CHAPTER 3

The Evolution of Cybersecurity within the American Financial Sector

The American Financial Sector: Tempting Targets for CyberAttackers

Intuitively, banks and other key financial institutions are quite often major targets of cybercriminals, via cyberattacks, across the globe. Generally speaking, financial institutions are tempting target because, quite simply, this is where the money is kept. However, the collective impact of U.S. banking institutions extends well beyond the mere management of monetary currency inventories. Networked banking systems enable billions of financial e-transactions and monetary transfers, loans, and payments every day through a vast array of financial services networks.

Collectively speaking, America's financial institutions form the backbone of the global financial system—which is heavily reliant on information technology (IT) systems. These financial IT systems orchestrate virtually every aspect of financial operations—from executing billions of dollars in daily transactions to generating financial audit reports to managing consumer services. Because of the criticality of these operations, the integrity and security of the financial data contained on these IT systems is paramount. To maintain this essential data security, highly robust and resilient IT systems and well-maintained/secured networks are required. So long as the financial sector's institutional financial data and its supporting infrastructure remains both secure and operational from cyberattacks, this only strengthens and reenforces the global financial

P.-L. Pomerleau and D. L. Lowery, *Countering Cyber Threats to Financial Institutions*,
https://doi.org/10.1007/978-3-030-54054-8_3

system as a whole (Zheng & Carter, 2015). As the Center for Strategic and International Studies (2020) explains, for the would-be cybercriminals, banking institutions offer "multiple avenues for profit through extortion, theft, and fraud," (p. 1) while sovereign nation-state actors and hacktivists also intentionally "target the financial sector for political and ideological leverage" (p. 1).

The American Economy: A Major Element of National Security

Because American financial institutions play such an out-sized and critical role in the world's overarching Global Financial System, the U.S. economy makes an extremely tempting target—and can therefore be vulnerable to nefarious cyber-related economic/financial-related criminal activities. However, keep in mind that threats to America's economy are not just solely limited to would-be cybercriminals seeking financial e-commerce-related treasure. The key elements of the U.S. economy—including both the financial sector and key infrastructure components—can also be susceptible to a variety of offensive cyberspace operations by any number of America's nation-state competitors. Non-state national security-related actors, such as terrorist organizations, could also seek to do the United States harm (Borghard, 2018).

Borghard (2018) effectively illustrates her point by pointing to public congressional testimony on February 13, 2018 to a Congressional committee by the directors of National Intelligence, the National Security Agency, the Central Intelligence Agency, and the Federal Bureau of Investigation all warned that cyberattacks perpetrated by foreign adversaries as being one of the most significant concerns to national security. In his opening remarks, the Director of National Intelligence, former U.S. Senator Dan Coats, bluntly told his former congressional colleagues that America is "under attack" by "entities using cyber to penetrate virtually every major action that takes place in the United States" (p. 1). Coats also added there many federal agencies involved in preventing further cyberattacks from happening against the United States with significant support nowadays also coming from the private sector. "We can't as a government direct them what to do" stated Coates, "but we're spending every effort to work with them to provide answers" (CBS News, 2018, p. 1). By sharing real-time risk assessment and warnings about potential newly emerging cybersecurity threats across the American financial sector, both the federal government and individual financial institutions ensure a higher degree of cybersecurity situational awareness and collective mitigation posturing.

The Evolution of Cybersecurity within America's Financial Sector

Early Federal Legislation (1970–1991)

According to Zheng and Carter (2015), the early foundations of IT-related security requirements for America's financial sector began in October 1970 with the passage of the *Bank Secrecy Act* (BSA) and, later, in December 1991 with the subsequent passage of the *Federal Deposit Insurance Corporation Improvement Act* (FDICIA). These two early federal laws largely focused on the monitoring and operational assurance of financial transactions by requiring financial institutions to ensure the data and physical security of their individual information systems. This was seen as a necessary industry-wide standard in order to ensure the fundamental integrity of each individual financial transaction, customer account identification, and to provide an avenue for identifying suspicious or fraudulent financial transactions.

Because the BSA was originally signed into federal law decades before the modern internet took shape, it should be noted the contemporary term of "cybersecurity" was not used in the original statutory verbiage. Despite this omission, the core concepts of contemporary cybersecurity are still plainly articulated as industry-wide compliance requirements. This includes the requirements to (a) maintain strict physical and data security of the individual financial systems, (b) log customer information, and (c) analyze account transactions for suspicious activity. The BSA also mandated American financial institutions report suspicious financial activities to a nation-wide Financial Crimes Enforcement Network (Zheng & Carter, 2015; Federal Financial Institutions Examination Council, 2014).

Twenty-one years later, in December 1991 the U.S. Congress passed the FDICIA as a modernization amendment to the September 1950 Federal Deposit Insurance Act (FDIA). This legislation required the establishment of "operational and managerial standards" relating to "internal controls, information systems, and internal audit systems" (Cornell University Legal Information Institute, 2020, ii. Section 39a).

Four years later, a subsequent requirement was added for American financial depository institutions to have adequate internal controls and IT-related capabilities that were appropriated-sized based on the nature and scope of the institution's financial activities (Zheng & Carter, 2015).

Consumer Protection During the Infancy of e-Commerce (1999–2003)

The next three major American legislative advancements in the realm of evolving cybersecurity threats came about with the *Gramm-Leach-Bliley Act* (GLBA) in November 1999, the *Sarbanes-Oxley Act* (SOX) in July 2002, and the *Fair and Accurate Credit Transactions Act* (FACTA) in December 2003. All three of these pieces of federal legislation came about at a time when online banking was still a relatively new concept in its technical infancy, but was rapidly expanding nation-wide. Collectively, these three pieces of federal legislation sought to ensure a variety of personal consumer and financial data-related protections by mandating a variety of IT system-related security enhancements that we now know as cybersecurity-related activities today.

Signed into law in late 1999, the GLBA codified personal data security requirements as a way to protect American consumers by guarding against unauthorized disclosures of personal consumer data through a robust series of data safeguards that included multilayer accessibility of IT data systems, the monitoring of network activity, appropriately responding to suspicious activities/policy violations, and implement measures to detect/prevent malicious code (Federal Financial Institutions Examination Council IT Examination Handbook, n.d.). As a result, at least in part, of the national headline-grabbing financial accounting scandal of Enron financial accounting scandal in late 2001, the U.S. Congress passed the SOX in the summer of 2002. The SOX mandated the use of accurate audit and regulatory reporting systems, which drove financial institutions to conduct annual security assessments of their own IT security systems and internal data (Stults, 2004).

Congress passed the Fair and Accurate Credit Transactions Act (FACTA) in December 2003 as a way to prevent a surging problem not only within America's e-commerce sector, but world-wide: consumer identity theft. Extending well beyond America's traditional banking institutions, this law also required any American business entity considered a "creditor" to adhere to strict protocols to providing, acquiring, or sharing credit reports/histories of individual American consumers (Federal Trade Commission, 2013). The FACTA also drove specific IT compliance requirements to identify suspicious activities, possible data breaches, and a legal requirement to notify U.S. consumers of situations where their personal data may have been compromised (Zheng & Carter, 2015).

The Payment Card Industry Data Security Standard (2004)

In December 2004, the big five global credit card companies—American Express, Discover, MasterCard, Visa, and JCB International—collectively used their dominant positions in both the American and worldwide marketplaces to proactively establish a new industry-wide financial credit security standard known as the Payment Card Industry Data Security Standard (PCI-DSS) (Zheng & Carter, 2015; Williams, Chuvakin, & Bradley, 2007). Unlike the prior legislatively mandated actions taken by the U.S. Federal Government, this is a key example of the industry leaders within the American Financial Sector proactively huddling together and effectively driving the establishment of a new common data security standard across their respective market sector. Generally speaking, PCI-DSS drove strong data security enhancement measures, which included the establishment of six core system control objectives and fourteen software protection features, to govern the processing of credit card financial transactions in real-time (PCI Security Standards Council, 2020).

Executive Order 13636 (2013) and the Implication to "Section 9" Firms

On February 12, 2013, then-U.S. President Barack Obama signed *Executive Order #13536: Improving Critical Infrastructure Cybersecurity*, which enabled the Federal Government to prioritize its efforts to assist our America's most critical infrastructure entities. Identified as "Section 9" entities, the executive order defined these entities as "critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economy security, or national security" (Obama, 2013, pp. 1–2). Generally speaking, Section 9 entities perform critical functions within the U.S. economy, but are reliant on the operational security and resiliency of America's existing cyber infrastructure to perform those functions (Krebs, 2019).

By prioritizing federal funding and services support to Section 9 entities within the American Economy, which includes the U.S. Financial Sector, it is considered an effective and efficient way to mitigate national risk overall. *Executive Order #13636* also designated the U.S. Department of Homeland Security (DHS) as the executive agent to implement this order, thereby giving DHS a central orchestrating role in directly supporting a wide array of voluntary Section 9 cybersecurity risk management efforts "by offering programs, sharing information, and providing technical assistance to help organizations reduce their individual risk" (Krebs, 2019, p. ii).

One of the major deliverables that came about as a direct result of this executive order was the establishment of the National Risk Management Center (National Risk Management Center, 2018), which launched in the fall of 2018. The NRMC works in close coordination with the Section 9 entities, other key private sector organizations, and major stakeholders in the critical infrastructure community to:

> Identify, analyze, prioritize, and manage the most strategic risks to our National Critical Functions — the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on security, national economic security, national public health or safety, or any combination. (National Risk Management Center, 2018, p. 1)

One of the key primary functions of the NRMC is known as the "Pipeline Cybersecurity Initiative," which collaboratively works directly with pipeline asset owners and operators to include an in-depth review and evaluation of the control system's network design, configuration, and interdependencies (National Risk Management Center, 2018, p. 1).

An illustrative example of this federal-private partnership focused on joint resiliency collaboration began in October 2018, when DHS kicked off a long-term active partnership with America's Oil & Natural Gas Sector to manage long-term risk in this critical infrastructure sector. As DHS Undersecretary Christopher Krebs explained the "NRMC is DHS's effort to secure tomorrow's infrastructure, providing a central point of entry for working with industry to manage long-term strategy risk across our critical infrastructure sectors" before adding this collaborative effort is a:

> Key milestone in the partnership between the federal government and the oil and natural gas industry, as we launched the pipeline cybersecurity initiative that partners DHS' NPPD [National Protections and Programs Directorate] cybersecurity resources, DOE's [Department of Energy] expertise, with TSA's [Transportation Security Administration] regular and ongoing assessments of pipeline security to get a broader understanding of the risks the sector faces. Collaborative efforts like this allow us to better understand the threat landscape and direct more targeted and prioritized risk management activities. (Department of Homeland Security, 2018, pp. 1–2)

Assistant U.S. Energy Secretary for Electricity Bruce Walker explained "boosting public and private investments to improve the country's critical energy infrastructure and technology is paramount to ensuring a reliable and resilient electric grid" (Randolph, 2018, p. 1). Walker added that since the Department of Energy was the lead federal interface with the American Energy Sector, "we are prioritizing work with our federal partners, the oil and gas industry, and the electric industry to incentivize these crucial and necessary investments" (Randolph, 2018, p. 1).

The Roll-Out of the NIST Cybersecurity Framework (2014–2018)

The American-based National Institute of Standards and Technology (NIST) is a U.S. Department of Commerce physical sciences laboratory chartered to promote technical innovation and industrial competitiveness. Originally established as the "National Bureau of Standards" by an act of the U.S. Congress in 1901, this Gaithersburg, Maryland-based organization was tasked with boosting the American Economy's then-lagging Industrial Sector. The organization was ultimately credited to assist the sector effectively compete globally with the United Kingdom, Germany, and other international economic rivals of the day. Today, NIST's activities include a wide array of technology-related research endeavors and serves as a technical authority on the establishment and maintenance of technical standards in the fields of cybersecurity/information technology, engineering, and nanoscale technologies (National Institute of Standards and Technology, 2018a).

One of the NIST's key technological standardization frameworks is the NIST Cybersecurity Framework, officially known as "*Framework for Improving Critical Infrastructure Cybersecurity.*" The original version of the NIST Framework, commonly referred to as "Version 1" was released in February 2014 and was subsequently superseded by an updated "Version 1.1" in April 2018. This framework serves as a set of detailed guidelines and industry best practices as a way to assist governmental and private organizations alike with effectively reducing and mitigating potential cybersecurity risks. Originally designed to be versatile, the framework was constructed around the fundamental premise that recommended guidelines, standards, policies, procedures, and protocols can only be effective if implemented across the organization as a whole—not just by the organization's internal IT department (National Institute of Standards and Technology, 2018b).

As a functional construct, the NIST Cybersecurity Framework is transportable between various industries and is intended to facilitate active, cyber hygiene awareness, and cybersecurity-minded communications organization-wide. Delving a bit deeper into the NIST Cybersecurity Framework, it can serve as a foundational baseline for an organization's cybersecurity policies or enhance existing policies and procedures. Central to this framework are five core continuous functions: to *Identify, Protect, Detect, Respond*, and *Recover.* Collectively, these five distinct operational pillars form the essential components of a holistic cybersecurity program that revolve around the three basic types of cyber threats: *perimeter threats* (i.e., firewalls and anti-virus protection), *intranet threats* (i.e., portable data devices and network protection), and *human security* (i.e., poor cyber hygiene practices and potential insider threats) (National Institute of Standards and Technology, 2018a).

It should be noted that collectively speaking, the third element of the cyber threat "triad" poses the most significant vulnerabilities—the human cybersecurity risks—for a multitude of potential reasons. Whether due to unintended human error, deliberate covert actions (i.e., unauthorized disclosure of sensitive information), or concerted technical modifications of existing cybersecurity-related IT system functions, unauthorized changes, activated email-embedded phishing hyperlinks, or inadvertent HTML-enabled system loaded malware, any of these actions can negatively impact a major IT system or network through a significant decrease in system-level functionality and data security (National Institute of Standards and Technology, 2018a). Additionally, beyond the NIST Cybersecurity Framework, NIST also provides *NIST Special Publication 800-30*, an overarching cyber risk assessment framework for conducting risk assessments of individual organizational-level networks based on federal information systems assessment standards (National Institute of Standards and Technology, 2012).

DoD Cyber Strategy (2015) and Presidential Policy Directive 41 (2016)

In April 2015, the U.S. Department of Defense (DOD) formally laid out its own *DoD Cyber Strategy* (2015) for defending the national security interests of the United States within the cyberspace domain. Rather than continuing to focus on risk mitigation-centered data sharing, this new framework focused on three core strategic goals for its cyber mission is to "defend the nation against cyberattacks of significant consequence" (p. 3) (Department of Defense, 2015). Extending well beyond its own heavily firewalled military networks, this new DoD strategy called for collaborative cyber-centric partnerships with the private sector in order to facilitate intelligence gathering and cyber-threat warning capabilities. Within the DoD, the Cyber National Mission Force was established with the responsibility of serving as the departmental focal-point for the major public–private partnership efforts necessary to adequately defend America's critical infrastructures in cyberspace (Borghard, 2018).

Just over a year later, in July 2016, *Presidential Policy Directive-41* (PPD-41) laid out the principle actors for a major federal response to cyber-related incidents occurring either in the public or private sectors. It is important to note this directive stressed an overall unity of effort between the two distinct sectors in order to ensure the overarching strategic importance of providing proper security and resiliency for America's critical infrastructures. PPD-41 succinctly stated, "the private sector and government agencies have a shared vital interest in protecting the Nation from malicious cyber activity and managing cyber incidents and their consequences" (Obama, 2016, p. 1).

America's National Cyber Strategy (2018)

On September 20, 2018, the White House released U.S. President Donald J. Trump's newly signed *National Cyber Strategy of the United States of America* (2018). In a formal statement, President Trump said the United States "cannot ignore the costs of malicious cyber activity — economic or otherwise — directed at America's Government, businesses, and private individuals" (White House, 2018, p. 1). In his own White House Press Conference following the release of the new American Cyber Strategy, U.S. National Security Advisor John Bolton remarked "we will identify, counter, disrupt, degrade, and deter behavior in cyberspace that is destabilizing and contrary to national interests, while preserving the United States' overmatch in and through cyberspace" (Lyngaas, 2018, p. 1).

Overall, this new national-level American cybersecurity strategy made several major enhancements that gave governmental agencies and their law enforcement organizations greater operational abilities to aggressively respond to cybercrime and nation-state attacks. This strategy specifically spotlighted DHS' active cultivation of domestic cyber defense roles. It also highlighted enhanced international offensive cyber stances authorized for the U.S. DoD to take—allowing the DoD to respond more quickly and proactively in response to international cyberattacks (Trump, 2018).

America's new national cyber strategy also succinctly outlined four "pillars of priority" which included: (1) protect the American People, the [American] Homeland, and the American Way of Life, (2) Promote American Prosperity, (3) Preserve Peace through Strength, and (4) Advance American Influence [through building international cyber-capacities with U.S. international allies to go after "threats of mutual interest"] (Trump, 2018). Furthermore, this new cyber strategy also made one central message crystal clear: America will not sit ideally by and watch when attacked in cyberspace (Trump, 2018). Several core "Section 9" areas were also included on a list of areas/functions where the United States would respond offensively within cyberspace—ranging from the protection of critical infrastructural and intellectual property to space exploration (Trump, 2018). Additionally, this strategy also added upon many foundational/apolitical policies of the two previous presidential administrations [of former U.S. Presidents George W. Bush (2001–2009) and Barack Obama (2009–2017)] in areas such as enhancing America's cybersecurity workforce and strengthening critical infrastructure. This included the U.S. Financial Sector and the operation of America's electrical grids—components that literally impact the lives of every single American (Arampatzis, 2018).

The U.S. Financial Sector's Militarized Approach to Fighting Cybercrime (2018–Present)

By the fall of 2018, armed with a new national-level cyber strategy, significantly enhance cooperation/collaboration with both DHS/DoD, and formal U.S. Treasury Department guidance declaring ongoing cyberattacks to be one of the greatest risks to the country's financial sector, American financial institutions have responded to calls to increase their own internal cybersecurity mitigation efforts with an increasingly militarized approach. According to Cowley (2018), "former government cyber-spies, soldiers, and counterintelligence officials now dominate the top ranks of [American] banks' security teams. They've brought to their new jobs the tools and techniques used for national defense: combat exercises, intelligence hubs modeled on those used in counterterrorism work and threat analysts who monitor the internet's shadowy corners" (pp. 2–3).

Within the American Financial Sector, major U.S. financial institutions have actively recruited some of the best and brightest cybersecurity professionals from across the industry over the past decade to help secure and maintain their own financial networks and data systems. Due to a sizeable number of these highly-skilled cybersecurity professional recruits hailing from U.S. military-trained cyberspace/network defense backgrounds, a variety of operational network security-centric military-styled tactics, techniques, and procedures (TTPs) were also translated into the civilian sector. As these prior-military cybersecurity professionals integrated into their new civilian institutions and actively leveraging their own technical skill sets, new functional coordination entities known as "corporate fusion centers"—the civilian equivalent of a military operational command center—quickly began to dominate the financial sector's cybersecurity rapidly expanding landscape.

In tandem with the rise of financial institutional fusion centers also came the establishment of the Financial Services Information Sharing and Analysis Center (FS-ISAC). An American-based financial industry-wide consortium, FS-ISAC was created in 1999 and the organization is dedicated to reduce cyber-risk in the global financial system and connects over

7000 member financial institutions—banks, brokerages, credit unions, financial trade associations, insurance companies, investment firms, bank service providers, and payment processors—spanning 70 jurisdictions (FS-ISAC, 2018; Sedenberg & Dempsey, 2018). In 2017, FS-ISAC expanded its operational reach by establishing international regional hubs in London and Singapore as well (Financial Services Information Sharing and Analysis Center, 2018).

By leveraging its collaboration-based peer-to-peer intelligence data-sharing platform, resiliency resources, and cybersecurity experts, FS-ISAC actively seeks to anticipate, identify, and effectively mitigate emerging cyber-based threats against its vast financial network. Because a cyber-attack against one of FS-ISAC's member financial institution could affect the entire U.S. Financial Sector or even the global-level financial system, these cyber-partnerships consolidate key cyber-defense expertise, early warning and detection, and share rapid response mitigation strategies (Financial Services Information Sharing and Analysis Center, 2018).

Within this trusted peer-to-peer consortium of financial institutional fusion centers, the name of the game is the continued real-time sharing of situational awareness and identification of emerging cyber-threats. With a concerted focus that is "to the left of the boom"—a military term referring to the critical moments just before a bomb detonates—the name of the game in these military-styled civilian financial cyber-fusion centers is the proactive detection and rapid mitigation of technical vulnerabilities/cyber-hacks before they can occur (Cowley, 2018). Through the sharing and collaboration of evolving cybersecurity-related mitigation strategies, cyber-related policies, and deterrence initiatives, the overall cybersecurity of the entire network is collectively enhanced.

Looking Ahead: Layered Cyber Deterrence

Authorized as part of the Fiscal Year 2019 National Defense Authorization Act, the Cyberspace Solarium Commission (CSC) (2020) was tasked to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyberattacks of significant consequences" (p. 1). The CSC's finished report was released to the public on March 11, 2020. This newly released strategy called for a future end-state of multilayered cyber-deterrence posturing, which the CSC viewed as necessary in order to reduce the overall impacts of future cyberattacks.

The CSC's (2020) public report outlined three ways to achieve a layered cyber deterrence posture though (a) the promotion of responsible international cyber behavior, (b) the denial of benefits to cyber-adversaries who have historically exploited the cyberspace domain to their advantage through increased cybersecurity and resiliency of the cyber-ecosystem, and (c) impose significant retaliatory costs to those who target America's national security interests through cyberspace. According to Homeland Security Today (2020), each of the three layered deterrent postures is dependent on continued (and further enhanced) American public/private sector cybersecurity collaborative partnerships to strategically alter how potential cyber adversaries (competitor nation-states and cybercriminal groups) fundamentally perceive the costs and benefits of leveraging the cyberspace domain to strike at American national security and economic interests around the globe.

The CSC's (2020) public report also outlined more than 80 key recommendations organized into six distinct pillars of: (a) reform the U.S. Federal Government's current cyberspace organizational structures, (b) continue to strengthen worldwide cyberspace norms among allies/partners and other nation-states, (c) continue to further enhance the country's national resiliency efforts, (d) seek to positively reshape the contours of the worldwide "Cyber Ecosystem" (p. 1), (e) continue to integrate operational cyber collaboration efforts between the U.S. Government and private sectors, and (f) further enhance America's "military instrument of National Power" (p. 1) to be employed with overwhelming effectiveness when called upon to do so.

According to Homeland Security Today (2020), these six pillars represent both the strategic and technical means by which the United States can proactively implement a layered cyber deterrence moving forward. While deterrence-backed-with-overwhelming-military-force has been the long-standing, core American national security strategy for close to a century, two key factors make this new multilayered cyber deterrence approach unique. First, this construct readily focuses on a strong, standing, and ever-resilient cybersecurity force comprised of the best and brightest cybersecurity professionals (from both the public and private sectors) partnered together for mutual cyber defense. Through constant collaboration, cyber vulnerabilities can be dramatically reduced—thus preventing cyberattackers from having opportunities to attack American interests in the cyber realm. Secondly, this new multilayered strategy seeks to "defend forward" as a pathway to significantly reduce both the severity and frequency of cyberattacks that would not generally rise to a conventional military response. The basic premise of defending forward centers around the identification of strategic centers of gravity or leverage points may need to be proactively countered/neutralized by actions that are (a) short of armed conflict and (b) consistent with international law, but still provide an appropriately measured government response from the United States (Homeland Security Today 2020).

Conclusion

As we strive to look ahead across today's cyber "lay of the land" and attempt to ascertain what future challenges might arise just over the horizon, a few core going-in assumptions remain quite clear. First, cyber-related technologies, opportunities, challenges, and threats are all-but-certain to continue to evolve at a rapid pace. Second, just as contemporary American society continues to become ever more dependent on modern infrastructures and technologies in virtually all aspects of our daily lives, so too must the physical/technical/cyber-based defensive security and overall resiliency of those critical infrastructures/technologies be continually enhanced.

Many of tomorrow's cyberspace and critical infrastructure enhancements will be readily made through continued (and further expanded) public/private sector partnerships. Specifically looking at the American Financial Sector and its associated cyber-connected infrastructure, the more the U.S. Federal Government understands the key vulnerabilities, challenges, and opportunities of the private financial sector's infrastructure, the more fidelity can be achieved against mitigating specific risks or vulnerabilities against those infrastructures. With greater and more frequent collaboration, joint partnerships and interoperable training/exercises/real-world response activities become more routine—thus, allowing all public and private sector stakeholders to be better prepared when future cyberattacks do take place.

References

Arampatzis, A. (2018). U.S. national cyber strategy: What you need to know. *Tripwire.com*. Retrieved from https://www.tripwire.com/state-of-security/government/us-cyber-strategy/.

Borghard, D. E. (2018). *Protecting financial institutions against cyber threats: A national security issue*. The Carnegie Endowment for International Peace. Retrieved from https://carnegieendowment.org/2018/09/24/protecting-financial-institutions-against-cyber-threats-national-security-issue-pub-77324.

CBS News. (2018). *Intelligence officials say U.S. "under attack," cybersecurity at-risk in 2018*. Retrieved from https://www.cbsnews.com/news/christopher-wray-mike-pompeo-dan-coats-testify-on-worldwide-threats-live-stream/.

Center for Strategic and International Studies. (2020). *The evolution of cybersecurity requirements for the U.S. financial industry*. Washington, DC: CSIS. Retrieved from https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/financial-sector-cybersecurity.

Cornell University Legal Information Institute. (2020). *12 CFR part 30, appendix A to part 30—Interagency guidelines establishing standards for safety and soundness*. Retrieved from https://www.law.cornell.edu/cfr/text/12/appendix-A_to_part_30.

Cowley, S. (2018). Banks adopt military-style tactics to fight cybercrime. *The New York Times*. Retrieved from https://www.nytimes.com/2018/05/20/business/banks-cyber-security-military.html.

Cyberspace Solarium Commission. (2020). *The United States of America cyberspace solarium commission*. Retrieved from https://www.solarium.gov/.

Department of Defense. (2015). *The Department of Defense cyber strategy*. Retrieved from https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf.

Department of Homeland Security. (2018). *DHS and DOE meet with oil and natural gas sector coordinating council, announce pipeline cybersecurity initiative*. Retrieved from https://www.dhs.gov/news/2018/10/03/dhs-and-doe-meet-oil-and-natural-gas-sector-coordinating-council-announce-pipeline.

Federal Financial Institutions Examination Council. (2014). *Bank secrecy act anti-money laundering examination manual appendix A: BSA laws and regulations*. Retrieved from https://bsaaml.ffiec.gov/manual.

Federal Financial Institutions Examination Council IT Examination Handbook. (n.d.). *Security guidelines*. Retrieved from https://ithandbook.ffiec.gov/it-booklets/e-banking/risk-management-of-e-banking-activities/information-security-program/security-guidelines.aspx.

Federal Trade Commission. (2013). *Fighting identity theft with the red flags rule: A how-to guide for business*. Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/fighting-identity-theft-red-flags-rule-how-guide-business.

Financial Services Information Sharing and Analysis Center. (2018). *Overview*. Retrieved from https://www.fsisac.com/who-we-are.

Homeland Security Today. (2020). *Cyberspace solarium commission recommends layered cyber deterrence in new report*. Retrieved from https://www.hstoday.

us/subject-matter-areas/cybersecurity/cyberspace-solarium-commission-recommends-layered-cyber-deterrence-in-new-rep.

Krebs, C. (2019). *Improving critical infrastructure cybersecurity; Fiscal year 2017 report to congress*. Retrieved from https://www.dhs.gov/sites/default/files/publications/cisa_-_improving_critical_infrastructure_cybersecurity.pdf.

Lyngaas, S. (2018). White House announces federal cyber strategy, vows to go on offensive. *Cyberscoop.com*. Retrieved from https://www.cyberscoop.com/white-house-cyber-strategy-john-bolton-announcement/.

National Institute of Standards and Technology (NIST). (2012). *NIST special publication 800-30: Guide for conducting risk assessments*. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

National Institute of Standards and Technology (NIST). (2018a). *About NIST*. Retrieved from https://www.nist.gov/about-nist.

National Institute of Standards and Technology (NIST) (2018b, April 16). *Framework for improving critical infrastructure cybersecurity—Version 1.1*. Retrieved from https://www.nist.gov/cyberframework/framework.

National Risk Management Center. (2018). *The National Risk Management Center*. U.S. Department of Homeland Security. Retrieved from https://www.cisa.gov/sites/default/files/publications/NRMC%20100%20Days%20Fact%20Sheet%2020181115_CISA%20v2.pdf.

Obama, B. (2013). *Executive order 13636: Improving critical infrastructure cybersecurity*. Washington, DC: The White House. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

Obama, B. (2016). *Presidential Policy Directive 41: United States cyber incident coordination*. Washington, DC: The White House. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

PCI Security Standards Council. (2020). *PA-DSS security standards library*. Retrieved from https://www.pcisecuritystandards.org/document_library?category=padss&document=pci_pa_dss_program_guide.

Randolph, K. (2018). DOE, DHS officials discuss cybersecurity and oil, natural gas infrastructure. *The Daily Energy Insider*. Retrieved from https://dailyenergyinsider.com/news/15250-doe-dhs-officials-discuss-cybersecurity-and-oil-natural-gas-infrastructure/.

Sedenberg, M. E., & Dempsey, X, J. (2018). *Cybersecurity information sharing governance structures: An ecosystem of diversity, trust, and tradeoffs*. Retrieved from https://arxiv.org/abs/1805.12266.

Stults, G. (2004). An overview of Sarbanes-Oxley for the information security professional. *SANS Institute InfoSec Reading Room*.

Retrieved from http://www.sans.org/reading-room/whitepapers/legal/overviewsarbanes-oxley-information-security-professional-1426.

Trump, D. (2018, September 20). *National Cyber Strategy of the United States of America*. Washington, DC: The White House. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Williams, B., Chuvakin, A., & Bradley, T. (2007). *PCI compliance: Understand and implement effective PCI data security standard compliance*. Waltham, MA: Syngress Publishing.

White House. (2018). *President Donald J. Trump is strengthening America's cybersecurity*. Retrieved from https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-is-strengthening-americas-cybersecurity/.

Zheng, E, D., & Carter, A, W. (2015). *Leveraging the Internet of things for a more efficient and effective military*. Retrieved from https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150915_Zheng_LeveragingInternet_WEB.pdf.