *See* Evan D. Wolff et al., *Highlights of Obama's Ambitious New Cybersecurity Plan*, LAW360 (Feb. 10, 2016, 5:47 PM) http://wwww.law360.com/articles/757763/highlights-of-obama-s-ambitious-new-cybersecurity-plan (noting the cybersecurity initiatives "draw heavily on the private sector's experience with cyber resilience and an enterprise-wide, multiyear approach to cybersecurity" and "does not impose cybersecurity obligations on the private sector").

25. *See infra* Part II.

26. *See infra* Part III.

27. *See infra* Part IV.

28. *See infra* Part V.

II. FIs' STAKE IN CYBER WARFARE

The Carbanak attacks demonstrate the very real and growing threat of cyber attacks on FIs.[29] Over the past decade, the networks of our nation's critical infrastructure have converged to create a digitized cyberspace that has transformed the way business is transacted across the globe.[30] Our information travels throughout this interdependent network of information technology infrastructures, and unfortunately it does not travel alone.[31] Cybercriminals, terrorists, and our adversaries launch cyber attacks through this interdependent network, leaving our nation's financial system and other critical infrastructures vulnerable to significant risk and potential destruction.[32]

A. The Cost of Cyber Warfare

Cyber attacks may significantly damage and disrupt the financial sector, requiring institutions to develop robust cybersecurity programs tailored to their individual needs.[33] Given the constantly evolving nature of these attacks, FIs must learn to adapt to new, emerging threats.[34] The price tag on any single cyber attack varies dramatically based on the interplay of a number of factors such as the type, frequency, and duration of the attack.[35]

---

29. Goncharov, *supra* note 3; *see also* Kevin L. Petrasic, *A Cybersecurity Catch-22 For Banks*, LAW360 (May 13, 2015, 10:25 AM) http://www.law360.com/articles/654392/a-cybersecurity-catch-22-for-banks (discussing "the increase in the number and sophistication of cyber attacks [that] [have] alarmed bank regulators and law enforcement officials").

30. General Keith Alexander, Address at AFCEA Conference at 5–6 (June 28, 2013). At the time of the address, General Alexander was the Director of the National Security Agency and Commander of U.S. Cyber Command. *Id. see also* White House Office of the Press Secretary, *supra* note 21.

31. General Keith Alexander, *supra* note 30, at 5–6.

32. *See id.* at 6; *see also* White House Office of the Press Secretary, *supra* note 21 ("Criminals, terrorists, and countries who wish to do us harm have all realized that attacking us online is often easier than attacking us in person."); Carlson, *supra* note 13, at 10 ("Many cybersecurity incidents, regardless of their original motive, have the potential to disrupt critical systems.").

33. *See* Press Release, U.S. Dep't of Treasury, Remarks of Deputy Secretary Raskin at the Texas Bankers' Association Executive Leadership Cybersecurity Conference (Dec. 3, 2014), https://www.treasury.gov/press-center/press-releases/Pages/jl9711.aspx ("Banks should have risk management frameworks that are appropriately tailored to the cyber risks presented by their specific businesses and operations.").

34. *Id.*

35. PONEMON INST., 2015 COST OF CYBER CRIME STUDY: UNITED STATES at 12–14

In cyber warfare, time is money.[36] The longer it takes to detect, mitigate, and fully resolve a cyber attack, the more costly it becomes.[37] According to a recent cybercrime study conducted by the Ponemon Institute,[38] participating organizations[39] spent the most on threat detection and recovery measures, which totaled over half of their annualized costs associated with cyber attacks.[40] Organizations that utilize security intelligence technologies reported having significantly lower costs than organizations that did not employ them.[41] The marginal difference between these entities is most prevalent in the detection phase, with nearly a $2 million increase in the annualized budget of organizations that do not deploy security intelligence technologies.[42] Despite the resources devoted to cybersecurity, running a successful cybersecurity program remains a challenge for many FIs.[43]

B. Budgeting for Defense

Due to the severe consequences associated with successful cyber attacks, FIs are increasingly willing to invest more in cybersecurity.[44] According to a report published by Homeland Security Research Corporation, the 2015 U.S. financial services cybersecurity market will reach $9.5 billon, which makes it the largest non-government cybersecurity market.[45] Branch Banking & Trust ("BB&T"), which has

---

(2015), http://www.ponemon.org/library/2015-cost-of-cyber-crime-united-states.

36. *See id*. at 4 (indicating a positive relationship between the time to contain an attack and organizational cost).

37. *Id*.

38. PONEMON INST., http://www.ponemon.org (last visited Feb. 1, 2016). The Ponemon Institute engages in private research on privacy, data protection, and information security in order to enable organizations to better protect their data and enhance their security practices. *Id.*

39. PONEMON INST., *supra* note 35, at 27. Financial service entities represented 17% of the study's sample size. *Id.*

40. *Id*. at 17. The average time to resolve a cyber attack was 46 days, with an average cost to participating organizations of $1,988,554 during this 46-day period. *Id.*

41. *Id*. at 19.

42. *Id*.

43. *See* Press Release, U.S. Dep't of Treasury, *supra* note 33 ("We have learned from these attacks, that the prevalence of cyber risk creates a persistent and complex challenge for FIs spanning the sector, including FIs of all types and all sizes.").

44. *See* PWC, TURNAROUND AND TRANSFORMATION IN CYBERSECURITY: FINANCIAL SERVICES 19 (2015), http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html (noting average information security spending is up 24%).

45. PRWeb, *U.S. Banking & Financial Services Cybersecurity Market to Reach $9.5*

$186.8 billion in assets, doubled its cybersecurity budget in the last several years.[46] Similarly, Bank of America CEO Brian Moynihan indicated that his company will spend approximately $400 million on cybersecurity in 2015.[47] Moynihan also disclosed that cybersecurity is the only unrestricted budget item within his company, reinforcing the notion that as cybersecurity constantly evolves, FIs must invest more to protect themselves, their networks, and their customers from cyber attack.[48]

C. Cyber Attacks Targeting the Financial Sector Continue to Increase in Volume and Sophistication

When famous bank robber Willie Sutton was asked why he robbed banks, he famously replied, "because that's where the money is."[49] Cybercriminals operate on the same wavelength; the volume of cyber attacks against FIs is three times that of any other industry.[50] The financial sector is thus inherently susceptible to cyber attacks given that banks and other FIs are quite lucrative targets to hackers.[51] Additionally, operative features employed by FIs, such as mobile banking and ATMs, increase their cyber threat vulnerability.[52] The increasing volume of threats affects all institutions regardless of size or type, and the malicious cyber actors vary considerably in terms of their internal motivation for the attack.[53]

Billion by 2015 Following an Unprecedented Annual Hike of 23% (Nov. 13, 2014), http://www.prweb.com/releases/2014/11/prweb12313135.htm.

46. Tracy Kitten, *BB&T CEO Making Security a Priority*, BANKING INFO SECURITY (May 5, 2015), http://www.bankinfosecurity.com/interviews/bbt-ceo-on-making-security-priority-i-2688.

47. Adam O'Daniel, *Moynihan: BofA's Cyber Security Given Unlimited Budget 'To Keep Us Safe'*, CHARLOTTE BUS. J. (Jan. 21, 2015), http://www.bizjournals.com/charlotte/blog/bank_notes/2015/01/moynihan-bofas-cyber-security-given-unlimited.html.

48. *Id.*

49. Carlson, *supra* note 13, at 11 (attributing the original quote to Sutton while noting that it is limited in its purpose for explaining why FIs are vulnerable to cyber threats given that the "quote does not capture the entirety of the situation we face today" as "FIs are [also] being targeted in response to international conflicts").

50. WEBSENSE SEC. LABS, 2015 INDUSTRY DRILL-DOWN REPORT FINANCIAL SERVICES 4 (2015), https://www.websense.com/content/2015-finance-industry-drilldown.aspx?intcmp=nav-mm-resources-finance-drill-down-report.

51. *Id.*

52. *See* FED. FIN. INSTS. EXAMINATION COUNCIL, *supra* note 14, at 1–2.

53. Carlson, *supra* note 13, at 11.

In addition to the significant increase in cyber attacks against the financial sector, these attacks are becoming more intricate and sophisticated.[54] Most FIs indicate that the greatest challenge to building an adequate cybersecurity program arises from the evolving nature and complexity of cyber threats, rather than budget restrictions.[55]

Cybercriminals are focusing on targeted attacks that are specifically tailored to individual FIs.[56] Targeted attacks theoretically carry more potential to damage the financial sector than "untargeted attacks," because they are generally more successful and harder to protect against.[57] In addition to the aforementioned Carbanak attacks, two common examples of targeted cyber attacks are spear-phishing campaigns and distributed denial-of-service attacks ("DDoS").[58] Spear-phishing campaigns appear to employees as seemingly legitimate e-mails that trick users into supplying sensitive information such as passwords that compromise the integrity of the network.[59] DDoS attacks impede access to banking services for extended periods of time by overwhelming web-based applications with voluminous, malicious network traffic designed to cause applications to shut down.[60] These attacks may also function as a diversion to draw attention away from simultaneous, but separate cyber attacks designed to steal customer account and proprietary information from the FIs network.[61]

In 2012 and early 2013, ten major U.S. banks fell victim to DDoS

---

54. Petrasic, *supra* note 29.

55. N.Y. STATE DEP'T OF FIN. SERVS., REPORT ON CYBER SECURITY IN THE BANKING SECTOR 10 (2014), http://www.dfs.ny.gov/about/press2014/pr140505_cyber_security.pdf ("The barriers to ensuring information security most cited by institutions were the increasing sophistication of threats (71%) and emerging technologies (53%).").

56. Petrasic, *supra* note 29.

57. *See id*. (distinguishing targeted attacks from untargeted attacks, as the former are specifically tailored to a single bank, and the latter is usually a mass wave designed to hit as many devices, users and services as possible).

58. *Id.*

59. Carlson, *supra* note 13, at 10.

60. Tracy Kitten, *DDoS Attacks: 2013 Forecast*, BANK INFO SEC. (Dec. 30, 2012), http://www.bankinfosecurity.com/ddos-attacks-2013-outlook-a-5396/op-1; *see also* Conference of State Bank Supervisors, *Cybersecurity 101: A Resource Guide for Bank Executives*, CSBS BLOG 18 (2014), https://www.csbs.org/CyberSecurity/blog/Pages/default.aspx ("Banks subject to a DDoS attack may face a variety of risks, including operational risks and reputation risks. The attack may also serve as a distraction while hackers attempt alternative types of fraud.").

61. Kitten, *supra* note 60 (referencing an alert issued by the Office of the Comptroller of the Currency on Dec. 21, 2012 "about the recent wave of DDoS attacks, noting that financial institutions had linked DDoS to fraud and the theft of proprietary information").

attacks, resulting in millions of dollars in losses.[62] The DDoS attacks not only illustrated the detrimental effect of successful cyber attacks on the financial sector, but they also sparked collaboration between the private and public sector to share information that fruitfully aided in mitigating active cyber attacks.[63]

III. STEPS TO IMPLEMENT AN EFFECTIVE CYBERSECURITY FRAMEWORK

The financial sector cannot single handedly defend against the complex and constantly evolving threat of cyber attacks.[64] The start of a solution to mitigate and prevent cyber attacks requires a collaborative, proactive relationship premised on information sharing between the government and private sector.[65] Although critical, information sharing is but one facet of cybersecurity.[66] Additional action is required by FIs in order to counter, prevent, and mitigate cyber attacks.[67]

Various financial service regulators have published best practices for FIs to consider when creating and modifying their individual cybersecurity programs.[68] Additionally, New York's top financial regulator, the Department of Financial Services, announced a plan to implement mandatory cybersecurity requirements for banks to complete "mandatory annual audits, enhance identity authentication for key data bases", and appoint a "single executive charged with managing their

62. *Id.*; *see also* Germano, *supra* note 16, at 11.

63. *See* Carlson, *supra* note 13, at 11 ("The DDoS attack also catapulted the cybersecurity issue to a CEO level across the entire financial services sector for the first time. When the CEOs of [FS-ISAC] member financial services companies engaged directly it resulted in even greater collaboration among the financial associations and government agencies.").

64. *See* Germano, *supra* note 16, at 1 ("Ultimately, the short answer is that no single actor (or group of actors) can figure it out alone.").

65. *See id.* at 1–2 ("A strategic cybersecurity solution mandates the combined resources and coordination of government and industry, within a practical framework that balances effectiveness with efficiency, and security with privacy and innovation.").

66. ERIC A. FISCHER & STEPHANIE M. LOGAN, CONG. RESEARCH SERV., R43996, CYBERSECURITY AND INFORMATION SHARING: COMPARISON OF H.R. 1560 AND H.R. 1731 4 (2015).

67. *Id.* at 4–5.

68. KATTEN MUCHIN ROSENMAN LLP, CYBER-ATTACKS: THREATS, REGULATORY REACTION AND PRACTICAL PROACTIVE MEASURES TO HELP AVOID RISKS (Jun. 24, 2015), https://www.kattenlaw.com/Cyber-Attacks-Threats-Regulatory-Reaction-and-Practical-Proactive-Measures-to-Help-Avoid-Risks. For example, the Securities and Exchange Commission ("SEC"), Commodities Future Trading Commission, and the Financial Industry Regulatory Authority all have best published practices. *Id.*

information security."[69] While there is no "silver-bullet" solution, or a universal approach to defend against the vast array of cyber attacks, cybersecurity programs based on a holistic view of technology, operational practices, and cyber threat intelligence will prove most efficient in tackling the cyber threats that carry the most destructive potential.[70]

The Pareto Principle ("80/20 rule") reflects the notion that approximately 80% of effects originate from only 20% of causes.[71] The 80/20 rule provides sound guidance on how FIs should individually approach cybersecurity protection measures.[72] Given that not all cyber attacks create the same level of risk, resources should be prioritized to defend against attacks that compose the critical 20% of incidents.[73] Further, no two FIs are the same, and thus, cybersecurity program decisions must be based on a particular institution's unique assets and characteristics.[74] An assessment of an FI's inherent risk and cyber incident response program is a highly informative first step to developing an effective cybersecurity program, and identifying the 20% of causes that pose the greatest risk.[75]

A. Cybersecurity Risk Assessment: The Discovery Phase

The discovery phase requires a baseline examination of a particular FI's inherent cybersecurity risk, which incorporates the type, volume, and complexity of operational features utilized by the

---

69. Evan Weinberger, *NY Outlines Coming Bank, Insurer Cybersecurity Rules*, LAW360 (Nov. 10, 2015, 12:51 PM), http://www.law360.com/articles/725482/ny-outlines-coming-bank-insurer-cybersecurity-rules.

70. *See* Germano, *supra* note 16, at 14; *see also* Mark Clancy, *Applying the 80/20 Rule to Cyber Security Practices*, INFORMATIONWEEK DARK READING (Aug. 19, 2015), http://www.darkreading.com/perimeter/applying-the-80-20-rule-to-cyber-security-practices/a/d-id/1321818.

71. *See* Clancy, *supra* note 70.

72. *Id.*

73. *Id.* (noting that this critical 20% of incidents will differ depending on a specific FIs characteristics and operational practices).

74. *See id.* ("Unfortunately, we continue to see too many instances where firms take a 'one-size fits all' approach to their cyber defenses, focusing too many resources on lower-level risks, such as wide-scale malware campaigns, and not enough on the most destructive attacks.").

75. *Id.* Significant financial resources are often drained when cybercriminals strike, as hefty costs are incurred in the discovery, analysis, mitigation and closure phases of a cyber attack. *Id.*

institution.[76] On June 30, 2015, the Federal Financial Institutions Examination Council ("FFIEC")[77] launched a comprehensive Cybersecurity Assessment Tool[78] ("Assessment") to help FIs identify their inherent risks and assess their cybersecurity preparedness.[79] The Assessment serves as a tool for FIs of all sizes to understand their unique cybersecurity risks, especially when introducing new products, services, or initiatives.[80]

Whether or not the Assessment is mandatory for FIs has been discussed among examiners, bankers, and experts in the financial sector.[81] The conclusion is that legally the Assessment is not mandatory, but it may be necessary as a practical matter.[82] Looking collectively at the supplemental announcements of the Federal Reserve Board ("the Fed"), the Office of the Comptroller of the Currency ("OCC") and the Federal Deposit Insurance Corporation ("FDIC"), the Assessment will at least be discussed, if not used in the regulators' next examination cycle for FIs.[83] The OCC and the Fed have been the most explicit in their intention to incorporate the Assessment into their examinations—by late 2015 for the OCC and by early 2016 for the Fed.[84] The FDIC, however, maintains that the Assessment is voluntary, but will be discussed by FDIC

---

76. FED. FIN. INSTS. EXAMINATION COUNCIL, *supra* note 14.

77. *Regulatory Agencies*, FED. FIN. INSTS. EXAMINATION COUNCIL, https://ffiec.gov/agencies.htm. The FFIEC consists of the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Consumer Financial Protection Bureau. *Id.*

78. FED. FIN. INSTS. EXAMINATION COUNCIL, OVERVIEW FOR CHIEF EXECUTIVE OFFICERS AND BOARDS OF DIRECTORS (Jun. 2015), https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_CEO_Board_Overview_June_2015_PDF1.pdf [hereinafter "FFIEC OVERVIEW FOR CEOS AND BOD"]. The Assessment functions as two parts, the inherent risk profile and the cybersecurity maturity assessment. Intertwined in the inherent risk profile assessment are both internal and external concerns that take into account the risks posed by FIs connection types, products, services and technologies used by examining the type, volume and complexity of these operational features. On the other hand, the maturity assessment focuses more specifically on an institution's response and recovery ability by looking at specific controls and practices that are in place. *Id.*

79. *Id.* at 1; Press Release, Fed. Fin. Insts. Examination Council, Releases Cybersecurity Assessment Tool (Jun. 30, 2015), https://www.ffiec.gov/press/pr063015.htm

80. FFIEC OVERVIEW FOR CEOS AND BOD, *supra* note 78, at 4.

81. *See* Chad Knutson, *Is the FFIEC Cybersecurity Assessment Tool Required*? SECURE BANKING SOL. (2015), https://www.protectmybank.com/is-the-ffiec-cybersecurity-assessment-tool-required/.

82. *Id.*

83. *Id.*

84. *Id.*

examiners with institution management during the examination.[85] An adverse score on cybersecurity measures will affect the management ("M") column of a banks CAMELS[86] rating, as failure to conduct the Assessment may send a negative message regarding an FI's ability or willingness to manage cyber risks.[87]

As a practical matter, the Assessment advances FIs' interest in network and data protection by incorporating cybersecurity-related principles from regulatory guidance to identify areas in their security plans and response programs that may need improvement.[88] The Assessment also reflects the notion that cybersecurity should be viewed as an element of an FI's overall risk management strategy, rather than as an independent subset of the IT department.[89] This shift in cybersecurity focus to management and board oversight helps set a strong interconnected cybersecurity culture from the top down.[90]

1. Cybersecurity Inherent Risk: Connection Types & Mobile Banking

FIs are inherently susceptible to cyber attacks due to their use of certain operative features that contribute to their vulnerability.[91] In particular, the risks accompanying the use of third-party and cloud vendors, as well as the dangers associated with mobile banking applications and ATMs, puts a bulls-eye on the networks of FIs of all

85. FED. DEPOSIT INS. CORP., FINANCIAL INSTITUTION LETTERS: CYBERSECURITY ASSESSMENT TOOL (July 2, 2015).

86. *See generally* FED. DEPOSIT INS. CORP, 5000 – STATEMENTS OF POLICY, UNIFORM FINANCIAL INSTITUTIONS RATING SYSTEM (1996) (explaining the CAMELS rating system).

87. Knutson, *supra* note 81.

88. *See* Alan Deer & Brad Neighbors, *Assessing Your Cybersecurity Preparedness: It May Be Time to Update Your Bank's Information Security and Response Program*, JB SUPRE BUS. ADVISOR (July 2015), http://www.jdsupra.com/legalnews/balch-bingham-financial-update-july-57357/.

89. *See* Judy A. Selby & Jonathan A. Forman, *C for Cybersecurity: There's a New Meaning To "C-Suite" As Cybersecurity Is Not Just An IT Risk*, LEGAL TECH NEWS (Jun. 5, 2015), http://www.legaltechnews.com/id=1202728196571/C-Is-for-Cybersecurity?slreturn=20160020134828 ("Regulators have made clear that cybersecurity is now a C-suite issue.").

90. FED. FIN. INSTS. EXAMINATION COUNCIL, *supra* note 14, at 1–2.

91. *See id.* at 1 ("Cybersecurity inherent risk is the amount of risk posed by a financial institution's activities and connections, notwithstanding risk-mitigating controls in place. A financial institutions cybersecurity inherent risk incorporates the type, volume, and complexity of operational considerations, such as connection types, products and services offered, and technologies used.").

sizes.[92] Additionally, the numerous connection types and access points may contribute to FI's inherent risk.[93] Each operative feature employed by an FI to carry out banking services may impose a unique cybersecurity risk to an institution given that cyber hackers tend to develop specially tailored techniques to target specific products, services, and technologies used such as core systems, ATMs, and mobile applications.[94]

FIs use a variety of connection types and access points and each presents a potential entry point for cyber attackers.[95] Failure to take proactive measures to protect these entry points may lead to undetected exposure to malware or other types of attacks.[96] In order to prevent entry point cyber attacks, all devices used by employees to access the institution's network should have the appropriate anti-virus and anti-malware protections in place.[97] Additionally, routine network scans for unauthorized devices and malware are highly encouraged to better detect and mitigate cyber attacks.[98]

Customer use of mobile banking has increased substantially in recent years.[99] With greater convenience comes greater security concerns as mobile banking has created a new entry point for cyber attackers.[100] Customers engaged in mobile banking do so with security settings of their choosing, but the baseline of such settings is still at the discretion of the institution.[101] FIs that only require minimal security settings may

92. *Id.* at 2–4.

93. *Id.* at 1.

94. *Id.* at 1–2.

95. *Id.* at 1.

96. *Id.*

97. *See id.* at 3 ("Most financial institutions have tools in place, such as anti-virus and anti-malware tools, to detect previously identified attacks.").

98. *See id.* ("[FIs] institutions should routinely scan IT networks for vulnerabilities and anomalous activity, test systems for their potential exposure to cyber attacks, and remediate issues when identified.").

99. Conference of State Bank Supervisors, *supra* note 60. By 2016, an estimated 96 million U.S. consumers will adopt mobile banking to conduct financial transactions. *Id.*

100. *See id.* ("Mobile banking has opened a new door for cybercriminals and the ecosystem of mobile banking involves several players, which can be challenging when addressing issues of security.").

101. *See* Jerome F. Combs, *Mobile Banking Risk Identification and Mitigation*, CMTY. BANK CONNECTIONS (2014), https://www.communitybankingconnections.org/articles/2014/q1/mobile-banking-risk-identification-and-mitigation ("Providing consumers with the ability to transact banking business using a mobile device — with security settings of the customer's choosing — places an increasing amount of control over sensitive financial data into consumers' hands.").

increase the risks of mobile-banking.[102] Accordingly, increased security technology that surpasses basic username and password sign-in, known as "multi-factor authentication," ("MFA")[103] is in the works for many companies such as Intel, American Express, and MasterCard.[104] The primary goal of MFA is to make it more difficult for hackers to penetrate a network or database by building a layered defense.[105] President Obama has even called upon his administration to "kick off a public awareness campaign and work in coordination with technology and financial services companies to make MFA technology accessible and to help individual Americans understand their role in protecting the nation's cybersecurity."[106]

Some suggest replacing passwords altogether with biometric data such as fingerprints, iris scans, and voice recognition to verify a mobile banking user's identity when logging in.[107] The launch of the iPhone 6s also presents a new way to secure mobile banking through its 3D touch and improved camera features.[108] Mobile banking is constantly evolving

---

102. *See id.* ("The net loss of control over information makes it more difficult for the bank to assess risks and implement effective risk mitigation strategies.").

103. Margaret Rouse, *Multifactor Authentication (MFA) Definition*, TECH TARGET (last visited Jan. 20, 2015), http://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA (MFA "is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction. [MFA] combines two or more independent credentials: what the user knows (password), what the user has (security token) and what the user is (biometric verification).").

104. *See* White House Office of the Press Secretary, *FACT SHEET: White House Summit on Cybersecurity and Consumer Protection* (Feb. 13, 2015), https://www.whitehouse.gov/the-press-office/2015/02/13/fact-sheet-white-house-summit-cybersecurity-and-consumer-protection; *see also* PwC, *supra* note 44, at 8 ("Banks, in particular, are moving away from traditional passwords for both clients and employees.").

105. *See* PWC, *supra* note 44, at 8 (discussing multiple benefits of advanced authentication, such as improved customer/business partner confidence in security and privacy, enhanced/reduced fraud protection, more secure online transactions, improved customer experience, and improved regulatory compliance).

106. Wolff, et al., *supra* note 24; *see also* White House Office of the Press Secretary, *supra* note 21 ("The President is calling on Americans to move beyond just the password to leverage multiple factors of authentication when logging-in to online accounts.").

107. *See* Sandeep Sood, *Passwords Are Dead: Biometrics and The Future of Banking Security*, THE FIN. BRAND (Feb. 3, 2015), http://thefinancialbrand.com/49952/biometrics-mobile-banking-security/; *see also* PwC, *supra* note 44, at 8 (noting an example of how biometrics enabled a Texas based financial services and insurance firm to enhance security and customer service, while improving the ease of use for mobile banking customers).

108. Jim Marous, *iPhone 6s Provides Opportunity for Banking*, THE FIN. BRAND (Sept. 11, 2015), http://thefinancialbrand.com/53943/iphone-6s-banking-opportunity/. The iPhone 6s's improved FaceTime camera may be utilized for facial recognition in improved identity verification processes on mobile banking applications, as well as to enhance mobile check

as technology becomes more innovative, and therefore FIs' cybersecurity posture must also evolve with innovation.[109]

2. External Dependency Management: Third-Party Vendors

FIs depend on numerous third-party vendors to carry out critical banking functions.[110] Reliance on third-party vendors is a continuing challenge as it frustrates cybersecurity solutions across the financial sector.[111] Improper controls over a third-party vendor's handling of sensitive consumer data may result in successful cyber attacks that expose the FI's network and thus, consumer data.[112] Such lack of control over third-parties essentially wastes any resources invested in cybersecurity protection by the FI.[113] In order to prevent wasting resources invested in cybersecurity protection, FIs should consider increasing spending and allocation towards addressing third-party security concerns.[114]

Financial regulators have also made it clear that FIs cannot evade liability for damages that result from inadequate cybersecurity controls of third-party vendors.[115] Therefore, if third-party vendors are left unregulated, their lack of security measures can tremendously weaken the cybersecurity infrastructure of an FI, which may lead to astronomical losses for FIs that are left responsible for the resulting damage.[116]

---

deposit practices. *Id.*

109. *See* Conference of State Bank Supervisors, *supra* note 60 ("As technology continues to advance and rapidly change, it is critical that all [FIs], regardless of size, constantly assess their cybersecurity preparedness and review their technology infrastructure for vulnerabilities.").

110. *See* N.Y. STATE DEP'T OF FIN. SERVS., UPDATE ON CYBER SECURITY IN THE BANKING SECTOR: THIRD PARTY SERVICE PROVIDERS 3 (2014) (noting examples of high-risk third-party vendors utilized by FIs, such as "check/payment processors, trading and settlement operations, and data processing companies").

111. *Id.* at 2.

112. INDEP. CMTY. BANKERS OF AM., CYBERSECURITY: THE COMMUNITY BANK PERSPECTIVE 1–2 (May 19, 2015), http://www.icba.org/files/ICBASites/PDFs/test051915.pdf.

113. *See id.* ("Securing financial data at [FIs] is of limited value if it remains exposed at the point-of-sale and other processing points.").

114. *Id.*

115. *See* KATTEN MUCHIN ROSENMAN LLP, *supra* note 68 (noting the importance for firms to conduct vendor due diligence given that "financial regulators are making it increasingly clear that financial services firms will be liable for cyber-attacks as a result of improper controls at third-party service providers").

116. N.Y. STATE DEP'T OF FIN. SERVS., *supra* note 110, at 6 ("47% of the surveyed institutions reported having cyber insurance policies that explicitly cover information security

Management of this particular facet of external dependencies requires FIs of all sizes to establish rigorous vendor management controls guided by a clear delineation of the third parties' responsibilities.[117] FIs should adopt risk management processes that align the complexity of their relationship with third-party vendors that ensures comprehensive risk management and oversight of their critical activities.[118] A crucial component of such an agreement requires the third-party to notify the parent FI if a data breach or cyber attack comprises their or their subcontractor's network.[119] Accordingly, third-party vendor contracts should require notification if they intend to use subcontractors, and include further specifications and limitations on such use.[120]

Contracts between third-party vendors and FIs should also clearly define the parties' respective duties and liability in the event of a successful cyber attack.[121] Strict agreements that impose financial responsibility on third-party vendors who fail to take adequate security precautions may serve as a strong incentive for them to implement effective security measures.[122] Also, a detailed contractual agreement may demonstrate that an FI exercised due care, thus decreasing the likelihood it will face penalties for potential civil or regulatory liability.[123] The financial industry has started to take action to address risks imposed by third-party vendors, but this progress is far from uniform and tends to vary based upon the size and type of institution.[124]

---

failures by a third-party vendor."). The results discussed in the update are based on the responses of 40 state regulated banking organizations in New York. *Id.* at 2.

117. *See* Office of the Comptroller of the Currency, *Third-Party Relationships: Risk Management Guidance*, U.S. DEPT. OF THE TREASURY (Oct. 30, 2013), http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

118. *Id.*

119. *Id.*

120. *See id.* (FIs may also want to "[r]eserve the right to terminate the contract without penalty if the third party's subcontracting arrangements do not comply with the terms of the contract.").

121. *Id.*

122. *See* INDEP. CMTY. BANKERS OF AM, *supra* note 112 ("Allocating financial responsibility with the party that is best positioned to secure consumer data will provide a strong incentive for it to do so effectively.").

123. *See* Office of the Comptroller of the Currency, *supra* note 117 ("Developing a contract that clearly defines expectations and responsibilities of the third party helps to ensure the contract's enforceability, limit the bank's liability, and mitigate disputes about performance."); *see also* KATTEN MUCHIN ROSENMAN LLP, *supra* note 68 (noting the importance for firms to conduct vendor due diligence).

124. N.Y. STATE DEP'T OF FIN. SERVS., *supra* note 110, at 2. Larger to midsize financial firms are more likely than small firms to require a pre-contract or periodic on-site assessment

3. Cybersecurity Management and Staff Training

Clear delegation of cybersecurity management oversight responsibilities to a specific senior employee can strengthen cybersecurity programs because it holds a single person accountable for lapses in oversight or implementation of the FI's cybersecurity policies.[125] Inadequate security awareness among employees has been documented as one of the greatest inhibitors to an effective cybersecurity posture.[126] Therefore, management should also focus on educating employees through exercises that animate various types of cyber threats and associated complications.[127]

Utilization of cyber simulations has been noted as one extremely effective measure to facilitate a comprehensive and effective cyber response program.[128] A cyber incident simulation requires the IT security team to create a simulated attack to which the staff responds by working through their incident response procedure—this provides critical insight into any weaknesses in the program that need strengthening.[129] Additionally, such exercises may allow the IT team, management, and other personnel to individually understand their respective role in the event of a successful cyber attack.[130] An understanding of their role may accordingly reduce the damage caused by the attack through more efficient and educated threat mitigation responses.[131]

---

of high risk third-party vendors, and smaller firms are also significantly less likely to require third-party vendors to impose minimum information security requirements on subcontractors. *Id*. at 3.

125. KATTEN MUCHIN ROSENMAN LLP, *supra* note 68.

126. WEBSENSE SEC. LABS, *supra* note 50.

127. Kitten, *supra* note 46.

128. *Id.* Kelly King, CEO of BB&T, declared in an interview that cybersecurity training, such as cyber attack simulations play a vital role at his company. *Id*.

129. *See id.* (Kelly King, CEO of BB&T, expressly endorsed the exercise, referring to it as "an extremely eye-opening process" that he considers "one of the best things [he] [has] done at BB&T."); *see also* Press Release, U.S. Dep't of Treasury, *supra* note 33 ("These exercises allow CEOs, directors, and other key players to figure out how they will navigate the pressures and problems that come from the intrusion.").

130. Press Release, U.S. Dep't of Treasury, *supra* note 33.

131. *Id.*

B. Cyber Threat Intelligence and Collaboration: The Analysis Phase

The analysis phase of cybersecurity programs hinges on threat intelligence[132] and collaboration that seeks to speed up incident detection, response, and mitigation.[133] Cyber incident analysis requires institutions to gather, monitor, evaluate, and *share* information in order to identify and prevent cyber threats in the industry.[134] The necessity of this phase has begun to leverage collaborative industry utilities, such as the Financial Services Information Sharing and Analysis Center ("FS-ISAC"), that share threat information and remediation tactics across the financial sector.[135]

The FS-ISAC is the financial sector's primary resource for cyber threat information analysis and sharing.[136] Over the past decade, participation in FS-ISAC has grown exponentially from sixty members in 2004 to over 6,000 members as of 2015.[137] The FS-ISAC offers a wide range of information sharing capabilities designed to provide members with actionable threat information to better detect and mitigate cyber attacks.[138] In order to quickly disseminate information throughout the financial sector, the FS-ISAC utilizes Soltra-Edge, an industry-driven threat intelligence sharing platform designed to decrease the time of detection and mitigation from weeks and days to hours and minutes.[139] Soltra-Edge is the product of a joint venture between FS-ISAC and

---

132. FED. FIN. INSTS. EXAMINATION COUNCIL, *supra* note 14, at 3. The FFIEC defines threat intelligence as "the acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions and activities that offer courses of action to enhance decision making." *Id.*

133. Clancy, *supra* note 70.

134. *See* FED. FIN. INSTS. EXAMINATION COUNCIL, *supra* note 14, at 3.

135. Clancy, *supra* note 69; *see also* FED. FIN. INSTS. EXAMINATION COUNCIL, *supra* note 14, at 3.

136. Press Release, U.S. Dep't of Treasury, *supra* note 33.

137. *See* Carlson, *supra* note 13, at 2 (identifying member organizations to include "commercial banks and credit unions of all sizes, markets and equities firms, brokerage firms, insurance companies, payments processors, and 40 trade associations representing all of the U.S. financial services sector").

138. FIN. SERV. INFO. SHARING AND ANALYSIS CTR., *About FS-ISAC* (2015), https://www.fsisac.com/about; *see also* Carlson, *supra* note 13, at 2 ("The FS-ISAC's goals are to disseminate and foster the sharing of relevant and actionable information and analysis among participants to ensure the continued public confidence in the global financial services and to protect the financial services sector against cyber and physical threats, vulnerabilities, and risk.").

139. *Id.* at 8.

Depository Trust and Clearing Corporation to develop a fully automated cyber threat information sharing process.[140]

This information sharing platform leverages deep cybersecurity expertise from the financial industry.[141] FS-ISAC works closely on risk mitigation strategies with the U.S. Treasury Department, financial regulators, the Department of Homeland Security ("DHS"), and other government and law enforcement agencies.[142] This ongoing collaboration is set in place to respond to changing threats and seeks to build on the strong risk management culture within the financial industry.[143] FS-ISAC also conducts "joint exercises to test its communications, response and resiliency protocols during incident scenarios affecting different segments of the financial system."[144]

C. The Value of Information Sharing

The private sector can benefit from valuable information collected and analyzed by the government by integrating that information into effective risk controls and cybersecurity management to better mitigate and detect cyber attacks.[145] FS-ISAC has picked up on this notion and has accordingly worked closely with government agencies to obtain security clearances for key financial services sector personnel that have been utilized to brief the sector on developing security threats and information.[146] Furthermore, the cost of sharing information is relatively small, and the benefits can be quite rewarding.[147]

---

140. Press Release, Fin. Servs. Info. Sharing and Analysis Ctr., Soltra Edge, The First Industry Driven Threat Intelligence Sharing Platform Now Generally Available, Easy to Use and Free to License (Dec. 3, 2014), https://www.fsisac.com/sites/default/files/news/FINAL2%20Soltra%20Edge%20GA%20press%20release_12%203%2014WEB2.pdf.

141. *Id.*

142. Carlson, *supra* note 13, at 12.

143. *See id.* (noting also that these collaborative efforts are performed "in conjunction with extensive regulatory requirements").

144. *Id.* at 4.

145. N. ERIC WEISS, CONG. RESEARCH SERV., R43821, LEGISLATION TO FACILITATE CYBERSECURITY INFORMATION SHARING: ECONOMIC ANALYSIS 1, 5 (2015).

146. Carlson, *supra* note 13, at 8 ("These clearances have been used to brief the sector on new information security threats and have provided valuable information for the sector to implement effective risk controls to combat these threats.")

147. *See* WEISS, *supra* note 145, at 4 (noting that despite the cost reducing benefit of information sharing, "a review of recent data breaches shows that most of the details about breaches are released by third party experts, not the firms involved"); *see also* Clancy, *supra*

The success of such collaboration in mitigating cyber threats is illustrated by the combined response to the 2012 DDoS attacks on American banks.[148] At the time of the attacks, representatives from Wells Fargo, PNC Financial Corp., and U.S. Bank affirmed they had cybersecurity strategies in place to fend off DDoS attacks, but these attacks were simply unprecedented in terms of the volume of traffic that was used to bombard the online banking systems to a point of disruption.[149] As FIs were scrambling to mitigate the voluminous and destructive threats, banks began to share information with other FIs and the federal government at an unprecedented level.[150] The increased information sharing proved extremely beneficial to FIs that were later targeted on the second, third and fourth wave of DDoS attacks.[151] FIs later attacked were able to utilize threat intelligence information from the initial attack to detect and more quickly mitigate subsequent DDoS attacks.[152] The faster recovery and mitigation by FIs attacked in the latter waves illustrates the value of collaboration and information sharing on a more proactive basis, rather than waiting for crisis mode to strike.[153]

Despite the incident response and mitigation benefits illustrated above, FIs that have been hit by a cyber attack still often hesitate to share, analyze or discuss information regarding the attack.[154] Such insular thinking leaves other FIs vulnerable to the same attack, and only further frustrates cybersecurity solutions.[155] A major premise of the FS-ISAC is

---

note 70 ("Collaborative cyber security threat information tools will not only enable firms to identify incidents more quickly, but at their best, should also empower them to either proactively prevent issues or mitigate them quickly.").

148. Germano, *supra* note 16, at 11–12.

149. Nicole Perlroth, *In Cyberattacks on Banks, Evidence of a New Weapon*, NY TIMES (Oct. 5, 2012), http://bits.blogs.nytimes.com/2012/10/05/in-cyberattacks-on-banks-evidence-of-a-new-weapon/?_r=0; *see also* Germano, *supra* note 16, at 11 ("At the peak of those DDoS attacks, U.S. banks were grappling with
electronic traffic of up to 120 gigabytes per second—at least three times the volume of traffic most large bank websites were equipped to handle at the time—and banks were spending tens of millions of dollars to mitigate the problem.").

150. Carlson, *supra* note 13, at 11.

151. *Id.*

152. Not only did the DDoS attacks ignite a wave of information sharing, but it also for the first time launched the issue of cybersecurity to a CEO level across the financial sector. *Id.*

153. Germano, *supra* note 16, at 2–8.

154. WEISS, *supra* note 145, at 4–5 (discussing perceived legal barriers to information sharing and economic incentives to not share information about cyber attacks and defenses).

155. WEISS, *supra* note 145, at 6; *see also* Clancy, *supra* note 70.

to preserve anonymity of the threat intelligence data, which should reduce the concerns of reluctant FIs that fear public disclosure of their vulnerability.[156] However, the services offered by FS-ISAC lack the clearly delineated liability protections, for which the private sector has advocated, and therefore, the incentive for FIs to share threat information.[157]

IV. COLLABORATIVE IMPERATIVE: THE NEED FOR SYMBIOSIS IN THE CYBER ECOSYSTEM

Given their breadth of resources, crucial insight, and expertise, FIs are in an optimal position to provide valuable cyber threat information to the federal government that may aid mitigation of cyber attacks across the nation.[158] However, concerns regarding reputational damage, regulatory enforcement actions, and civil liability risks often inhibit private entities' willingness to share sensitive threat information.[159] Such hesitation is largely due to the unique challenges faced by FIs in cyber warfare that require they balance two separate, but very much intertwined interests.[160] On one hand, they have to focus on their business interest in preventing cyber attackers from gaining access to valuable data or money through the FI's network.[161] On the other hand, FIs must always consider their duty to protect customer privacy and civil liberties.[162] Striking a balance between these intertwining interests has vexed Congress and the executive branch for many years, and remains a controversial debate

156. *Id.* at 5 (listing "[p]ublic disclosure of a breach may cost an organization customers and sales and affect its stock price" as one example of an economic incentive not to share cyber threat information).

157. Carlson, *supra* note 13, at 17.

158. *See* Germano, *supra* note 16, at 2–3 (discussing the optimal position of the private sector, i.e. FIs to engage in a collaborative information sharing relationship with the government); *see also* Carlson, *supra* note 13, at 12 ("[R]eliance on others gives us in the financial services sector a unique and critical role in the cyber landscape and requires coordinated action for the most effective response.").

159. *See* Germano, *supra* note 16, at 2–8 (discussing the "legal, pragmatic, cultural, and competitive hurdles to effective cooperation that need to be addressed"); *see also* ALSTON & BIRD, *supra* note 20, at 1; FISCHER & LOGAN, *supra* note 66, at 2.

160. *See* Petrasic, *supra* note 29 ("[B]anks are fighting a two-front war—preventing cybercriminals from gaining access to funds and private data, and satisfying compliance and regulatory requirements imposed by regulators and law enforcement.").

161. *Id.*

162. *See id.* (noting that successful cyber threat defense strategies may be partially impeded by a misalignment between the goals of the FI and their regulators or law enforcement agencies).

among privacy advocates and business leaders in the private sector.[163]

A. The Call for Legislation

Over 100 cybersecurity bills have been introduced in Congress in the past five years, most of which were largely unsuccessful.[164] In 2014, the National Cybersecurity Protection Act made official DHS's already-existing cybersecurity information sharing center, known as the National Cybersecurity and Communications Integration Center (the "Integration Center").[165] The Integration Center, a creature of DHS, functions in essentially the same voluntary manner as FS-ISAC, as it works closely with private entities and the federal government to "analyze[] cybersecurity and communications information, share[] timely and actionable information, and coordinate[] response, mitigation and recovery efforts."[166] Despite the partial leap forward afforded by the 2014 National Cybersecurity Protection Act, the law still lacked the clearly defined liability protections advocated for by private entities.[167] The financial sector continued to actively voice its desire for Congress to delineate specific legal protections for private entities that wish to share cyber threat information with one another and the federal government.[168] In a letter to Senate leaders, various financial trade groups[169] expressed

---

163. *See* ALSTON & BIRD, *supra* note 20, at 1.

164. JAMES ARDEN BARNETT JR., RECENT TRENDS IN NATIONAL SECURITY LAW: LEADING LAWYERS ON BALANCING US NATIONAL SECURITY CONCERNS AND THE RIGHTS OF CITIZENS, IN CYBER SECURITY: FIXING POLICY WITH NEW PRINCIPALS AND ORGANIZATION 3 (Aspatore 2014).

165. National Cybersecurity and Critical Infrastructure Protection Act of 2014, H.R. 3696, 113th Cong. (2013–2014).

166. U.S. Comput. Emergency Readiness Team, *National Cybersecurity and Communications Integration Center*, U.S. DEP'T OF HOMELAND SEC., https://www.us-cert.gov/nccic (last visited Feb. 13, 2016).

167. *See Joint Trades Letter Supporting S.754 Cybersecurity Information Sharing Act of 2015*, CONSUMER BANKERS ASS'N. (Apr. 13, 2015), http://consumerbankers.com/cba-issues/comment-letters/joint-trades-letter-supporting-s754-cybersecurity-information-sharing-act ("The financial services industry is dedicated to improving our capacity to protect customers and their sensitive information but as it stands today, our laws do not do enough to foster information sharing and establish clear lines of communication with the various government agencies responsible for cybersecurity.").

168. *Id.*

169. *Id.* The trade groups include: American Bankers Association, American Financial Services Association, American Insurance Association, The Clearing House, Consumer Bankers Association, Credit Union National Association, Electronic Transactions Association, Financial Services Forum, Financial Services Roundtable, Independent Community Bankers of America, Investment Company Institute, NACHA-The Electronic

this desire, explaining that such liability protections will foster more proactive information sharing among the private sector and federal government.[170]

On October 27, 2015, the Senate passed the Cybersecurity Information Sharing Act of 2015 ("CISA"), which set forth a voluntary framework for private entities and the federal government to share cyber threat information.[171] Although the financial sector as a whole demonstrated overwhelming support for CISA, the Financial Services Roundtable expressed very specific concerns about problematic language found in Section 407, which addressed protecting critical infrastructures that are at the greatest risk to cyber attack.[172] If enacted, Section 407 would have essentially created duplicative regulatory oversight for large financial service firms.[173] Section 407 would have granted authority to the Secretary of Homeland Security and the appropriate agency head to conduct an assessment and develop a strategy that addresses each of the "covered entities," which may have encompassed large FIs.[174] Further, Section 407 would have granted the federal government the authority to *mandate* reporting requirements by covered entities that would have completely undermined the voluntary nature of the bill.[175]

FIs viewed the Senate's passage of CISA as a major win.[176] At first blush, it seemed that a tough battle remained to reconcile the bill with similar House-passed legislation earlier in 2015— HR. 1560 and

---

Payments Association, National Association of Federal Credit Unions National Association of Mutual Insurance Companies, Property Casualty Insurers Association of America, Securities Industry and the Financial Markets Association. *Id.*

170. *Id.* The letter stated in part, "[t]he financial services industry is dedicated to improving our capacity to protect customers and their sensitive information but as it stands today, our laws do not do enough to foster information sharing and establish clear lines of communication with the various government agencies responsible for cybersecurity." *Id*.

171. Cybersecurity Information Sharing Act, S. 754, 114th Cong. (2015).

172. Press Release, Fin. Servs. Roundtable, FSR Applauds Senate's Passage of CISA as a Victory for Strengthening Defenses Against Cyber Attacks (Oct. 27, 2015), http://fsroundtable.org/fsr-applauds-senates-passage-of-cisa-as-a-victory-for-strengthening-defenses-against-cyber-attacks/.

173. *Id.*

174. *See id*. Covered entities are identified pursuant to Section 9(a) of Executive Order 13636, which identifies critical infrastructures "where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security." Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 12, 2013).

175. Press Release, Fin. Servs. Roundtable, *supra* note 172.

176. *Id.*

H.R. 1731.[177] In general, both CISA and the House-passed bills limited the use of shared information to cybersecurity purposes.[178] However, the bills differed in respect to which entities are authorized to receive shared cyber threat information, and the proposed standard of how much personal information must be removed prior to sharing.[179]

Dissatisfied privacy and civil liberties advocates seemed to stand as the final hurdle in ending the deadlock on cyber legislation.[180] A failed amendment to CISA proposed by Senator Ron Wyden (D-OR), sought to impose more stringent requirements for private companies to remove sensitive customer information "to the extent feasible" before sharing cyber threat indicators.[181] If effectuated, this amendment would have ignited the very legal uncertainty that CISA aims to prevent because the qualifier "to the extent feasible" is entirely too subjective.[182] Use of this subjective language would have complicated and deterred information sharing because lawyers, security professionals, and others would have remained concerned over whether or not they have sufficiently removed information, thus frustrating the central purpose of the bill.[183]

---

177. Alexei Alexis, *Additional Hurdles Await Cybersecurity Legislation*, BLOOMBERG: TELECOM LAW REPORT (Oct. 28, 2015). The House bills were effectively merged by a House resolution. PCNA is Title I and NCPAA is Title II. H.R.J. Res. 212, 114th Cong. (2015).

178. Cybersecurity Information Sharing Act, S. 754, 114th Cong. §102(4) (2015). "The term 'cybersecurity purpose' means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability." *See also* H.R.J. Res. 212, 114th Cong. (2015).

179. *See* Alexis, *supra* note 177 ("A key difference is that the House legislation would allow companies to share data with multiple federal agencies, while the Senate version would establish a single portal at the Department of Homeland Security for the purposes of sharing information with the government.").

180. *Id.*

181. *See* Kaveh Waddell, *The 22 Amendments That Could Determine the Fate of the Senate's Cybersecurity Bill*, NAT'L J. (Aug. 26, 2015), http://www.nationaljournal.com/s/50094/cybersecurity-information-sharing-act-cisa-amendments.

182. *See id.* (quoting U.S. Chambers of Commerce senior director Matt Eggers in saying that the "more restrictive definitions of threats and indicators could be stumbling blocks for businesses that want to participate in the sharing program"; *but see* Greg Nojeim & Jadiza Butler, *Guide to Cybersecurity Information Sharing Act Amendments*, CTR. FOR DEMOCRACY & TECHN. BLOG, (Oct. 23, 2015), https://cdt.org/blog/guide-to-cybersecurity-information-sharing-act-amendments/ (arguing that "the amendment also provides an appropriate degree of flexibility for companies because it only requires them to remove unnecessary PII 'to the extent feasible'").

183. *See* Waddell, *supra* note 181 (quoting Eggers, "businesses are constantly on the lookout for vague or subjective language that eludes easy interpretation" and the "Wyden Amendment falls into that trap"); *see also* Letter from Kenneth E. Bentsen, President & CEO, Securities Industry and Financial Markets Association, Frank Keating, President & CEO,

Senators rejected the Wyden Amendment by a 41-55 margin.[184] One expert argued that the relatively close vote inferred that there could still be strong debate over the details of the bill in the reconciliation process.[185] However, less than two months later, a compromise bill was signed into law by President Obama that contained much of the original text of CISA, minus the problematic text identified by the Financial Services Roundtable, and effectively ended the cyber legislation stalemate.[186]

B. Cybersecurity Act of 2015

On December 18, 2015, the Cybersecurity Act of 2015 (the "Act") was signed into law by President Obama as part of a $1.1 trillion omnibus spending bill.[187] The Act establishes a voluntary framework for private entities and the federal government to share cyber threat indicators and defensive measures, and delineates the specific liability protections advocated for by the financial sector.[188] This framework differs from FS-ISAC in that it enables all industries to improve cybersecurity defenses and more quickly detect and mitigate threats across the nation.[189] Under the Act, if an FI gets hit by a cyber attack and immediately shares the threat information with the government, the government can then simultaneously distribute warnings to other private entities.[190] Private entities operating in other critical infrastructures, such

---

American Bankers Association, & Tim Pawlenty, President & CEO, Financial Services Roundtable, to Senate Leadership on CISA (Oct. 20, 2015), http://www.aba.com/Advocacy/LetterstoCongress/Documents/JointTradesLetterToSenateLeadershipCISA102015Final.pdf (advocating against the Wyden Amendment as it would create "unnecessarily restrictive roadblocks to timely and effective sharing about cyber threats").

184. Andy Greenberg & Yael Grauder, *CISA Security Bill Passes Senate With Privacy Flaws Unfixed*, WIRED (Oct. 27, 2015), http://www.wired.com/2015/10/cisa-cybersecurity-information-sharing-act-passes-senate-vote-with-privacy-flaws/.

185. *See id.* (quoting Robyn Greene, policy counsel for the Open Technology Institute at New America Foundation, who specializes in issues concerning surveillance and cybersecurity).

186. *See* Cybersecurity Act of 2015, H.R. 2029, 114th Cong. (2015) [hereinafter "Cybersecurity Act"]; *see also* CADWALADER, *supra* note 20.

187. CADWALADER, *supra* note 20.

188. ALSTON & BIRD, *supra* note 20, at 1–2; *see also* CADWALADER, *supra* note 20.

189. *See* Jose Pagliery, *Senate Overwhelmingly Passes Historic Cybersecurity Bill*, CNN MONEY (Oct. 30, 2015), http://money.cnn.com/2015/10/27/technology/cisa-cybersecurity-information-sharing-act/.

190. *Id.*

as energy and utility services, may learn how to defend themselves from a cyber attack that hit an FI, and vice versa, all within a matter of minutes.[191]

The Act maintained its very straightforward voluntary nature, as it lacks any official *mandate* on private entities to share threat data with the federal government.[192] Therefore, if private entities do not wish to participate, they are by no means required to.[193] And, even if they do participate, sharing information with a non-federal entity does not create a right or benefit to similar information by such non-federal entity in return.[194] The Act clarifies a number of critical aspects of the competing bills—namely, where in the government information sharing can occur, clear delineation of liability protections, and forthcoming guidelines on the standard by which personal information must be removed prior to sharing.[195] Section 102 of the Act provides definitions of recurring key terms such as: cyber threat indicator, defensive measure, cybersecurity purpose, and appropriate federal entities.[196]

1. Extent of Government Authorization to Receive and Disseminate Cyber Threat Information

The Act designates a single information portal[197] at DHS that authorizes an automatic forward of information to other "appropriate Federal entities"[198] *after* the required steps have been taken to scrub personal information from the data.[199] Prior to the passage of the Act, the White House Administration advocated utilization of a single portal for receiving and disseminating threat information because the associated

191. *See id.* ("Every cyber attack is like a flu virus, and CISA is intended to be a lightning-fast distribution system for the flu vaccine. Opt in, and you get a government shot in minutes, not months.").

192. Cybersecurity Act, § 108(i).

193. *See id.* (noting further that there is no liability for non-participation).

194. *Id.* § 104(f).

195. *See id.* §§ 102–106.

196. *Id.* at § 102.

197. *See infra* note 165. This information portal is the Integration Center made official by the National Cybersecurity Protection Act of 2014. *Id.*

198. Appropriate federal entities include the Departments of Commerce, Defense, Energy, Justice, and the Treasury, as well as the Office of the Director of National Intelligence. Cybersecurity Act § 102(3).

199. *See id.* § 103 (sharing of information by the federal government).

efficiencies will ensure real-time sharing.[200] Centralized sharing will enhance situational awareness and further facilitate robust privacy controls through active oversight of information sharing.[201]

The federal government is limited in its ability to disclose, retain, and use cybersecurity information acquired through the sharing portal.[202] The Act generally limits the use of shared information to a "cybersecurity purpose", which is defined as the "purpose of protecting information systems or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability."[203] Additionally, the Act exempts disclosure of shared information under the Freedom of Information Act.[204]

Cyber threat indicators and defensive measures may also be disclosed to, retained, or used by the federal government to identify a cybersecurity threat, including the source of such cybersecurity threat or a security vulnerability.[205] Information shared with the federal government under the Act may be used in certain other law enforcement investigations, but only in limited circumstances such as those that relate to preventing or mitigating *specific* threats of death, bodily harm, and serious economic harm.[206] Information relating to threats of death and bodily harm are relatively straightforward and will likely function as a very narrow, and easily definable exception category.[207] Specific threats of "economic harm" may be harder to categorize, and thus may operate as a more flexible exception.[208]

2. Privacy Concerns

The Act includes multiple layers of privacy protections that function to prevent inappropriate sharing of sensitive, personally

200. Alexis, *supra* note 177.

201. *Id.*

202. CADWALADER, *supra* note 20.

203. Cybersecurity Act §102(4).

204. *See id.* § 105(d); *see also* CADWALADER, *supra* note 20.

205. Cybersecurity Act § 105(d)(5).

206. *See id.* § 105(d)(5).

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

208. *See id.* ("The [economic harm category] seems to [be] more capacious and capable of 'expansion' but still a cabining of some sort.").

identifiable information.[209] First, the Act explicitly requires private entities to remove information that they "know[] at the time of sharing" to contain sensitive, personally identifiable information.[210] The Act's narrow definition of what constitutes a "cyber threat indicator" also provides a "key privacy protection in the Act because it creates an exhaustive list of the types of cyber threat information that can be shared."[211] Cyber threat indicators focus on the techniques and malware used by cybercriminals, rather than actual personal information contained in the affected network.[212] The narrow definition limits the sharing of sensitive customer information to the extent necessary to describe the threat.[213]

The duty to protect personal information from unauthorized use or disclosure through cyber threat information sharing is two-fold, as it applies equally to federal entities.[214] The federal government's duty to safeguard the privacy and civil liberties of persons whose information is shared under the Act extends beyond what is required by private entities.[215] The Act specifically requires the federal government to notify persons whose personal information is shared by a federal entity in violation of the Act.[216] Furthermore, the Act calls for sanctions to be developed and implemented against "officers, employees, or agents of a Federal entity who knowingly and willfully conduct activities under this title in an unauthorized manner."[217]

The Act calls for the Attorney General, and the Secretary of Homeland Security, in consultation with the heads of the appropriate federal entities, as well as other designated officers, to develop final guidelines relating to privacy and civil liberties.[218] The final guidelines will govern the receipt, retention, use, and dissemination of cyber threat

209. ALSTON & BIRD, *supra* note 20, at 3–4.

210. Cybersecurity Act § 104(d).

211. S. REP. NO. 114-32, at 3–4 (2015).

212. *Id.*

213. *Id.*

214. Cybersecurity Act § 105(d)(5)(c).

215. *See* ALSTON & BIRD, *supra* note 20, at 3 (noting the requirement for the government to "notify individuals whose personal information is shared by a federal entity in violation of the statute").

216. Cybersecurity Act § 103(b)(1)(F); ALSTON & BIRD, *supra* note 20, at 3.

217. Cybersecurity Act § 103(a)(3)(C).

218. Cybersecurity Act § 105(b). Interim guidelines will be released within 60 days of the Act, and the final guidelines will be available within 180 days. *Id.*

indications acquired by a federal entity under the Act.[219] Numerous requirements for the final guidelines are listed in the Act limiting the effect on privacy and civil liberties.[220] The final guidelines must also include a designated process for the destruction of any shared information that is known to not be directly related to cybersecurity purposes, and requires specific limitations on the length of any period in which a cyber threat indicator may be retained by a Federal entity.[221]

3. Liability Protections

The Act clearly defines liability protections for private entities who choose to share cyber threat information with one another or the federal government.[222] These protections seek to incentivize information sharing to improve cyber threat detection and shorten the lifespan of active threats.[223] However, the extent of this liability protection is very narrowly tailored, and must remain in accordance with the similar terms set forth by the Act.[224]

To qualify for liability protections under the Act, any information shared must be for cybersecurity purposes *only*.[225] Section 106 outlines such liability protections, establishing that "[n]o cause of action shall lie or be maintained in any court against any private entity" for the monitoring and sharing of cyber threat indicators or defensive measures authorized by Section 104.[226] Section 106(c) also reiterates the voluntary nature of the Act, clarifying that nothing in the Act shall be construed to "create a duty to share a cyber threat indicator or defensive measure; nor a duty to warn or act based on the receipt of a cyber threat indicator or defensive measure."[227] Further, the protection afforded by the Act does not include unauthorized monitoring or sharing, including gross negligence or willful misconduct that puts sensitive data at risk of being

219. *Id.* § 105(b)(2).
220. *See id.* § 105(b)(3).
221. *Id.* § 105(b)(3)(B).
222. *Id.* §106(b).
223. *See* S. REP. NO. 114-32, at 3 (2015); *see also* ALSTON & BIRD, *supra* note 20, at 1.
224. Cybersecurity Act, *supra* note 186, § 106(b)(1).
225. *Id.* § 106(b).
226. *Id.*
227. *Id.* § 106(c).

compromised.[228]

Although the Act provides clear liability protections to private entities who wish to share cyber threat information, such entities are still encouraged to consult their legal counsel.[229] The Act was broadly drafted to authorize sharing of information "notwithstanding any other provision of law" for cybersecurity purposes that are consistent with the protection of classified information.[230] However, entities must still share information in accordance with the forthcoming guidelines that will govern the receipt, retention, use and dissemination of cyber threat information.[231] The Act's provisions will be reconciled with other laws and regulations that govern the access and use of sensitive personal information.[232] Although there is no clear answer to how the Act will interact with existing laws, the Act's exception to antitrust liability may serve as a useful lens to examine other similar concerns.

In the past, antitrust issues may have functioned as a deterrent for institutions to share technical cyber threat information with others in the industry.[233] Institutions feared that sharing cyber threat information with others in the industry would subject them to liability under anti-trust laws that seek to limit information sharing among competitors for other purposes.[234] The Act codified an earlier premise set forth in a joint statement released by the Department of Justice's Antitrust Division and the Federal Trade Commission in April of 2014, which made it quite clear they do not believe that antitrust issues should be a roadblock to legitimate cybersecurity information sharing.[235] The Agencies differentiated cyber threat information from sensitive information that relates to any particular business' plans or pricing information.[236] The Act clearly limits the scope of liability protection offered to private entities that share information with one another to *cybersecurity purposes*

228. *See id.*; *see also* S. REP. NO. 114-32 at 3.

229. CADWALADER, *supra* note 20.

230. Cybersecurity Act § 104(c)(1).

231. *Id.* § 105(b).

232. CADWALADER, *supra* note 20.

233. *See* DEP'T OF JUSTICE AND FED. TRADE COMM., ANTITRUST POLICY STATEMENT ON SHARING OF CYBERSECURITY INFORMATION 1, 5 (Apr. 10, 2014), https://www.ftc.gov/system/files/documents/public_statements/297681/140410ftcdojcyberthreatstmt.pdf; *see also* WEISS, *supra* note 145, at 4.

234. *See* WEISS, *supra* note 145, at 4.

235. *See* DEP'T OF JUSTICE AND FED. TRADE COMM., *supra* note 233, at 1–2.

236. *See id*. at 1–4.

only.[237] Thus, the antitrust exemption does not seek to protect private entities from "engaging in anti-competitive behavior under the guise of cybersecurity."[238]

C. Remaining Concerns

The mixed response to the passage of the Act mirrors the controversy that contributed to the lengthy stalemate in cybersecurity legislation.[239] The debate boils down to striking a mutually satisfying balance between the two competing interests any private entity faces in dealing with cybersecurity—protecting privacy and civil liberties, versus protecting business interests that may be compromised by a successful cyber attack.[240] Opponents of the Act believe customer privacy and civil liberties are compromised by the proposed information sharing authorization standard, and that the legislation essentially functions as a surveillance bill.[241] Privacy advocates such as Senator Ron Wyden (D-OR) have publicly denounced the Act, stating that it is extremely flawed and "would 'seriously threaten privacy and civil liberties, and could undermine cybersecurity, rather than enhance it.'"[242] A handful of lawmakers voted against the omnibus spending bill, solely because it included the Cybersecurity Act.[243]

Those in favor of the Act believe privacy protections are sufficiently addressed, and any deficiencies may only be realized through utilization of the processes authorized by Act.[244] Furthermore, the Act is a much needed step in the direction of successful cybersecurity defense

---

237. *See* Cybersecurity Act § 104(e).

238. *See id.*; *see also* S. REP. NO. 114-32 8 (2015).

239. *See* Cory Bennett, *Lawmakers to Oppose Spending Bill Over Cyber Language*, THE HILL (Dec. 16, 2015, 7:04 PM), http://thehill.com/policy/cybersecurity/263537-cyber-bill-spurs-several-no-votes-on-omnibus (discussing the debate over adequately addressing privacy concerns).

240. *See* Petrasic, *supra* note 29; *see also* Waddell, *supra* note 181.

241. *See* Everett Rosenfeld, *The Controversial "Surveillance" Act Obama Just Signed*, CBNC (Dec. 22, 2015, 12:34 PM), http://www.cnbc.com/2015/12/22/the-controversial-surveillance-act-obama-just-signed.html.

242. *Id.*

243. Bennett, *supra* note 239; *see also* Rosenfeld, *supra* note 241 (quoting California Rep. Zoe Lofgren and Senator Wyden voting against the bill because it functions as a surveillance tool).

244. *See* Greenberg & Grauder, *supra* note 184 (quoting Senate Intelligence Committee Chair, Richard Burr (R-NC)).

and threat mitigation for FIs and the nation as a whole.[245] Senator Diane Feinstein (D-CA) referred to the Act as "an important first step to address a significant drain on our economy and threat to our national security."[246] The Act was designed to combat perceived barriers to collaboration in cyber-warfare, and accordingly incentivize, but not require, information sharing among the private sector and government.[247]

Aside from the privacy debate, some have raised concerns over the quiet means by which the Act was inaugurated.[248] Open Technology Institutes policy counsel, Robyn Greene referred to the Act's place in the federal budget as "pulling a second Patriot Act," given that this bill has been "kicked around for years and ha[s] been too controversial to pass, so they've seen an opportunity to push it through without debate."[249]

The actual degree to which the Act increases information sharing and aids in threat mitigation remains to be seen.[250] Section 207 of the Act requires the Comptroller General of the United States to submit an assessment of the implementation of the Act, and to a reasonable extent, any findings regarding increases in the sharing of cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents at the Integration Center.[251] The Comptroller's assessment is due within two years after the date of the enactment of the Act.[252] In the meantime, private entities should recognize that although critical to threat mitigation, information sharing is only one of many facets of cybersecurity.[253] Various unilateral measures are still necessary to take and maintain in order to develop an effective cybersecurity defense program.[254]

---

245. Rosenfeld, *supra* note 241.

246. Brandom, *supra* note 21; *see also* Rosenfeld, *supra* note 241 (quoting U.S. Chamber of Commerce President and CEO, Thomas Donahue, saying that the Act is "our best chance yet to help address this economic and national security priority in a meaningful way and help prevent future attacks").

247. CADWALADER, *supra* note 20.

248. *See* Rosenfeld, *supra* note 241 (referring to the Act as a "second Patriot Act").

249. Andy Greenberg, *Congress Slips CISA Into a Budget Bill That's Sure to Pass*, WIRED (Dec. 16, 2015, 12:24 PM).

250. FISCHER & LOGAN, *supra* note 66, at 4.

251. Cybersecurity Act § 207.

252. *Id.*

253. *See* Susan Hennessey, *The Problems CISA Solves: ECPA Reform in Disguise*, LAWFARE (Dec. 23, 2015), https://www.lawfareblog.com/problems-cisa-solves-ecpa-reform-disguise.

254. *See id.* ("Effective cybersecurity includes network monitoring, scanning, and deep-

V. CONCLUSION

In light of the pervasive threat of increasingly sophisticated cyber attacks, FIs must continuously revamp, maintain, and adapt their cybersecurity infrastructures.[255] Modern cybersecurity defense requires FIs to focus *less* on network security and *more* on the data.[256] This focus necessitates a better, more collaborative relationship between FIs and the government.[257] The benefits of information sharing are quite clear, and any increase in such sharing is likely to have more positive effects on threat mitigation than negative implications feared by privacy advocates.[258] Sharing cyber threat information enables the government to analyze trends and data in a comprehensive cyber threat information database, which puts both the private sector and the federal government in a better position to mitigate and defend against cyber attacks.[259] However, information sharing is most relevant to imminent threats rather than broader issues in cybersecurity that may be addressed through individually tailored cybersecurity programs.[260] FIs must continue to spend time, money, and resources to address the growing threat of cyber attacks on an institutional basis alongside any efforts to contribute to the collaborative information sharing initiative.[261]

The famous words, "united we stand, divided we fall" ring as true in cyber warfare as they did in the Revolutionary War.[262] The critical

---

packet inspection. . . [which] includes contents of communications in order to detect malicious activity. Federal and state laws create major impediments to that activity. [The Act] is designed to begin fixing this.").

255. *See* Press Release, U.S. Dep't of Treasury, *supra* note 33 ("Given the sheer number and continual morphing of assaults . . . we have to increasingly focus our efforts on making response and recovery more efficient, effective, and predictable.").

256. *See* Clancy, *supra* note 69 (noting that as information sharing and analysis increases, "the process of detection and mitigation will become more efficient and the balance of power will shift away from the criminals").

257. *See* Germano, *supra* note 16, at 2 ("Accordingly, because significant access, expertise, and perspective needed to address the cyberthreat reside in both the private and public sectors, . . . collaboration is essential to attain feasible and effective cybersecurity solutions.").

258. *See* Rosenfeld, *supra* note 241.

259. V. Gerard Comizio, *Information Sharing is Key to Avoid a Cyber* Attack, TECH CRUNCH (Nov. 15, 2015), http://techcrunch.com/2015/11/15/information-sharing-is-key-to-avoiding-a-cyberattack/#.

260. *See id; see also* FISCHER & LOGAN, *supra* note 66, at 4.

261. *See* FISCHER & LOGAN, *supra* note 66, at 4.

262. History of the Motto, Smithsonian National Museum of American History, http://amhistory.si.edu/1942/campaign/campaign24.html (last visited Feb. 17,

infrastructures of the United States are more technologically integrated than ever before, which amplifies the potential for cyber attacks.[263] Therefore, to lessen the vulnerability of such infrastructures, FIs must take measures to protect their own networks, and aid in the mitigation of threats to others through collaborative information sharing.[264]

ARIANA L. JOHNSON

2016). In 1768, founding father John Dickinson coined this patriotic motto in the Liberty Song that encompassed collaboration as a central theme.

263. Comizio, *supra* note 259; *see also* White House Office of the Press Secretary, *supra* note 21.

264. Comizio, *supra* note 259; *see also* Hennessey, *supra* note 253 ("[The Act] comes at a cybersecurity crisis point. The principal solutions to the crisis all require that private industry do more to protect the personal data in its possession and under its control.").