OFR
OFFICE OF FINANCIAL RESEARCH

VIEWPOINT

Cybersecurity and Financial Stability: Risks and Resilience

17-01 | February 15, 2017

Cybersecurity incidents can cause real harm to the operations and customers of a financial firm. Moreover, firms and regulators widely agree that these incidents can also threaten the stability of the financial system. The next step for regulators and industry is to address those risks. This OFR viewpoint shows how regulators and industry can build on their approaches to cybersecurity to promote financial stability. It describes how a cybersecurity incident could threaten financial stability through three channels: Incidents can (1) disrupt the operations of a financial firm that provides critical services, (2) reduce confidence in firms and markets, and (3) damage the integrity of key data.

The OFR identified cybersecurity as a key threat to financial stability in our *2016 Financial Stability Report* and *2016 Annual Report to Congress*. Financial firms are vulnerable because they rely heavily on information technology (IT), and because of their many links to each other, to financial markets, and to other parts of the economy. Cybersecurity has become more urgent as malicious actors develop more sophisticated techniques. But quantifying the risks or the resilience of institutions to cybersecurity incidents is difficult. The lack of standardized data about such incidents and firms' controls adds to the challenge of protecting the financial system.

This OFR viewpoint describes how cybersecurity incidents can threaten financial stability. It reviews the forms incidents can take. It then discusses the channels through which an incident can threaten financial stability. The viewpoint also looks at how U.S. financial firms and regulators deal with the threat of cyber incidents, including how those approaches vary across types of firms.

Firms are primarily responsible for their own security. They fight malicious cyber activity on many fronts (see White House, 2013). In addition, regulators have acted to increase the resilience of the broader financial system. They have encouraged information sharing and collaboration among firms and regulators. Regulators have also issued cybersecurity guidance and

rules for financial firms. Still, more collaboration could benefit regulators. Regulators should also consider how regulatory boundaries may limit their individual perspectives on financial networks.

Cybersecurity Incidents Take Varied Forms

Cyberattacks are deliberate efforts to disrupt, steal, alter, or destroy data stored on IT systems. Tactics include finding weaknesses in software to get into IT systems, targeting e-mail accounts to steal passwords (spear-phishing), targeting websites to infect users with malicious software (malware), and planting software that locks users out of their own systems (ransomware). The Internet provides more ways for attackers to enter proprietary IT systems and networks.

Cyberattacks are deliberate efforts to disrupt, steal, alter, or destroy data stored on IT systems.

- Detailed data on frequency, tactics, and results of cybersecurity incidents are scarce.
- Attacks are often motivated by profit.
- Many intruders are technically sophisticated and have a nuanced understanding of a firm's operations.
- Recent incidents have touched banks — even central banks are at risk.

Detailed data on frequency, tactics, and results of cybersecurity incidents are scarce. Data are scarce in part because financial firms avoid reporting incidents due to reputation concerns. They also may want to avoid giving insights to hackers (see OFR, 2015; U.S. Congress, 2016). Evidence of the growth in cybersecurity concerns is apparent in industry surveys, reports from service providers, regulatory filings, and responses to high-profile incidents (see Symantec, 2016).

Attacks are often motivated by profit. Criminals can sell stolen credit card data and buy software and other tools on the black market to launch new infiltrations. Hackers may also have other aims, including goals related to foreign policy or espionage. Hackers linked to North Korea attacked Sony in 2014 (see FBI, 2014). An attack on computer systems at Saudi Arabia's aviation agency in December 2016 reportedly used data-clearing software like that used to attack Sony (see Chan, 2016). Such incidents may be matters of national security, especially when they have foreign government support.

Many intruders are technically sophisticated and have a nuanced understanding of a firm's operations. For example, in 2013, hackers used malware delivered over the Internet through a vendor's system to break into the IT system of Target, a retailer. Hackers planted the malware three months before they stole Target's credit card records (see Krebs, 2014).

Recent incidents have touched banks. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) in December 2016 confirmed several incidents with banks involving its payments messaging system. Hackers used stolen credentials to generate fraudulent messages authorizing payments to funnel cash to hackers. Although 80 percent of the investigated attempts failed, some banks still lost money (see Bergin and Finkle, 2016).

Even central banks are at risk. In February 2016, hackers broke into Bangladesh Bank and hacked its credentials to send payment messages over the SWIFT network. They stole $81 million (see Bangladesh Case Study Illustrates Vulnerabilities). In December 2016, Russia's central bank reported that hackers stole about $31 million during the year from its correspondent banks (see Reuters, 2016).

Cybersecurity Incidents Could Threaten Financial Stability in Three Ways

Cybersecurity threats impose direct costs on firms. Those costs include loss of funds or customer records, added IT spending, remediation costs, reputation costs, and legal expenses.

Cybersecurity incidents also can pose a broader risk to financial stability. Financial firms work within complex networks and rely on electronic transactions, often on a rapid just-in-time basis. They are linked digitally to each other and to nonfinancial entities, including third-party service providers. Some markets and systems depend on a few key firms. Other markets and systems may be decentralized, either by design or because participation is not concentrated. Hackers may have a hard time spreading havoc in those operations. However, defending a decentralized network with many entry points can be difficult (see Rosengren, 2015).

A cybersecurity incident that disrupts a systemically important firm could have spillover effects. For example, a large troubled firm could default on contracts or impair market liquidity. OFR analysis suggests three channels through which cybersecurity events can threaten financial stability (see **Figure 1**):

1 **Lack of substitutability.** The financial services industry relies on a robust IT infrastructure to complete transactions and move payments. In many financial networks, a few firms or utilities serve as hubs. Their services would be hard to replace if lost or interrupted. These hubs include central banks; custodian banks; and payment, clearing, settlement, and messaging systems. Problems at key hubs can raise stability concerns. To date, these cases have typically involved a type of operational risk other than cyber risk. For example, in 1985 the Bank of New York received a $23 billion discount window loan from the Federal Reserve to avert market spillovers from a software failure at the bank that left it unable to redeliver securities it had received from other institutions as an intermediary (see Ennis and Price, 2015). This was the largest ever discount window loan at the time. A cyber incident involving a financial firm providing key services to other market participants could create similar systemic risks. Policies that foster financial system redundancy can reduce those risks. Regulators should consider such policies.

2 **Loss of confidence.** Hackers often target customer account information and financial assets. Most of these hacks have been one-off events, hurting just the victim firm and its customers. However, a wide-reaching theft could cause a broader loss of confidence. In South Korea in 2014, hackers stole customer names, credit card data, and phone numbers from a credit rating firm. The news led many customers to call or visit their banks, where they demanded to know if their information was secure. Many people cancelled credit cards. However, the incident did not grow into a full-blown banking crisis (see Sang-Hun, 2014).

Figure 1: How Cybersecurity Incidents Could Threaten Financial Stability

Sources: Her Majesty's Government and Marsh Ltd. (2015); Securities and Exchange Commission; OFR analysis

3 **Loss of data integrity.** The integrity of financial data is critical. Many financial markets work on a just-in-time basis. Financial firms need robust backup data that can be recovered soon after a cybersecurity incident. However, tradeoffs exist between recovering quickly and ensuring that recovered data are safe, accurate, and do not spread cyber risks, especially for markets that process orders rapidly. Data corruption could disrupt market activity and may be hard to reverse or recover from (see IOSCO, 2016).

Financial Firms Increasingly See Cybersecurity Incidents as a Key Risk

Half of bank chief risk officers and board members who responded to a 2016 survey placed cyber risk among the top issues needing their attention (EY and IIF, 2016). In another survey in 2015, two-thirds of global regulators and

Bangladesh Case Study Illustrates Vulnerabilities

The recent event in Bangladesh illustrated the potential financial stability risks cyber incidents pose.

Hackers used stolen SWIFT credentials to access the central bank and steal funds. According to public reports, after the infiltration, the hackers sent fraudulent payment messages using the SWIFT network. The messages were authenticated over SWIFT as legitimate messages of Bangladesh Bank.

The intruders did not compromise the SWIFT network, which carries more than 25 million payment messages a day among banks. Still, the incident highlights concerns about end-user security and network security.

The hackers tried to steal $1 billion. They got $81 million. Bangladesh had foreign exchange reserves of $27 billion at the end of 2015. A loss of $1 billion in reserves could have shaken confidence and threatened financial stability (see Paul, 2016). As of late 2016, Bangladesh Bank was expecting to recover $45 million of the $81 million stolen.

This breach showed the patience, skill, and global reach of the hackers. They placed fraudulent orders on a Thursday. That timing delayed discovery of the theft until after the weekend (see Mallet and Chilkoti, 2016). The malware suppressed the transaction logs used for confirmation and reconciliation, which hid the fraud and gave the thieves time to launder the stolen money (see SWIFT, 2016; Shevchenko, 2016). The stolen funds moved through banks in the Philippines and were withdrawn from Philippine casinos.

This incident showed that hackers can bypass complex business controls. It also showed that cybersecurity threats require responses at both the end-user level and the network level. SWIFT has since started a customer security program. SWIFT is also developing new tools and raising awareness on best practices and security features in its products (see SWIFT, undated). In addition, SWIFT said it may sanction noncompliant institutions by reducing or suspending access to its network (see Arnold, 2016).

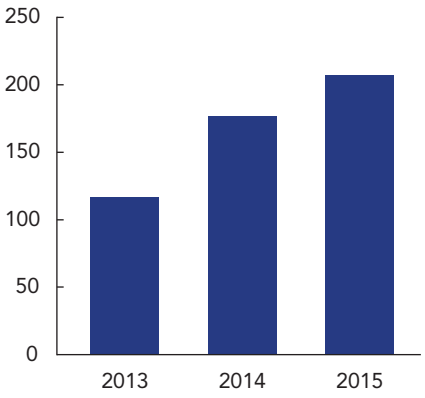
market experts placed cybersecurity threats second among financial stability risks (see Worner, 2015). Also, an OFR review found that banks more often included cyber risks and operational risks in the scenarios they submitted in their annual stress tests since 2013. Banks prepare these scenarios as part of mid-cycle stress tests required under the Dodd-Frank Act.

A number of U.S. financial firms reported cybersecurity as a key risk in Form 10-K filings submitted to the Securities and Exchange Commission (SEC) in 2015 and reviewed by the OFR. The OFR review covered U.S. global systemically important banks, global systemically important insurers, central counterparties, and government-sponsored enterprises. Cyber references in 2015 Form 10-Ks were nearly double those in 2013 10-Ks (see **Figure 2**). These filings typically note that cyber incidents can come from a variety of bad actors. Incidents can spread cyber risks to financial firms when clients, third-party service providers, or retail partners are targeted.

Financial firms include cybersecurity preparedness in their risk management. According to a 2016 survey, about 40 percent of financial services firms in North America with more than $1 billion in revenue budgeted $10 million or more for information security (see PricewaterhouseCoopers, 2016). The financial services industry budgeted more for information security than most other industries (see **Figure 3**).

Figure 2. Mentions of "Cyber" in Large U.S. Financial Firms' Form 10-Ks (number)

Cyber risk is rising for systemically important U.S. financial firms and government-sponsored enterprises

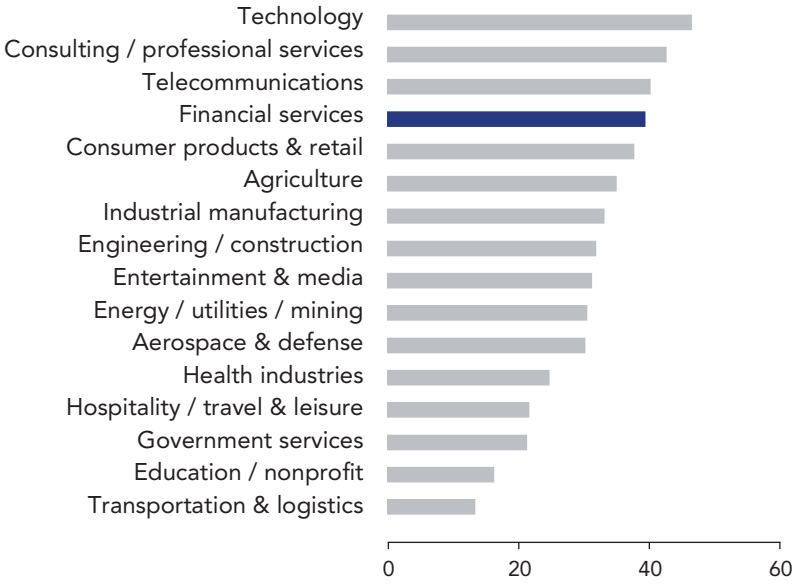


Note: Form 10-Ks for firms in the sample grew on average 2.5 percent in page count from 2013 to 2015.

Sources: Securities and Exchange Commission Form 10-K, OFR analysis

Figure 3. North American Firms that Budget $10 Million or More for Information Security, by Industry (percent)

Large financial firms make significant investments in information security compared with many other industries



Note: Survey results as of June 12, 2015. Responses from firms with more than $1 billion in gross revenue.

Source: PricewaterhouseCoopers (2016)

According to a 2016 survey, about 40 percent of financial services firms in North America with more than $1 billion in revenue budgeted $10 million or more for information security.

Using the National Institute of Standards and Technology cybersecurity framework as a starting point

- Overall security strategy.
- Security standards and baselines for third-party service providers.
- A chief information security officer in charge of IT security.
- Formal collaboration with others in the industry.
- Active participation of the board of directors in the firm's cybersecurity strategy.

Many firms use the cybersecurity framework of the National Institute of Standards and Technology as a starting point (see Fitzgibbons, 2016). The framework is voluntary. According to a 2016 survey, more than half of large financial firms had some safeguards that align with the framework:

- Overall security strategy.
- Security standards and baselines for third-party service providers.
- A chief information security officer in charge of IT security.
- Formal collaboration with others in the industry.
- Active participation of the board of directors in the firm's cybersecurity strategy.

The financial services industry is working with regulators to be able to quickly respond to cybersecurity threats and recover from cyber incidents (see **Figure 4**). One industry program, Soltra, is developing a platform for firms to share threat intelligence (see DTCC, 2015).

Industry, government, and academia have also held exercises to boost the readiness of the financial services industry to respond to systemwide incidents. These exercises are called the Quantum Dawn series (see Deloitte and SIFMA, 2015). Two other key programs are the Hamilton series of exercises, and international work with the United Kingdom through Operation Resilient Shield (see Treasury and HM Treasury, 2015; Waterman, 2016).

After these exercises, the financial services industry recently announced a data protection program called Sheltered Harbor. Sheltered Harbor is an industry-backed nonprofit group that covers U.S. retail banking and

Figure 4. Major Public and Private Groups Addressing Cyber Risks

Organization	Description
Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC)	Group of trade associations, financial utilities, and financial companies that works with the public sector on policy issues related to resilience and response to cybersecurity issues, natural disasters, and terrorism.
Financial and Banking Information Infrastructure Committee (FBIIC)	Group of federal and state financial regulators created after the 9/11 attacks to improve coordination and communication among regulators, enhance resilience of the financial sector, and promote public-private partnerships.
Financial Services – Information Sharing and Analysis Center (FS-ISAC)	Nonprofit center that provides member financial services firms with anonymous, global information sharing about cyber and physical threat intelligence.

Source: OFR analysis

brokerage firms. Sheltered Harbor supports a distributed data storage system. That is, data are not stored centrally. The purpose of Sheltered Harbor is to allow a financial firm to securely store customer account data and reconstitute those data, even if a cyber incident disrupted the firm's operations. Participants use a common set of data formats, encryption standards, and data storage standards (see FS-ISAC, 2016). The data are held in a separate data vault with a service provider or another financial firm. Sheltered Harbor gives member firms a layer of resilience beyond their own backup and recovery plans and systems.

Sheltered Harbor is now operating and the organization expects increased adoption during 2017. Its membership includes firms holding 60-70 percent of U.S. retail bank and brokerage accounts.

Cybersecurity Approaches of U.S. Financial Regulators Vary

U.S. regulators recognize the threat of cyber incidents to the firms they supervise. Regulators have emphasized cybersecurity threats in public statements and guidance. They have begun to develop specific assessment standards and set enforceable expectations and benchmarks. **Figure 5** lists some key U.S. financial regulatory guidance on cybersecurity.

Approaches to cyber risk differ among financial regulators. Risk profiles differ among types of financial firms and statutory authorities vary. Some regulators have set enforceable standards, while others have issued guidance.

Bank regulators conduct IT examinations that factor cybersecurity preparedness into stress testing, resolution planning, and safety and soundness supervision. The standards of the IT Examination Handbook used by bank regulators cover third-party vendors and contractors that provide key services to banks (see U.S. Congress, 2010). Bank regulators also introduced a voluntary cybersecurity assessment tool in June 2015. Banks may use it to assess their risk and cybersecurity preparedness (see FFIEC, 2015). The tool supplements existing standards for examining banks' IT management. It establishes a process that banks can use to assess their preparedness for several types of risk over time. However, the tool on its own is not an enforceable standard.

More recently, the Federal Reserve, Office of the Comptroller of the Currency (OCC), and Federal Deposit Insurance Corporation (FDIC) issued a proposed rule in October 2016 to set enhanced cybersecurity standards for large financial institutions. The proposed rule would apply to banks with more than $50 billion in assets, nonbank financial institutions and financial market utilities that are subject to Federal Reserve supervision, and third-party service providers. The proposed rule sets enforceable standards for the governance and management of cybersecurity risks. It also sets expectations for resilience and recovery (see Board of Governors, OCC, and FDIC, 2016). For example, the proposed rulemaking raises the

Figure 5. U.S. Financial Regulatory Guidance on Cybersecurity

Regulatory Body	Relevant Cybersecurity Guidance	Institution
Federal Financial Institutions Examination Council (FFIEC) member agencies (Consumer Financial Protection Bureau, Federal Deposit Insurance Corporation, Federal Reserve Board of Governors, National Credit Union Administration, Office of the Comptroller of the Currency, FFIEC State Liaison Committee)	Cybersecurity Assessment Tool and *IT Examination Handbook*	Banks
		Bank holding companies
		Federal savings associations
		Credit unions
Securities and Exchange Commission	Regulation SCI	Registered clearing agencies
		Stock and option exchanges
		Municipal Securities Rulemaking Board
		High-volume alternative trading systems
		Securities information processors
		Financial Industry Regulatory Authority
	Regulation S-P	Broker-dealers
		Investment companies
		Investment advisers
State insurance regulators via National Association of Insurance Commissioners (NAIC)	*Financial Condition Examiners Handbook* and *Market Regulation Handbook*	Insurers
Federal Housing Finance Agency	Advisory Bulletin 2014-05, Cyber Risk Management Guidance	Government-sponsored enterprises
		Federal Home Loan Banks
	Policy Guidance PG-01-002, Safety and Soundness Standards for Information	Government-sponsored enterprises
Commodity Futures Trading Commission	System Safeguards Testing Requirements	Designated contract markets
		Swap execution facilities
		Swap data repositories
	System Safeguards Testing Requirements for Derivatives Clearing Organizations	Derivatives clearing organizations
National Futures Association	Interpretive Notice 9070	Futures commission merchants
		Commodity trading advisors
		Commodity pool operators
		Introducing brokers
Financial Industry Regulatory Authority	Report on Cybersecurity Practices	Broker-dealers

Note: Several proposed rules are related to financial institution cybersecurity: the SEC's Adviser Business Continuity and Transition Plans Rule (June 2016); the Federal Reserve, Office of the Comptroller of the Currency, and Federal Deposit Insurance Corporation joint proposed rule for Enhanced Cyber Risk Management Standards (October 2016); and NAIC's Data Security Model Law (March 2016).
Source: OFR analysis

possibility of covered firms maintaining secure off-line storage for critical records formatted using defined data standards to facilitate recovery. The comment period on the proposed rule was extended to February 2017 given the range and complexity of issues.

The SEC's Regulation Systems Compliance and Integrity (SCI) mandates corrective action by covered firms after a cybersecurity incident or other operational risk event (see SEC, 2015). Covered firms include registered clearing agencies, alternative trading systems, and plan processors. The regulation went into effect in November 2015. Regulation SCI focuses on assessing firms' business continuity and disaster recovery abilities. It aims to assure recovery within two hours after an incident for critical systems, such as clearing and settlement. The regulation also requires covered firms to promptly notify regulators of an event. However, compared with bank regulators, the SEC has more limited authority over third-party vendors that sell services to its regulated firms (see FSOC, 2016). The SEC has also issued a draft rule that would set cybersecurity expectations for investment advisers.

In contrast with other regulators, insurance regulators focus on securing customer data. Criminals have targeted customer records in several hacks of health insurance firms. The National Association of Insurance Commissioners is concerned that more breaches of customer data could hurt consumer confidence. Customers could keep information from insurers, impeding the ability of insurers to assess risk. State regulators are starting baseline cyber assessments of insurers. State regulators also are working with insurers that had breaches. They drafted a model law for states that would set higher standards for data protection. This model law was available for public comment until September 2016. A final model law has not yet been published.

Approaches to cyber risk differ among financial regulators. Risk profiles differ among types of financial firms and statutory authorities vary.

The Commodity Futures Trading Commission (CFTC) issued a rule in September 2016 that established five types of cybersecurity testing requirements for derivatives clearing organizations, designated contract markets, swap execution facilities, and swap data repositories. In addition to requirements for risk assessment and testing for cybersecurity vulnerabilities, the rule mandates business continuity and recovery plans. The plans are designed to assure recovery by the next business day after a disruption.

In June 2016, the Committee on Payments and Market Infrastructures and the board of the International Organization of Securities Commissions (CPMI-IOSCO) proposed international guidelines on cyber resilience for financial market infrastructures (FMIs). The guidelines set expectations for FMIs to preempt cyber incidents, respond rapidly and effectively, and meet recovery objectives (see BIS and IOSCO, 2016). The guidance encourages FMIs to work toward same-day final settlement or real-time settlement, to reduce cyber risks. More timely final settlement would reduce the lag between transaction start and settlement and could lessen the disruption

from a cybersecurity incident. The Federal Reserve, SEC, and CFTC helped develop the guidance as members of CPMI-IOSCO. The rule that U.S. banking regulators proposed in October 2016 references the CPMI-IOSCO guidance. The Federal Reserve's existing risk management standards for systemically important financial market utilities (Regulation HH) give limited guidance on cyber risks. The CFTC and SEC have yet to propose rules to apply the CPMI-IOSCO guidelines for FMIs they supervise.

Conclusion

Strong Regulatory Progress but Opportunities for Improvement Remain

U.S. financial regulators are making meaningful progress in addressing cyber risks of individual firms. But firms and regulators broadly agree that addressing the channels through which cyber incidents could create systemic risks is just as important. Regulatory boundaries may limit regulators' perspectives on key parts of financial networks. Potential blind spots include third-party vendors, overseas counterparties, and cross-border service providers.

Financial regulators can build on their progress with a broader approach to cyber resilience that focuses on the many links among financial firms. Those links occur through systems for payments and settlements, counterparty credit relationships, and the use of common IT systems and platforms. They also occur through participation in financial markets.

The OFR sees three channels through which cybersecurity events can affect financial stability: (1) lack of substitutability, (2) loss of confidence, and (3) loss of data integrity. Regulators can benefit from more collaboration to develop a common lexicon and a shared risk-based approach. Regulators also could benefit from more standardized data on cyber incidents and financial firms' cybersecurity preparedness. More collaboration is already evident in some recently proposed rules. Regulators can work together to update cybersecurity standards and guidance.

Regulators and firms also need to keep working together to build capacity to recover from a cybersecurity incident. Cyber "stress tests" of industry-wide capabilities in information sharing, business continuity, and disaster recovery include exercises such as the Quantum Dawn and the Hamilton series.

Financial industry initiatives are emerging from those exercises to improve the recovery of the financial sector. Sheltered Harbor is a recent example. Regulators should continue to set expectations for recovery times for financial firms' critical systems and to validate firms' capacities for recovery. For example, the banking regulators' October 2016 proposed rulemaking sets recovery expectations. Regulators should continue to work with the industry to strengthen firms' ability to recover.

References

Arnold, Martin. "Swift Threat to Suspend Vulnerable Members." *Financial Times*, June 3, 2016. www.ft.com/cms/s/0/9af78732-28da-11e6-8ba3-cdd781d02d89.html#axzz4En4WBbpr (accessed Oct. 13, 2016).

Bank for International Settlements: Committee on Payments and Market Infrastructures and Board of the International Organization of Securities Commissions. *Guidance on Cyber Resilience for Financial Market Infrastructures.* Basel: BIS and IOSCO, June 2016. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf (accessed Oct. 20, 2016).

Bergin, Tom, and Jim Finkle. "SWIFT Confirms New Cyber Thefts, Hacking Tactics." Reuters, Dec. 12, 2016. www.reuters.com/article/us-usa-cyber-swift-exclusive-idUSKBN1412NT (accessed Dec. 13, 2016).

Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and Federal Deposit Insurance Corporation. *Enhanced Cyber Risk Management Standards.* Joint Advanced Notice of Proposed Rulemaking. Washington: Board of Governors, OCC, and FDIC, Oct. 19, 2016.. https://www.federalreserve.gov/newsevents/press/bcreg/20161019a.htm (accessed Oct. 28, 2016).

Board of the International Organization of Securities Commissions. *Cyber Security in Securities Markets – An International Perspective.* Madrid: IOSCO, April 2016. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf (accessed Dec 13, 2016)

Chan, Sewell. "Cyberattacks Strike Saudi Arabia, Harming Aviation Agency." *The New York Times*, Dec. 1, 2016. www.nytimes.com/2016/12/01/world/middleeast/saudi-arabia-shamoon-attack.html?_r=0 (accessed Dec. 1, 2016).

Deloitte Advisory and Securities Industry and Financial Markets Association. *Quantum Dawn 3 After-Action Report*. Washington: Deloitte and SIFMA, Nov. 23, 2015. www.fbiic.gov/public/2015/Quantum_Dawn_3_AAR_Public_Report.pdf (accessed Oct. 20, 2016).

Depository Trust & Clearing Corp. "New Soltra Network Offering to Connect and Coordinate Cyber Threat Intelligence Sharing." Press Release: DTCC, Oct. 12, 2015. www.dtcc.com/news/2015/october/12/new-soltra-network-offering-connect-coordinate-cyber-threat-intelligence (accessed Oct.20, 2016).

Ennis, Huberto, and David Price. "Discount Window Lending: Policy Trade-offs and the 1985 BoNY Computer Failure." Economic Brief no. 15-05. Richmond, Va.: Federal Reserve Bank of Richmond, May 2015. https://www.richmondfed.org/~/media/richmondfedorg/publications/research/economic_brief/2015/pdf/eb_15-05.pdf (accessed Oct. 20, 2016).

Federal Bureau of Investigation. *Update on Sony Investigation*. Press Release: FBI, Dec. 19, 2014. https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation (accessed Sept. 23, 2016).

Federal Financial Institutions Examination Council. *Cybersecurity Assessment Tool*. Online Content: FFIEC, June 2015. https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf (accessed Sept. 7, 2016).

Financial Services Information and Analysis Center and Sheltered Harbor. Sheltered Harbor Fact Sheet. Washington: FS-ISAC, Nov. 23, 2016. https://www.fsisac.com/sites/default/files/news/SH_FACT_SHEET_2016_11_22_FINAL3.pdf (accessed Jan. 26, 2016).

Financial Stability Oversight Council. *Update on Review of Asset Management Products and Activities*. Washington: FSOC, April 18, 2016. www.treasury.gov/initiatives/fsoc/news/Documents/FSOC%20Update%20on%20Review%20of%20Asset%20Management%20Products%20and%20Activities.pdf (accessed Oct. 28, 2016).

Fitzgibbons, Russell. *Views on the Framework for Improving Critical Infrastructure Security.* Herndon, Va.: Financial Services Sector Coordinating Council, Feb. 9, 2016. http://csrc.nist.gov/cyberframework/rfi_comments_02_2016/20160219_Financial_Services_Sector_Coordinating_Council.pdf (accessed Oct. 13, 2016).

Her Majesty's Government and Marsh. *UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk*. London: Her Majesty's Government and Marsh, March 2015. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf (accessed Oct. 28, 2016).

Krebs, Brian. "A First Look at the Target Intrusion, Malware." Online Content: *Krebs on Security*, Jan. 15, 2014. http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/ (accessed Sept. 6, 2016).

Mallet, Victor, and Avantika Chilkoti. "How Cyber Criminals Targeted Almost 1BN in Bangladesh Bank Heist." *Financial Times*, March 18, 2016. www.ft.com/cms/s/0/39ec1e84-ec45-11e5-bb79-2303682345c8.html#axzz4En4WBbpr (accessed Oct. 13, 2016).

Office of Financial Research. *2015 Financial Stability Report*. Washington: OFR, Dec. 15, 2015. www.financialresearch.gov/financial-stability-reports/files/OFR_2015-Financial-Stability-Report_12-15-2015.pdf (accessed Sept. 6, 2016).

Paul, Ruma. "Bangladesh hopes to recover $30 million more from cyber heist." Reuters, Nov. 14, 2016. http://uk.reuters.com/article/us-cyber-heist-bangladesh-idUKKBN1390JN (accessed Nov. 16, 2016).

PricewaterhouseCoopers. *The Global State of Information Security Survey 2016*. Online Content: PricewaterhouseCoopers, 2016. www.pwc.com/gx/en/issues/cyber-security/information-security-survey/data-explorer.html (accessed Sept. 7, 2016).

Reuters. "Russian central bank, private banks lose $31 mln in cyber attacks." Reuters, Dec. 6, 2016. www.reuters.com/article/us-russia-cen-bank-cyberattack-idUSKBN13R1TO?-feedType=RSS&feedName=technologyNews (accessed Dec. 13, 2016).

Rosengren, Eric. "Cyber Security and Financial Stability." Speech to the Basel Committee on Banking Supervision, Cape Town, Jan. 30, 2015. www.bostonfed.org/news/speeches/rosengren/2015/013015/013015text.pdf (accessed Sept. 6, 2016).

Sang-Hun, Choe. "Theft of Data Fuels Worries in South Korea." *The New York Times*, Jan. 20, 2014. www.nytimes.com/2014/01/21/business/international/theft-of-data-fuels-worries-in-south-korea.html?_r=1 (accessed Oct. 14, 2016).

Securities and Exchange Commission. *Regulation Systems Compliance and Integrity*. Final Rule. Washington: SEC, Feb. 3, 2015. https://www.sec.gov/rules/final/2014/34-73639.pdf (accessed Oct. 13, 2016).

Shevchenko, Sergei. "Two Bytes to $951M." *BAE Systems Threat Research Blog*, April 25, 2016. http://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html (accessed Jan. 24, 2017).

Society for Worldwide Interbank Financial Telecommunication. "Customer Communication: Customer Security Issues." Press Release: SWIFT, May 13, 2016. https://www.swift.com/insights/press-releases/swift-customer-communication_customer-security-issues (accessed Jan. 24, 2017).

Society for Worldwide Interbank Financial Telecommunication. *Customer Security Programme (CSP)*. Online Content: SWIFT, undated. https://www.swift.com/myswift/customer-security-programme-csp_/programme-description (accessed Jan. 24, 2017).

Symantec Corp. *Internet Security Threat Report*. Herndon, Va.: Symantec, April 2016. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf (accessed Oct. 13, 2016).

U.S. Congress. *Bank Service Company Act, 12 USC 1867 (c)*. Washington: Government Printing Office, 2010. http://uscode.house.gov/view.xhtml?path=/prelim@title12/chapter18&edition=prelim (accessed Oct. 28, 2016).

U.S. Congress. *Consolidated Appropriations Act 2016*. 114th Congress, 1st Session. Washington: Government Printing Office, 2016. https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf (accessed Oct. 14, 2016).

U.S. Department of the Treasury and Her Majesty's Treasury. *Joint Statement from the U.S. Department of The Treasury and Her Majesty's Treasury*. Press Release: Treasury and HM Treasury, Nov. 12, 2015. https://www.treasury.gov/press-center/press-releases/Pages/jl0262.aspx (accessed Oct. 28, 2016).

Waterman, Shaun. "Bank Regulators Briefed on Treasury-led Cyber Drill." *FedScoop*, July 20, 2016. http://fedscoop.com/us-treasury-cybersecurity-drill-july-2016 (accessed Sept. 27, 2016).

White House. *Critical Infrastructure Security and Resilience*. Presidential Policy Directive (21). Washington: White House, Feb. 12, 2013. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed Oct. 28, 2016).

Worner, Shane. "A Survey of Securities Market Risk Trends 2015: Methodology and Detailed Results." Staff Working Paper no. 7. Madrid: International Organization of Securities Commissions, December 2015. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD516.pdf (accessed Sept. 7, 2016).