Cooperation amidst competition: cybersecurity partnership in the US financial services sector

JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2021, 1–11
https://doi.org/10.1093/cybsec/tyab024
Research paper

Research paper

Cooperation amidst competition: cybersecurity partnership in the US financial services sector

Sean Atkins*† and Chappell Lawson

Department of Political Science, Massachusetts Institute of Technology, Cambridge, MA 02139, USA

*Correspondence address. MIT Political Science, 30 Wadsworth Street, E-53-470, Cambridge, MA 02142, USA. Tel/Fax: +1 (617)-253-5262; E-mail: atkinss@mit.edu

†The views expressed in this article are those of the author and do not necessarily reflect the official policy or position of the US Air Force, the US Department of Defense or the US government.

Received 11 May 2021; revised 6 August 2021; accepted 10 November 2021

Abstract

The US Financial Services Sector (FSS) is commonly regarded as one of the most successful in addressing cybersecurity through public–private partnership and as a potential model for less advanced sectors. However, how well the sector has actually fared remains poorly understood. Based on publicly available material and in-depth interviews with those intimately involved in business–government collaboration on cybersecurity in the FSS, we analyze how and why collaboration evolved into its current form. We find that considerable gaps remain, which both reveal limitations in the current policy framework for the FSS and suggest lessons for other critical infrastructure sectors.

Key words: public–private partnership, cybersecurity, financial services, critical infrastructure

Introduction

Over the last two decades, cyber threats to critical infrastructure in the United States have grown in intensity and sophistication [1]. The Financial Services Sector (FSS) has been a prominent target and has already faced significant attacks. Among others, these include a massive Iranian distributed denial of service (DDoS) assault and a large-scale North Korean campaign against the financial transaction messaging network [2, 3].

Potential cyberattacks are especially concerning to the FSS, for several reasons. First, most of the sector's products are literally digital, rather than based on paper money or specie. For many firms, especially banks, cyber threats are not just "IT problems" (affecting firms' data and communications) or even "OT problems" (affecting control and safety systems); rather, they constitute an existential threat to firms' assets.[1] Second, the sector is highly interconnected, and many firms mutually depend on the same systems for critical functions such as payments clearing and settlement [4–7]. Firms must have confidence in the information they receive from one another for the sector to operate at its current pace and scale [8]. Successful attacks against one firm or system can thus produce sector-wide slowdowns or worse [7, 9]. Finally, and related, parts of the FSS (such as banking) depend uniquely on public trust. Given the baseline amount of leverage in the system, the mere perception that its integrity has been compromised can be devastating, as historical "runs on banks" and related financial meltdowns in the past have demonstrated [10, 11]. This inherent fragility is not fundamentally a cyber problem, but interconnectedness and the digitalization of money have exacerbated it.

It is difficult to overstate the importance of securing the financial sector from devastating cyberattack. As one observer put it: "The world's financial system could collapse and create an economic downturn as disastrous as the coronavirus recession or the global financial crisis if growing fears of a devasting cyber-security hack are realized" [12]. Actual effects of course depend on the type and severity of attack, but one recent analysis indicates that a successful compromise of the integrity of even one of the top five financial institutions could result in severe consequences for the broader financial system (including triggering liquidity runs and hoarding) on the order of 2.5 times daily GDP [13]. Furthermore, the size of the US FSS and its deep interconnectedness with the global economy means these consequences will not be confined to the United States. The US economy is the largest in the world, its equity markets make up around

1 IT refers to Information Technology while OT refers to Operational Technology.

half of the global market, and the US dollar is the most widely used currency. Shocks within the US FSS have historically reverberated throughout the global market and this is likely to be the case with those that are cyber induced. Whether the current policy framework for the FSS is effective thus matters enormously for economic security and social stability within the United States and abroad. In addition, to the extent that the existing framework does so, it may offer lessons for other sectors, where continuity of operations is equally essential (e.g. the power grid or telecommunications) [14].

Policymakers and private sector executives consider industry–government relationships in the FSS to be among the most successful among US critical infrastructures, with various forms of voluntary and not-so-voluntary interactions between firms and the government. However, they also note that many aspects of the "partnership" remain underdeveloped [15, 16, 17–31]. Therefore, although the evolution of government–industry engagement in the FSS has positive lessons to offer to other critical infrastructure sectors, it also calls for attention to the limitations of the current policy framework.

We base our analysis not only on publicly available material—government documents, academic articles, news reports, etc.—but also on several dozen interviews with those most involved in business–government collaboration on cybersecurity in the FSS.[2] To our knowledge, this article represents the first in-depth analysis of how the cybersecurity "partnership" has actually developed in a critical infrastructure sector, including the barriers to deeper collaboration.[3]

The next section provides a brief overview of cybersecurity challenges in the FSS. In the third section, we outline how the government–industry cybersecurity partnership, which includes both regulation and voluntary collaboration, operates. In the fourth section, we provide detail on the halting evolution of the partnership. In the fifth section, we review the factors that best explain this evolution and discuss their implications for the future direction of the sector. Finally, we discuss how the FSS's development might inform policy in other sectors.

To anticipate, we find that cooperation was shaped by four factors. First, whenever threats appeared to create system-wide risks, government and firms accelerated collaboration. Second, in the face of similar threats, firms differed in their willingness to make investments based on size and market segment.[4] Smaller firms and those in the insurance industry have consistently lagged behind large banks and investment banks. Third, in the absence of shared perceptions of threats, regulatory pressure played a significant role in forcing firms to adopt cybersecurity standards and highlighting the potential liability that firms might face if they neglected to take the problem seriously. However, regulatory attention to cyber risk has varied over time, and regulation was not responsible for the much greater and more valuable investments that large firms made on their own, which were primarily driven by the nature of the sector. Regulatory pressure was also mainly effective in compelling firms to adopt minimalist measures that do relatively little to protect against well-resourced threat actors—i.e. the principal systemic danger to the sector. Finally, competition among firms impeded cooperation, especially on the crucial dimension of information sharing. This impediment diminished over time, but it has retarded (and continues to retard) the needed measures.

The ultimate result of these four factors was a patchwork of collaborations and capabilities. Only recently has the sector devised useful, novel initiatives outside of the original framework—such as operational coordination between firms (on the one hand) and various federal agencies (on the other). Furthermore, these collaborations are limited to the largest companies.

Some of the most important factors that drove collaboration in the FSS are not present in other critical infrastructure sectors, or even in parts of the FSS. Extending the positive lessons of the FSS will thus require industry-specific arrangements, tailored to the idiosyncrasies of each sector, that can create trust among competing firms and between industry and the government. Many of these arrangements are simply not scalable beyond a small number of firms.

Cybersecurity in the FSS

The FSS is composed of over 40 000 firms of strikingly different sizes and types: depository institutions, investment firms, insurance companies, other credit and financing organizations, and providers of critical financial utilities and services [32, 33]. The shared information technologies on which these firms rely create a highly interdependent sector. Nevertheless, not all elements of the sector are equally crucial to its integrity and stability. A small number of very large players—sometimes described as "systemically important" or "too big to fail"—are critical for continuity of operations, as are certain clearance hubs and systems [34, 35]. There would be little substitutability if one of these entities were brought down by a cyberattack [9, 36].

Cyber threats differ considerably across a heterogeneous sector. In the insurance industry, concerns focus primarily on securing personal information about individuals. By contrast, smaller brokerage firms tend to be most concerned about ransomware attacks. Still others are primarily preoccupied with confronting sophisticated attempts at scams or theft. The banking industry sees all of these threats, in addition to larger concerns about public confidence.

Threat actors also vary, from amateur hackers to professional cybercriminals to the security services of adversary nation-states. From a systemic perspective, the most concerning threat actors are foreign governments that possess both the resources and the interest in disrupting or exploiting the financial system [37]. Some, such as North Korea, want to take advantage of the system for financial gain without regard for systemic consequences [3]. Others, such as Iran, want to disrupt the FSS as part of geostrategic competition with the United States and its allies [2]. Still others, such as Russia, seek to hold systems at risk as a deterrent [1].

Collaboration among firms, as well as between industry and government, is essential to mitigating systemic risk [22, 26, 28, 30, 31, 38–40]. The government has only limited visibility into private networks, and private firms cannot respond effectively to the most sophisticated and well-resourced actors. There is always a public interest in preventing and prosecuting criminal activity in cyberspace, as well as in forcing firms to protect personally identified data. In terms of critical infrastructure, however, the central issue for the federal government lies in protecting a small number of systemically important critical functions and very large firms against such sophisticated, well-resourced actors. Policy documents from the Department

2 An extensive Methodological Appendix discusses how we selected our interviewees and conducted the interviews [https://polisci.mit.edu/files/ps/imce/faculty/documents/Lawson%20PAR%20Methodological%20Appendix.pdf]. To preserve confidentiality, interviewees are identified here by monikers plus the year in which they were interviewed, e.g. "interview with Dulcinea 2019."

3 For a less ambitious review of the sector, see Tishuk 2012, Crisp *et al.* 2016, and San Juan Menacho and Martin 2019; Atkins and Lawson 2021 also provide short sketches of three different critical infrastructure sectors, one of which is the FSS.

4 See Friedman and Gokhale 2019.

of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) suggest an increasing focus on these "critical functions" [41].

In general, the FSS has "long been at the forefront of cybersecurity and industry-wide information sharing and cooperation" [42]. A recent Deloitte report indicated that financial firms spend between 0.2% and 0.9% of revenue on cybersecurity annually—far higher than in other critical infrastructure sectors, like energy [43]. The largest firms have invested billions of dollars in tools and personnel and possess advanced in-house capabilities. For instance, Morgan Stanley operates a sophisticated Cybersecurity Fusion Center charged with preventing, detecting, assessing, and responding to cyber threats, vulnerabilities, and incidents that create risk for the firm [44].

However, cybersecurity capabilities vary considerably across the FSS by subsector and firm size [45, 43]. For mid-size firms, wholly in-house capabilities are too expensive, and firms instead opt for a combination of in-house capacity and outside vendors that offer security as a service. Smaller firms that are unable to invest in building their own infrastructure often use technology service providers for their platforms, with varying degrees of sophistication and varying supplemental investments in security.

Given the degree of interdependence in the FSS, firms have a shared interest in preventing disruptive attacks. One crucial ingredient in security is sharing information on threats and vulnerabilities, in order to determine whether an attempt is being made to broadly compromise the system and to respond accordingly. However, most FSS firms are market competitors, which creates a disincentive to share such information, even on an anonymized basis.

Another important ingredient is sharing of information between industry and the government. Firms are reticent about sharing information with the government that could lead to audits from regulators. Meanwhile, government agencies are reluctant to share classified information about threats with a large number of individuals.

Finally, both government and industry want to know that the sharing of threat information will be a basis for action. The government seeks to ensure that firms will actually invest in cybersecurity, especially when informed about threats. For their part, industry seeks assurance that the federal government will take decisive and effective action against identified threat actors, especially state-sponsored actors whose resources and sophistication are far greater than those of any one firm.

Government–Industry Relationships

The basic structure of the "voluntary partnership" model [46] in the FSS is nominally similar to that of the 15 other critical infrastructure sectors. A "Sector-Specific Agency" (in this case, the Treasury Department's Office of Critical Infrastructure Protection and Compliance Policy) coordinates the government side (in this case, through the Finance and Banking Information Infrastructure Committee). An industry council (the Financial Services Sector Coordinating Council) does the same on the private sector side. Finally, an industry-run, not-for-profit entity (the Financial Sector Information Sharing and Analysis Center, or FS-ISAC) facilitates collaboration across firms within the sector and between the sector and the government by sharing "timely, relevant, and actionable … threat and incident information" [47, 48, 33]. After meeting separately, generally on a monthly basis, the government and the private sector sides meet jointly on a quarterly basis to discuss critical infrastructure security issues and activities [28, 33]. In practice, the activity of the FS-ISAC falls at the upper end of the spectrum in terms of how well these arrangements operate [49, 50, 39, 51]. The FS-ISAC has broad participation across the sector, with the smaller and medium-sized firms being represented by their industry associations, and provides an anonymized platform for firms to share information. Members broadly regard the FS-ISAC as useful in feeding a general tactical-level threat awareness across the sector [52, 53, 26, 24, 29, 46].

In addition to the FS-ISAC itself, operational relationships between industry and government are stronger than in other sectors. These relationships reflect the fact that many large firms have drawn cyber talent from the military, federal law enforcement, and the Intelligence Community. Such individuals bring cyber expertise and knowledge of threat actors, as well as personal relationships with officials to whom firms can potentially reach out in case of an attack [54–56, 23, 57].

Separate from these voluntary arrangements, regulators—including federal and state agencies as well as some industry organizations[5]—also figure prominently in the FSS cybersecurity landscape. Generally, regulators are organized by the categories of services that firms provide with different sets of authorities and different "mission focuses" [33, 58]. For instance, deposit, consumer credit, and payment systems products are regulated primarily by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Office of the Comptroller of the Currency. Investment products are regulated by the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission, banking regulators, insurance regulators for certain products, and self-regulatory organizations [36]. Whereas some regulators simply provide guidance, bank regulators publish enforceable standards that are backed up by inspections and stress tests to assess cybersecurity preparedness, event resolution planning, and safety and supervision [36]. The SEC falls in the middle of this spectrum: it can directly regulate some firms but has less authority than do banking regulators over third-party vendors who sell services to regulated firms [36]. In theory, the prospect of conflicting mandates for firms operating in more than one part of the industry were resolved when the five main agencies jointly agreed to a single set of minimal standards, but regulatory authorities and efforts remain fragmented [45, 21, 54].

Recently, a fourth element of the collaboration has emerged that has been distinctive to the FSS: a direct operational relationship between a group of large firms and the government through the Financial Systemic Analysis & Resilience Center (FSARC). Although the FSARC was established under the FS-ISAC, its membership is limited mainly to the largest banks.[6] In comparison to the larger FS-ISAC, the FSARC provides a venue where firms can have "the systemic-level conversations we couldn't before" about state-sponsored threats and the "ability to translate that information into action" [20]. The FSARC is also the interface for Project Indigo and follow-on Pathfinder initiatives, in which firms work through the DHS with

5 These include, e.g.: Federal Financial Institutions Examination Council member agencies (the Consumer Financial Protection Bureau, Federal Deposit Insurance Corporation, Federal Reserve Board of Governors, National Credit Union Administration, Office of the Comptroller of the Currency, and the FFIEC State Liaison Committee), the Securities and Exchange Commission, the National Association of Insurance Commissioners, the Federal Housing Finance Agency, the Commodity Futures Trading Commission, the National Futures Association, and the Financial Industry Regulatory Authority.

6 FSARC membership included banks such as Bank of America, BNY Mellon, Citigroup, Goldman Sachs, JPMorgan Chase, Morgan Stanley, State Street, and Wells Fargo.

US Cyber Command to experiment with directly disrupting state-sponsored threats [59].

Despite these extensive connections, challenges remain in both information sharing and coordination of responses to potential attacks. Information-sharing mechanisms have not consistently translated to increased sector-level awareness on systemic threats. As two interviewees put it, "the FS-ISAC is not providing what the systemically important firms need on systemic-level awareness" and "the bigger banks need something more because they're dealing with sophisticated state actors" [25, 21]. Even the FSARC's efforts have not yet produced the comprehensiveness or real-time speed for which the FSARC aimed [40]. As one executive put it, "timelier sharing that might approach the goal of real-time exchange is held back by trust issues with firms," who are market competitors [28]. Finally, although firms in the FSARC "love the fact that they can task the Intelligence Community" about threats to their operations [60], and firms in the other critical infrastructure sectors covet the FSARC's connections to government [16], the degree to which new relationships have actually resulted in greater security remains unclear. Neither government officials nor industry executives are satisfied with the current situation, but neither side has articulated a coherent strategy to improve it [21, 27, 45, 54, 55].

Piecemeal Evolution

The current business–government relationship evolved piecemeal and in stages, rather than by any guiding vision. The following discussion is organized around four stages that interviewees identified as representing marked shifts in the sector's development in both form and degree of effort: (i) an early start in 1998–2001, reflected in the creation of a policy framework in response to increasing digitalization of the sector; (ii) challenges to consolidation in 2002–11, during which progress on the policy framework slowed after the spasm of initial activity; (iii) "getting religion" in 2011–16, beginning with a major Iranian attack; and (iv) "broadening, deepening, and streamlining" since 2016 based on a growing understanding of the cyber risk presented through the sector's many interdependencies. In general, its evolution along these stages was driven primarily by changes in perceptions of the cyber threat. However, the partnership was facilitated or moderated by the sector's distinctive characteristics, including the nature of market competition.

Early start (1998–2001)

Early digitalization and direct connection to national economic security made the FSS one of the first targets for federal government action, even before the terrorist attacks of 11 September crystallized the notion of "critical infrastructure" or "homeland security" [53, 57]. The original presidential directive on critical infrastructure security anticipated that attempts to undermine US power would likely include economic targets [46], and early legislation on critical infrastructure also highlighted the critical risks posed by increasing dependence on the sector's "information structures" [61]. PDD-63 recognized the Treasury Department as the lead agency for the FSS. It also called for establishing ISACs in each sector, and the FS-ISAC became the first to emerge only a year later. In 2002, before President George W. Bush's Critical Infrastructure Protection Partnership Model called for establishing Government Coordinating Councils (GCCs) and corresponding Sector Coordinating Councils (SCCs), the FSS's government and industry counterparts had already established the FBIIC and FSSCC [62, 55, 57]. When the broader national critical infrastructure policy caught up, both were later chartered officially as the SCC and GCC, respectively. The informal and formal relationships developed in these early efforts enabled the collaborative creation of a sector infrastructure protection plan that incorporated cyber threats ahead of a published national requirement for one [63, 55].

For industry, these initial advances were largely motivated by awareness of the growing risks of cyber dependence [64, 65, 54, 55, 66]. The resulting business operations-focused agenda prioritized "strategic activities, such as developing plans on how to resume operations as soon as possible" after a disruption [63]. For the government, interest in cybersecurity by both regulators and the Treasury Department was spurred by recognition of how cyber threats to the FSS could damage US economic security [52].

This rapid start also reflected FSS ability to adapt existing regulatory structures and relationships of trust. As the SSA, Treasury's extensive industry relationships and sector expertise made it a trusted and valued partner. A strong network of trade and professional organizations also facilitated intra-sector collaboration and provided convenient touchpoints for government to connect with a vast and disparate sector. In other words, many stars aligned to encourage early collaboration.

Challenges to consolidation (2002–11)

Despite these early foundational successes, however, FSS partnership efforts developed sluggishly after the initial framework was created. In general, industry did not share the government's sense of urgency about cyber threats. New information technologies so vastly improved efficiency in business operations that they swamped concerns about security [25, 26].

Progress was also undermined by other factors within the industry. Companies remained concerned that sharing information with market competitors would undermine their competitive advantage [63]. Firms' uncertainty about the possibility that close collaboration on cybersecurity could be used by regulators in bringing anti-trust actions also hampered information sharing [54, 66].

The financial sector is heavily regulated, and independent federal agencies had the authorities to impose mandates on firms. In addition, the Federal Financial Institutions Examination Council (FFIEC) and Federal Reserve Board (FRB) took an early interest in cybersecurity. However, "their lack of cybersecurity expertise was certainly an issue" [64]. In practice, firms initially felt little regulatory pressure to share cybersecurity information with one another or with the government, nor to make investments in security beyond those they were already motivated to undertake.

"Getting Religion" (2011–16)

The calculus for firms started to shift significantly in 2011 once cyber threats appeared that could alter perceived business interests. In 2011, Iran launched a cyber campaign against the FSS that evolved into a "large-scale coordinated campaign of DDoS attacks" against 46 US financial institutions [2]. It lasted for 176 days, at times overwhelming banking systems and impacting hundreds of thousands of customers. This "near miss" shook the sector, leaving banks "scared out of their minds about sophisticated cyber threats" [22]. Because Iran's cyberattacks were planned and executed as a campaign across the financial system, the individual banks recognized that they lacked the sort of "campaign-level awareness" [49] needed to identify systemic threats, as well as the ability to coordinate a commensurate campaign-level response [23, 30]. North Korea's 2015 compromise of the SWIFT financial transaction messaging system further underscored potential systemic risks [8]. These attacks were not only a cat-

alyst for changes to the payments systems but also forced "increased working together" [67].

By the end of 2014, industry leaders broadly cited cybersecurity as the biggest systemic risk to the economy (a jump from preceding years); it has maintained that position in quarterly surveys of industry stakeholders since then, with the number of firm respondents identifying it as the top risk nearly doubling between 2013 and 2015 [68–70]. One characteristic response noted how cyber risks were multiplying faster than controls could address the continually escalating threats [69].

In response, cybersecurity spending dramatically increased and large firms began shifting from a relatively passive defense posture to a more active, operationally engaged approach [71, 72, 25]. The big banks "realized that they're going to have to change the game in order to continue to operate well into the future" [25]. With the realization of "what can happen in a systemic way if they're all targeted" [45], meaningful collaboration across the sector and with government increased. In other words, this period was one of "getting religion" [65] on cybersecurity.

One significant investment was the establishment of the FSARC in 2016 by a small group of systemically important financial institutions to enable "enhanced" information sharing and collaboration [21, 23, 25, 54, 70]. The aim was to address true systemic risk, including conversations with the government in the classified domain, for which the broader FS-ISAC construct proved impractical. Funded and led by its industry membership, the FSARC built locations adjacent to prominent government national security and law enforcement facilities to better facilitate interaction [72]. The scale of these large firms and their motivation to change the construct began to pull the rest of the sector along [45, 54]. As a senior government official described the dynamic, "some firms are more on the leading edge, pushing all of this forward, even dragging along the others who are less engaged or motivated" [28]. Initially, such efforts took the form of larger firms showing less advanced smaller firms how to approach particular problems; as larger firms began to better appreciate the risk that less sophisticated security practices at smaller firms posed to them and the system, they began to apply more pressure on the laggards with which they did business [54].

The sector's advances during this period benefited from the significant depth in sector expertise, existing relationships, and resources at the Treasury Department. This enabled the government to further build from an existing foundation of trust and to tailor efforts in a way that fit closely to the sector's unique needs. From 2014–16, e.g. Treasury developed and convened 13 "Hamilton Series" cybersecurity exercises, bringing together various government agencies and broad industry participation to "better prepare the financial sector in addressing the risks and challenges presented by significant cybersecurity incidents" [73]. The Treasury Department and Federal Reserve Bank's sector expertise and well-developed relationship with industry was central to rallying key players and crafting exercises that generated useful outcomes [28]. These outcomes ranged from the simple development of links and methods for information exchange to the creation of "Sheltered Harbor," a program that relies on sharing of customer data between firms for resilience during catastrophic cyber events [74, 36, 45].

The trust networks and organizational foundations established in an earlier period laid the foundation for deeper collaboration. The FS-ISAC developed new mechanisms to enable more timely tactical information sharing and established subsector "communities of interest" to further tailor information sharing and enable direct collaboration. One example was the Depository Trust and Clearing Corporation collaboration to develop Soltra Edge, an automated information-sharing platform [75]. Trade associations, such as the Financial Services Roundtable or the Securities Industry and Financial Markets Association, as well as regional groups such as ChicagoFIRST, also facilitated collaboration among their members in coordinating security and resilience efforts [33]. Recognizing their value, the FS-ISAC ultimately integrated at least 40 of these organizations into its membership [28].

Additionally, a fast-growing informal network of individuals hired out of government service into FSS firms acted as "pioneers" in building new bridges between the government and industry. As one senior executive discussed, the big banks were aware that at one point or another they would be targeted "and people that have experiences and relationships within government to be able to pick up the phone and say, hey, look, we might need your help here … is a very powerful thing" [25]. Trust was essential for solving what is effectively an N-person Prisoner's Dilemma: firms would collectively benefit from cooperation with one another, but they also have an incentive to use the information about vulnerabilities and breaches in other firms to their competitive advantage. One senior executive noted how trust was crucial not just in building day-to-day cooperation but also during times of crisis such as large-scale compromises or disruptions [24]. As an executive put it, "anytime you're in the [news]paper for cybersecurity, it's a bad day for business … it's an incentive to avoid or delay disclosure and sharing" [25]. In one case, a large firm breached by a nation-state cyber actor delayed sharing details to avoid damaging its reputation, resulting in further compromise of other firms across the sector [28]. As one government official put it, "people aren't going to work together if they don't trust the other party, and leveraging existing trusted relationships has acted as the seeds of trust in their institutional capacities" [45].

Trust was also important when it came to the business–government relationship. Firms found the prospect of sharing information on risks or breaches with regulators unnerving, as doing so could result in audits. They were more comfortable sharing information with the Treasury Department, which lacked regulatory authorities and with which senior executives might have preexisting relationships [19, 55, 66].

In contrast to these collaborative and voluntary efforts, the influence of regulatory pressure remained mixed. Existing regulators gradually brought to bear their authorities on cybersecurity [76, 21]. However, the main effect was anticipatory action by firms rather than regulations themselves: as soon as regulators began to coalesce around particular issues, firms had an interest in getting ahead of the conversation to help shape it [21].

Regulatory mandates sometimes had perverse consequences. Compliance efforts absorbed ~40% of cybersecurity executives' energy: time-consuming reviews, comments, and often litigation, making it difficult to keep pace with evolving cyber threats [7, 25, 76]. The Internet Security Alliance found that it took many firms 1000–2000 h to comply with an FFIEC tool, as opposed to the 80 h the FFIEC predicted [7].[7] Firms argued that compliance efforts diverted resources from meaningful security improvements [25, 76]. Put simply, during

7 The FFIEC Cybersecurity Assessment Tool involves first determining a firm's "inherent risk profile" by analyzing its Technologies and Connection Types, Delivery Channels, Online/Mobile Products and Technology Services, Organizational Characteristics, and External Threats. Next, it calls for assessing firms' "cybersecurity maturity" by evaluating its Cyber Risk Management and Oversight, Threat Intelligence and Collaboration, Cybersecurity Controls, External Dependency Management, and Cyber Incident Management and Resilience. Despite the FFIEC's articulated intent for voluntary use, a number of regulators have used the Cybersecurity Assessment

this period, regulatory authorities were not combined with more collaborative efforts in a way that consistently improved security.

Broadening, deepening, and streamlining (since 2016)

An evolving threat landscape continued to highlight the risks FSS firms faced, even from beyond their sector. For instance, a joint Federal Bureau of Investigation (FBI)–DHS technical report revealed that in 2016 Russian cyber operators targeted parts of the US energy sector [77], and additional press reporting indicated that they even compromised some electricity grid controls [78]. These activities attracted the attention of FSS leaders concerned with their dependence on reliable electricity. Separately, threats to the communications and information technology sectors also hold implications for the FSS. As Healey *et al.* [42] point out, "a large (and growing) % of the world's computing and storage falls to just a few cloud service providers," implying a concentration of risk.

Recognition of cross-sector systemic vulnerabilities continues to drive expansion of information sharing and collaboration efforts [23, 25, 45]. Firms have learned that, "while they can do a lot to reduce risk to their firm on their own, a lot of risk is external" [45]. Over the last couple years, financial firms have reached out to the electricity, communications, and transportation sectors without government prompting [45]. Regulatory pressure is also motivating action, as regulators are considering risks imposed by vendors, service providers, and other external functions on which firms rely [21].

Furthermore, increasing cyber risks for mid-tier and small banks during this phase have highlighted the interaction between the significance of cyber threats and the idiosyncrasies of the sector. The thickly interconnected structure of the FSS creates third-party cyber risk that has required firms to better understand its intra-sector dependencies [23, 25]. As such, larger firms have begun to consider how cyberattacks on smaller firms may translate to systemic risk [45].

During this period, regulatory pressure again helped drive cybersecurity capability investment across the FSS but its complex structure initially made these advances slow to achieve. To address the challenge that the web of disparate and overlapping requirements presented, regulators and industry leaders worked to harmonize cybersecurity regulatory standards across the sector, somewhat easing the burden. In addition, both government and private sector executives noted how regulators began to focus less on traditional checklist style compliance and more on "getting … at the elements of security to produce robustness and resilience" [45, 54, 21]. Finally, firms' remaining concerns that sharing information could leave them open to charges of anti-trust violations [79] were largely overcome [21, 54, 66]. Nevertheless, movement toward a unifying standard to improve security and reduce compliance burden is taking years to accomplish.

Another significant development since 2016 was an increasing role for the Department of Defense (DoD) in countering cyber threats to critical infrastructure [80 Sections 1642 and 1650]. Following the passing of the 2018 National Defense Authorization Act, the DoD and DHS established a pilot effort that connected US Cyber Command elements to industry through DHS and Treasury. Brigadier General Tim Haugh, a former Cyber National Mission Force commander, described the task for the associated cyber operators as "protecting critical infrastructure from sophisticated state-based attacks" [81]. The aim was to conduct the kind of sensitive information sharing that sharpened both the Defense Department's and industry's ability to jointly counter nation–state cyber threats to FSS critical infrastructure. The primary interface for this effort is the FSARC for two reasons. First, the FSARC mission and membership is concentrated on systemic risk to the sector. Second, the FSARC is composed of a small number of US institutions, making trust far easier to develop than with organizations like the FS-ISAC with over 7000 members across multiple countries [82].

Separately, the government has made greater efforts to further expand its attention beyond the largest firms. To reach the numerous smaller institutions, it is attempting to partner through trade associations but, as one government executive noticed, they vary in the buy-in they have from their constituents and often lack understanding of their firms' cybersecurity challenges [45]. This limitation in participation and expertise reduces the ability of the government to meaningfully connect with a wide range of firms on cybersecurity.

Summary

Business–government collaboration has deepened substantially since 1998, but in halting and piecemeal fashion. The FSS was the first critical infrastructure sector to establish the foundational elements of a partnership. Progress then slowed as interest in the gains in efficiency from integration of new information technology outpaced concerns over growing vulnerability. After 2011, the degree of interest and investment in cybersecurity began to dramatically increase, with new approaches to cybersecurity being developed and growing collaboration between firms and with the government. Finally, by 2016 FSS cybersecurity efforts began to broaden (focusing more on externally sourced risk from vendors, other FSS firms, and other sectors), deepen (to include increasing operational coordination), and streamline (with movement toward regulatory harmonization and more practiced interactions). Table 1 summarizers these stages.

Explaining Success and Failure

In general, FSS partnership institutions have functioned better than those in most other critical infrastructure sectors. Several factors are responsible for the progress to date.

The central factor in influencing capability investment and degree of collaboration within industry and between industry and government was the threat and its significance to financial and national interests. The degree of risk cyber threats and vulnerability posed for both firms and the nation motivated direct CEO and Secretary-level involvement and investment. Whenever cyber threats presented shared systemic-level dangers or threatened to undermine trust and confidence in the industry, government and firms accelerated partnership efforts.

Regulatory relationships played a role in forcing firms to adopt standards by highlighting the potential liability that firms might face if they neglected cybersecurity. However, regulatory attention to cyber risk varied over time, and different regulators often focused on different aspects of cybersecurity. Furthermore, regulatory pressure primarily compelled firms to adopt minimalist measures; it was not responsible for the much greater investment firms made on their own.

In general, the nonregulatory interface with the government has proven a good match. In comparison to SSAs in other sectors, the Treasury Department is relatively well resourced and has a long-standing relationship with sector firms, trade organizations, and regulators [21–23, 25, 27, 28, 30, 31, 40, 45, 52]. This history enables Treasury to facilitate and lead FSS advances by providing funding to build out the capabilities of the FS-ISAC [31] or coordinating exercises that test the sector's cyber readiness, generate innovations, and build resilience [21, 23, 25, 28, 40, 66].

Tool during examinations making its criteria *de facto* regulatory requirements. See https://www.ffiec.gov/cyberassessmenttool.htm for more details.

Table 1: Evolution of cybersecurity policy in the FSS

	Stage A	Stage B	Stage C	Stage D
Time period	1998–2001	2002–11	2011–16	Since 2016
Defining initial event	PDD-63	Changes after 9/11	Foreign attacks	Risk from external failures
Investments by firms	High, especially among large banks	Medium, highest among large banks	High, especially among large banks	Medium, highest among large banks
Regulatory approach	Weak and uncoordinated	More aggressive but ham-fisted; uncoordinated	More flexible	Coordinated and more flexible
Information sharing with industry	Medium	Medium	Medium	Medium, led by large banks
Information sharing with government	Limited	Limited	Limited	Medium, highest among large banks
Operational coordination	None	Modest	Mainly through informal networks	Significant improvement with largest firms (FSARC)
Primary drivers of collaboration	Early digitalization, nature of industry, resources available to firms, strong SSA	As in (A), plus regulatory pressure	As in (A), plus increasing "trust networks"	As in (C)
Primary obstacles to collaboration	Interfirm competition, lack of preexisting industry structure, and regulatory inexperience	Interfirm competition, antitrust concerns, and Clunky regulation	Interfirm competition	Interfirm competition

At the same time, several other factors have consistently constrained progress. When it came to voluntary investments in cybersecurity capabilities, firm size and market segment mattered.[8] Smaller firms and those in the insurance industry have generally lagged behind large players, especially banks and investment banks [82, 16, 45, 54]. Driving the progress that large firms have made throughout the system remains a crucial challenge, and the FSS has not yet identified an efficient mechanism for doing so that would not prove excessively burdensome for smaller firms.

Second, although firms perceive significant benefit in sharing information on threats and vulnerabilities, they also face incentives not to collaborate with each other or with the government on cybersecurity. Cyber infrastructure is so closely tied to business operations and reputations, information related to these operations and security failures are tied to firms' competitive advantage. While the power of this incentive has reduced over time as firms have found it is largely not in their interest to compete on cybersecurity, it does resurface and become particularly acute after discovery of a cyber incident (just when collaboration and information sharing is most critical).

Third, because the sector is heavily regulated, firms have reservations about sharing information on threats and vulnerabilities with the government for fear of triggering audits or increasing their exposure to liability. Guidance from the Federal Trade Commission and the Department of Justice attempted to alleviate this concern, in order to facilitate greater sharing [83], but firms have remained concerned about how information they provided would actually be used in the context of an investigation, regulatory action, or large-scale lawsuit [54].

Another persistent challenge involves the complex of disparate regulators, each with differing authorities, expertise, and ideas about what cybersecurity means to their area of concern. Because many companies offer services from more than one category, they are subject to the scrutiny of overlapping but not necessarily aligned requirements. In theory, different regulators could impose cybersecurity mandates different from those of other regulators (as well as from whatever the Treasury or DHS might recommend). Recently, these agencies have undertaken efforts to harmonize requirements to align with common standards profiles [84, 85].

Larger firms intensely resent the "checklist-based" approach of regulatory agencies, with their accompanying audits [7], which they believe prevent firms from tailoring the cybersecurity efforts to the most important threats. Furthermore, standards developed by the government through the NIST framework are simultaneously beyond the capabilities of small firms and far below the extant capabilities of the large firms [21, 23, 25, 29, 49, 66, 52].[9] The current policy regime thus creates a clash between a classic regulatory approach aimed at ensuring that firms make the necessary investments to protect the public interest and a true partnership model aimed at jointly addressing mutually recognized threats [86].

These challenges manifest themselves at the operational level. In other words, the current regime looks better on paper (FS-ISAC, FSARC, etc.) than in practice. Private sector security officers often discuss frustrations with the quality and quantity of government information, as well as a lack of understanding of government capabilities [23, 25, 52]. Some described their sharing relationship as "throwing information over the wall with little reciprocation" [54, 66]. For their part, government interviewees often mentioned having an opaque sense of what was actually taking place within the sector and lacking the industry information needed to help focus its efforts to support them [28, 40, 45, 87]. Sharing with the government has worked best with a small number of large firms, where some greater degree of trust can potentially be established.

In this context, many of the advances in the sector have been based on informal trust relationships. The sources of this trust can

8 See also Friedman and Gokhale 2019.

9 The NIST cybersecurity framework was developed through collaboration between industry and government experts based on established standards, guidelines, and best practices. It is composed of a series of evaluation categories that fit within five cybersecurity functions: identify, protect, detect, respond, and recover. See https://www.nist.gov/cyberframework for more detail.

be found in trade organizations, a strong cyber workforce network, industry hiring from government organizations, and the longstanding relationships between the Treasury Department, regulatory agencies, and industry. For instance, the Treasury Department's well-developed relationships and close interaction with industry and regulators aligned deep sector expertise and a strong existing trust foundation to the cybersecurity challenge. This ensured that its leadership efforts as the SSA connected to the sector with increased effect. The most important challenge for advancing cybersecurity in the FSS is to convert these various informal relationships into something more stable and institutionalized.

The FSS itself will likely continue to be a moving target with technological advances evolving or disrupting the way the sector operates. For instance, traditional banks and securities firms are increasingly joined by nontraditional entities such as nonbanks that provide financial services to expanding parts of the market, often facilitated by fintech developments. This not only changes the sector's cyber vulnerability landscape but it also affects its ability to organize to address it, as these new firms likely have different or no established relationships with the sector's traditional firms, trade groups, and associated government organizations. This also poses a particular challenge for regulators attempting to increase the sector's overall cybersecurity baseline. New firms may be outside the bounds of regulatory scrutiny or may be introducing new infrastructure and ways of operating that outpace regulator expertise or confound the frameworks they use to evaluate firms [88, 89]. The previously mentioned migration to cloud infrastructure, for instance, even blurs the line of responsibility between regulated firms and cloud service providers.

The continuously shifting cyber landscape points to the need for a more adaptive regulatory model, i.e. an approach designed to enable routine learning and self-correction and adjustment to changing conditions over time [90, 91]. This stands in contrast to most regulatory approaches that devise solutions that are only reviewed when failure generates high enough costs to bring high-level attention. Regulation tends to create static checklists that make identifying the need for and process of adaptative change over time difficult. Even regulatory regimes that are intended to be more adaptive—i.e. "performance-based regulation"—tend to devolve in practice to static lists, as with the FFIEC Cybersecurity Assessment Tool and Cyber Risk Institute's Cybersecurity Profile [92, 93]. This places even higher demand on regulator expertise and on the relationship between firms and regulators. Although regulatory approaches—including liability shifting—can work well in forcing firms to protect personally identified data, they are a poor tool for forcing firms to share information on threats or mandating investments that actually lead to security among sophisticated firms.

Rather, further progress requires expanded and deeper (more operational-level) public–private cooperation, leveraging a broader range of government capabilities and tools of statecraft. For example, the recent Cyberspace Solarium Commission views a growing role for US military cyber operators to "defend forward" to secure US critical infrastructure: i.e. "proactive observing, pursuing, and countering of adversary operations and imposing costs in day-to-day competition to disrupt and defeat ongoing malicious adversary cyber campaigns, deter future campaigns, and reinforce favorable international norms of behavior" [94, 95]. The Departments of Justice and Homeland Security also possess capabilities and authorities that provide further advantage. However, to be effective these organizations require greater collaboration with the industry elements they are helping to defend. Success in cybersecurity is ultimately a matter of continuous improvement, rather than compliance with a specific set of measures. This is doubly true with regard to partnerships built upon trust, which can evolve and decay.

Lessons

Although the general policy that the US government adopted is similar across critical infrastructure sectors, it has not operated the same way in each [51]. The idiosyncrasies of each sector mean that only some of the lessons from the FSS apply elsewhere. For instance, whereas cyber threats to FSS firms directly threaten digital products and system trust, this is not true in other industries (such as oil and gas) where cyber threats may harm business operations but do not pose an existential threat. Consequently, the degree of voluntary investment by firms is destined to be smaller. In addition, sectors like electricity, water, electoral systems, and dams are often constrained in what they can invest in cybersecurity, as a result of budget constraints or a regulatory framework focused on lowering the rate base. If the government wishes to elevate cybersecurity capabilities in these sectors, it will have to rely more heavily on subsidies or regulation than it did in the FSS.

One important lesson from the FSS is the importance of the fit between government and industry interlocutors. In the FSS, relationships between the Treasury Department and the main financial institutions were strong and reciprocal. In other sectors (e.g. health care), however, the Sector Specific Agency (SSA) has been much less competent, experienced, connected to industry, aligned to the task, adequately resourced, or sufficiently expert in cybersecurity [50]. Furthermore, some regulators have enjoyed better relationships with industry, had greater expertise on cyber, or been better able to coordinate coherent policies than have other regulatory bodies. In the FSS, regulators were reasonably competent when it came to cybersecurity, but they were prone to checklists and (for several years) not well coordinated among themselves. For either regulatory or collaborative approaches to work well, the government must ensure that its side of the interface is well suited to the task. A good fit is particularly important for more advanced operational relationships, such as the FSARC/ARC, where trust among all parties is essential to success.[10]

The history of the FSS also highlights the importance of intra-industry relationships. In sectors that are too large for trust to develop among all firms, organizing trusted subgroups may be necessary. Because reliance on such subgroups in turn raises questions of bias in favor of certain firms, a "club" approach may in turn necessitate compensatory policies specific to that industry, as well as measures designed to extend security improvements among large firms to the rest of the sector. For instance, developing ways to expand the security benefits of FSARC/ARC participation beyond the handful of members should be a policy priority.

Another salient lesson from the experience of the FSS concerns the importance of industry-wide awareness when faced with nation-state threats. State-run cyber operations against any one firm are frequently part of a larger campaign. Addressing this type of threat requires aggregating and analyzing all the disparate indications that a campaign is underway and then coordinating a sector-wide response. This necessity underscores the value of established, durable, real-time connections across firms—and between firms and the government—at the operational level.

10 The FSARC has recently been reestablished as the Analysis and Resilience Center for Systemic Risk (ARC) with expanded membership that includes entities from the electricity subsector. See https://systemicrisk.org/who-we-are/ for more details.

A related lesson is that whatever form the business–government interactions take in each sector, they must be adaptable to a dynamic context. Cyber threats and vulnerabilities continuously evolve in all sectors, but the rate of change in threats may differ from one sector to another. Where change is fast and the information that should drive investment is dispersed, traditional regulatory processes are unlikely to keep pace and thus will be far less effective. By contrast, regulatory mechanisms may be useful in other sectors where development and integration of new infrastructure technologies occurs at a much slower pace, or where the government's goal is static (as with protection of personally identified information).

Finally, the FSS case underscores the increasing importance of cross-sector partnerships. As the financial service sector has addressed its own cyber risk, its susceptibility to potential failures in the communications sector and electricity subsector have risen in salience. With the growing interdependence of sectors on one another, directly or through the Internet, the urgency of addressing cross-sector threats has become increasingly apparent. Doing so will require not only direct communication among systemically important firms in separate industries, but also organization on the government side to overcome bureaucratic friction that impedes progress.

Looking Forward

Future research could address several aspects of the FSS on which this article could only touch briefly. First, quantitative measures that capture both quantity and quality of information sharing across the sector could refine our understanding of the evolution of the FSS. Second, expanding investigation of the FSS in other countries might reveal other factors at work there that played less of a role in the US case.[11]

By most accounts, the US FSS is a successful case of public–private partnership for critical infrastructure cybersecurity. A closer look, however, reveals the varied contours of success over time and across the sector, as well as the factors that explain them. Degree of systemic risk, firm characteristics such as size and market placement, regulatory pressure, and degree and type of competition between firms largely explain the sector's evolution. These same factors continue to drive and shape the FSS' efforts as it turns attention to areas where both government and industry leaders remain unsatisfied. These include information sharing that provides more timely and actionable awareness of systemic cyber threats, improved operational coordination within the sector and with government entities, and more operationalized partnerships below the largest firms and with other critical infrastructure sectors the FSS relies on. Understanding these factors can inform efforts that harness their positive influences, overcome the negative, and enable systemic adaptation at a speed and quality that match the cybersecurity challenge.

11 For instance, the United Kingdom's threat intelligence-led assessments that include a penetration testing phase are a potential way to shift regulation further away from static checklists and make it more adaptive to the threat environment (see Bank of England, CBEST Threat Intelligence-Led Assessments Implementation guide for CBEST participants, https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity/cbest-threat-intelligence-led-assessments-implementation-guide). See the GFMA Framework for the Regulatory Use of Penetration Testing for recent work on adopting this within the US FSS (https://www.gfma.org/wp-content/uploads/2020/12/gfma-penetration-testing-guidance-for-regulators-and-financial-firms-version-2-december-2020.pdf).

References

1. Coats D. Worldwide Threat Assessment of the US Intelligence Community. Office of the Director of National Intelligence. 2019.
2. USA v. Fathi et al. Sealed Indictment. No. 16 CRIM 48. US District Court Southern District of New York. 2016. https://www.justice.gov/opa/file/834996/download (26 August 2019, date last accessed).
3. USA v. Park. Criminal Complaint. No. MJ18-1479. US District Court for the District of Central California. 2018. https://www.justice.gov/opa/press-release/file/1092091/download (26 August 2019, date last accessed).
4. Claessens S. Competition in the financial sector: overview of competition policies. In: *The World Bank Research Observer*. Vol. 24. 2009, 83–118.
5. Claessens S, Laeven L. What Drives Competition? Some International Evidence. Paper prepared for the Federal Reserve Bank of Cleveland conference on Bank Competition. 2003.
6. The White House. PPD-21. Presidential Policy Directive: Critical Infrastructure Security and Resilience. 12 February 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (3 Jun 2019, date last accessed).
7. Crisp D. *et al.* Cybersecurity and the banking and financial sector. In: Clinton L, Perera D (ed). *The Cybersecurity Social Contract: Implementing a Market-Based Model for Cybersecurity*. Arlington, VA: Internet Security Alliance, 2016, 82–99.
8. Cilluffo F. Comments during panel on 'The Finance Sector and Countering Cyber Threats: Lessons from the Front Lines.' RSA Conference 2017. San Francisco.
9. OFR (Office of Financial Research). OFR Financial Stability Report. Department of the Treasury. 2017. https://www.financialresearch.gov/financial-stability-reports/files/OFR_2017_Financial-Stability-Report.pdf (9 February 2021, date last accessed).
10. Heffernan S. The causes of bank failures. In: Mullineux A, Murinde V (eds). *Handbook of International Banking*. Northampton, MA: Edward Elgar, 2003, 366–402.
11. Friedman M, Schwartz A. *A Monetary History of the United States, 1867–1960*. Princeton, NJ: National Bureau and Economic Research and Princeton University Press, 1963.
12. Wright S. Cyber attack could bring down entire financial system: IMF. *Sydney Morning Herald*, 8 December 2020. https://www.smh.com.au/politics/federal/cyber-attack-could-bring-down-entire-financial-system-imf-20201207-p56l6y.html (9 February 2021, date last accessed).
13. Eisenbach TM, Kovner A, Lee MJ. *et al.* Cyber risk and the U.S. financial system: a pre-mortem analysis. *Federal Reserve Bank of New York Staff Reports*. No. 909. May 2021.
14. Van Eeten M, Nieuwenhuijs A, Luiijf E. *et al.* The state and the threat of cascading failure across critical infrastructures: the implications of empirical evidence from media incident reports. *Public Adm* 2011;**89**:381–400.
15. Interview with Stockton. 2019.
16. Interview with Miami. 2019.
17. Interview with Dulcinea. 2019.
18. Interview with Corona. 2019.
19. Interview with Austria. 2019.
20. Interview with Anaheim. 2019.
21. Interview with Garden Grove. 2019.
22. Interview with Capistrano. 2019.
23. Interview with Tustin. 2019.
24. Interview with El Toro. 2019.
25. Interview with Orange. 2019.
26. Interview with Rancho. 2019.
27. Interview with Irvine. 2019.
28. Interview with Laguna. 2019.
29. Interview with Pilsner. 2019.
30. Interview with Delhi. 2019.
31. Interview with Salzburg. 2019.
32. Department of Homeland Security. *Banking and Finance: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan*. May 2007. https://www.dhs.gov/xlibrary/assets/nipp-ssp-banking.pdf (25 September 2019, date last accessed).

33. Department of Homeland Security. Financial Services Sector Specific Plan. Washington D.C. 2015. https://www.dhs.gov/sites/default/files/publications/nipp-ssp-financial-services-2015-508.pdf (3 June 2019, date last accessed).
34. Schmalz M. One big reason there's so little competition among U.S. banks. *Harv Bus Rev*. 13 June 2013.
35. Sorkin A. *Too Big to Fail: The Inside Story of How Wall Street and Washington Fought to Save the Financial System—and Themselves*. New York, NY: Penguin Press, 2009.
36. OFR (Office of Financial Research). Cybersecurity and Financial Stability: Risks and Resilience. Department of the Treasury. 15 February 2017. https://www.financialresearch.gov/viewpoint-papers/files/OFRvp_17-01_Cybersecurity.pdf (15 June 2019, date last accessed).
37. Bank of England. Topic Article: Could a Cyber Attack Cause a Systemic Impact in the Financial Sector. *Quarterly Bulletin: 2018 Q4*. 2018. https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2018/could-a-cyber-attack-cause-a-systemic-impact-final-web.pdf?la=en&hash=61555F2E3C15AD6B65E845C13238733B9364D4F6 (14 July 2019, date last accessed).
38. Brown M. *Cyber Imperative: Preserve and Strengthen Public–Private Partnerships*. National Security Institute at George Mason University. 2018.
39. Interview with Lake Forest. 2019.
40. Interview with Irwin. 2019.
41. Cybersecurity and Infrastructure Security Agency (CISA). National Critical Functions. 2020. https://www.cisa.gov/national-critical-functions (6 October 2019, date last accessed).
42. Healey J. *et al. The Future of Financial Stability and Cyber Risk*. Washington DC: Brookings Institution. 2018.
43. Friedman S, Gokhale N. Pursuing Cybersecurity Maturity at Financial Institutions. Deloitte. 1 May 2019. https://www2.deloitte.com/insights/us/en/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html (3 June 2019, date last accessed).
44. Easterly J. Interview on 'Beyond the Breach' July 2019. https://podcasts.apple.com/us/podcast/4-narration-jen-easterly/id963810915?i=1000444600269 (17 August 2019, date last accessed).
45. Interview with Monterey. 2019.
46. The White House. PDD-63. Presidential Decision Directive/NSC-63, Critical Infrastructure Protection. 22 May 1998. https://fas.org/irp/offdocs/pdd/pdd-63.htm (15 May 2019, date last accessed).
47. Office of the Inspector General. Cybersecurity: Department of the Treasury's Activities to Protect Critical Infrastructure in the Financial Services Sector. Audit Report. Department of the Treasury. April 28 2016. https://www.treasury.gov/about/organizational-structure/ig/Audit%20Reports%20and%20Testimonies/OIG-16-038.pdf (3 June 2019, date last accessed).
48. Department of the Treasury. Critical Infrastructure Protection and Compliance Policy . 2019. https://www.treasury.gov/about/organizational-structure/offices/Pages/–Office-of-Critical-Infrastructure-Protection-and-Compliance-Policy.aspx (6 October 2020, date last accessed).
49. Interview with Thailand. 2019.
50. Interview with Costa Mesa. 2019.
51. Atkins S, Lawson C. An improvised patchwork: success and failure in cybersecurity policy for critical infrastructure. *Public Adm Rev* 2021;**81**:847–61.
52. Interview with Huntington. 2019.
53. Chappell L, Bersin A, Kayyem J (eds). *Beyond 9/11: Homeland Security for the 21st Century*. Cambridge, MA: MIT Press. 2020.
54. Interview with Tico. 2019.
55. Interview with Milano and Montreal. 2019.
56. Interview with Brooklyn. 2019.
57. Interview with Broadway. 2020.
58. Abend V. *Comments During Panel on 'The Finance Sector and Countering Cyber Threats: Lessons from the Front Lines*.' RSA Conference 2017. San Francisco.
59. Borghard E. Protecting financial institutions against cyber threats: a national security issue. Carnegie Endowment for International Peace. 2018. https://carnegieendowment.org/2018/09/24/protecting-financial-institutions-against-cyber-threats-national-security-issue-pub-77324 (14 June 2019, date last accessed).
60. Interview with Jerusalem. 2019.
61. Critical Infrastructures Protection Act of 2001 (CIPA). 42 U.S. Code § 5195c. 2001.
62. Financial and Banking Information Infrastructure Committee (FBIIC). President's Working Group on Financial Markets, Sponsorship of the Financial and Banking Information Infrastructure Committee. 8 August 2003. https://www.dhs.gov/sites/default/files/publications/financial-banking-charter-2003-508.pdf (14 June 2019, date last accessed).
63. Government Accountability Office (GAO). Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Varies by Sector's Characteristics. October 2006. https://www.gao.gov/assets/260/252603.pdf (17 July 2019, date last accessed).
64. Interview with Doheny. 2019.
65. Interview with Wilhelm. 2019.
66. Interview with Fullerton. 2019.
67. McGuire C. *Comments During Panel on 'The Finance Sector and Countering Cyber Threats: Lessons from the Front Lines*.' RSA Conference 2017. San Francisco.
68. Depository Trust and Clearing Corporation (DTCC). Systemic Risk Barometer: 2013 Q1. May 2013. https://www.dtcc.com/systemic-risk/systemic-risk-barometer-surveys (15 June 2019, date last accessed).
69. Depository Trust and Clearing Corporation (DTCC). Systemic Risk Barometer: 2014 Q3. October 2014. https://www.dtcc.com/systemic-risk/systemic-risk-barometer-surveys (15 June 2019, date last accessed).
70. Depository Trust and Clearing Corporation (DTCC). Systemic Risk Barometer: 2016 Q3. October 2016. https://www.dtcc.com/systemic-risk/systemic-risk-barometer-surveys, (15 June 2019, date last accessed).
71. Morgan S. J.P. Morgan, bank of america, citibank and wells fargo spending $1.5 billion to battle cyber crime. *Forbes*, 13 December 2015. https://www.forbes.com/sites/stevemorgan/2015/12/13/j-p-morgan-boa-citi-and-wells-spending-1-5-billion-to-battle-cyber-crime/#6bc450f1116d (15 June 2019, date last accessed).
72. Rattray G. *Comments During Panel on 'The Finance Sector and Countering Cyber Threats: Lessons from the Front Lines*.' RSA Conference 2017. San Francisco.
73. Financial Services Sector Coordinating Council (FSSCC). Financial Services Sector Cybersecurity Recommendations. Letter to 'Policy Makers in the Administration and US Congress. 18 January 2017. https://www.fsscc.org/files/galleries/FSSCC_Cybersecurity_Recommendations_for_Administration_and_Congress_2017.pdf (15 June 2019, date last accessed).
74. Demos T. Banks build line of defense for doomsday cyber attack. *Wall Street Journal*, 3 Dec 2017. https://www.wsj.com/articles/banks-build-line-of-defense-for-doomsday-cyberattack-1512302401, (15 June 2019, date last accessed).
75. Depository Trust and Clearing Corporation (DTCC). FS-ISAC and DTCC Announce Soltra, a Strategic Partnership to Improve Cyber Security Capabilities and Resilience of Critical Infrastructure Organizations Worldwide. Press Release. 2014. http://www.dtcc.com/news/2014/september/24/fs-isac-and-dtcc-announce-soltra, (8 June 2020, date last accessed).
76. Interview with Hollywood. 2019.
77. USCERT. Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. National Cyber Awareness System. 16 March 2018. https://www.us-cert.gov/ncas/alerts/TA18-074A (15 June 2019, date last accessed).
78. Greenberg A. Hackers gain direct access to US power grid controls. *Wired*, 6 Sep 2017. https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/?verso=true (15 June 2019, date last accessed).
79. Bloom M. Information Exchange: Be Reasonable. Bureau of Competition, Federal Trade Commission. 2014. https://www.ftc.gov/news-events/blogs/competition-matters/2014/12/information-exchange-be-reasonable (20 August 2019, date last accessed).
80. John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019. Pub. L. No. 115-232. 2018. https://www.congress.gov/bill/115th-congress/house-bill/5515/text (15 June 2019, date last accessed).

81. Haugh T. *Speech to the International Conference on Cyber Engagement*. Washington DC: Atlantic Council. 23 April 2019.
82. Interview with Bermuda. 2019.
83. Federal Trade Commission (FTC) and The Department of Justice. Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cybersecurity Information. 10 April 2014. https://www.ftc.gov/system/files/documents/public_statements/297681/140410ftcdojcyberthreatstmt.pdf (21 August 2019, date last accessed).
84. National Institute for Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity. April 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (15 June 2019, date last accessed).
85. Financial Services Sector Coordinating Council (FSSCC). The Financial Services Sector Cybersecurity Profile (Draft v4.0). November 2020. https://fsscc.org/Sector-Profile-and-Risk-Tiering (11 January 2021, date last accessed).
86. Clinton L, Perera D (eds). *The Cybersecurity Social Contract: Implementing a Market-Based Model for Cybersecurity*. Arlington, VA Internet Security Alliance, 2016.
87. Interview with Balboa. 2019.
88. World Economic Forum. World Economic Forum Convenes New Consortium to Address Fintech Cybersecurity. 6 March 2018. https://www.weforum.org/press/2018/03/world-economic-forum-convenes-new-consortium-to-address-fintech-cybersecurity/ (2 April 2020, date last accessed).
89. Reuters. Citigroup, Zurich Insurance consortium to develop cyber security norms: FT. 6 March 2018. https://www.reuters.com/article/us-citigroup-cyber/citigroup-zurich-insurance-consortium-to-develop-cyber-security-norms-ft-idUSKCN1GI0L2 (2 April 2020, date last accessed).
90. McCray L, Oye K. *Adaptation and Anticipation: Learning from Policy Experience*. Center for International Studies working paper. Cambridge, MA: Massachusetts Institute of Technology. 2007.
91. McCray L, Oye K, Petersen A. Planned adaptation in risk regulation: an initial survey of US environmental, health, and safety regulation. *Technol Forecast Soc Change* 2010;77:951–9.
92. Cyber Risk Institute Financial Services Sector Cybersecurity Profile. 2018. https://cyberriskinstitute.org/the-profile/ (26 July 2021, date last accessed).
93. Federal Financial Institutions Examination Council. Cybersecurity Assessment Tool. 2017. https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf (2 February 2019, date last accessed)
94. US Cyberspace Solarium Commission. Final Report. 2020. https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view (5 January 2021, date last accessed).
95. Borghard E. Operationalizing defend forward: how the concept works to change adversary behavior. *Lawfare* 2020. https://www.lawfareblog.com/operationalizing-defend-forward-how-concept-works-change-adversary-behavior (28 Aug 2020, date last accessed).