September 30, 2015

Cybersecurity Update: Heightened Concerns, Legal and Regulatory Framework, Enforcement Priorities, and Key Steps to Limit Legal and Business Risks

Recently reported network intrusions and disruptions, thefts of electronic data, and other significant cyber incidents have impacted millions of people and exposed the increased and continuing risks for businesses and government agencies. These incidents have transformed the cyber threat from a theoretical problem into a clear and present danger. In a recent survey of U.S. executives, security experts, and others from the public and private sectors, "76% of respondents said they are more concerned about cybersecurity threats this year than in the previous 12 months."[1]

Cybersecurity has become a priority for lawmakers and law enforcement agencies, regulators and the White House. It has become part of the public consciousness, and across corporate America, the cyber threat has evolved from an information-technology problem that could be delegated to information-technology personnel to a key business and governance risk requiring the careful attention of boards and senior leadership.

In this memo, we: (1) provide an overview of this new reality; (2) address the nature and sources of the cyber threat; (3) discuss the potential financial, legal, and other consequences of cyber incidents; (4) present the legal and regulatory framework applicable to cybersecurity issues; (5) offer best practices and recommendations for boards and senior management; and (6) examine recent resources tailored to the particular cybersecurity risks facing financial institutions.

TABLE OF CONTENTS

Introduction

Cyber-related events during the last several months illustrate the current reality—cybersecurity is a growing business and governance risk that requires immediate and regular attention by business leadership:

- When the operations of the New York Stock Exchange and United Airlines were suddenly halted due to technological glitches, fears of a cyberattack quickly spread. In response, the NYSE issued a statement (on Twitter, no less) assuring the public that the outage resulted from "an internal technical issue and is not the result of a cyber breach."[2] Similar messages were delivered the same day by the White House ("[T]here is no indication that malicious actors are involved in these technology issues."),[3] the Director of the Federal Bureau of Investigation ("FBI") ("We do not see any indication of a cyber breach or a cyber attack."),[4] and the Secretary of Homeland Security ("[T]he malfunctions at United and the stock exchange were not the result of any nefarious actor."), who also reiterated that "cybersecurity is a top priority for me, for the President, and for this Administration."[5]

- The Department of Justice (the "DOJ") announced charges against nine people in connection with an international ring of organized cybercriminals who hacked into the networks of business newswires to steal press releases prior to their public release in order to trade on the stolen inside information.[6]

- Citing the "increasing barrage of cyber attacks on financial firms," the U.S. Securities and Exchange Commission (the "SEC") announced charges last week against a St. Louis-based investment adviser that the SEC alleged had "failed to establish the required cybersecurity policies and procedures in advance of a breach."[7]

- The Director of the U.S. Office of Personnel Management ("OPM") was forced to resign in the wake of a massive data breach that compromised sensitive personal information of millions of federal employees with security clearances.[8]

- *Wired* magazine documented a group of hackers remotely manipulating a vehicle's air conditioning, stereo controls, brakes, and transmission using a laptop miles away, and as *The New York Times* has reported, "[t]hough automakers say they know of no malicious hacking incidents so far, the risks are real."[9] Just days later, Fiat Chrysler announced a recall of 1.4 million vehicles due to "a potential cybersecurity flaw," reportedly prompting an investigation by the National Highway Traffic Safety Administration.[10]

- FBI Director James Comey warned that that the FBI is "picking up signs of increasing interest" among terrorist groups in a cyberattack against the United States.[11]

- The former Superintendent of the New York Department of Financial Services called cybercrime "a huge threat to our financial system" and predicted that there would be "a lot of action around cybersecurity and the regulation in that area."[12]

- The FBI arrested several people in the United States and Israel this summer who, according to several news reports, are linked to a data breach at one of the country's largest banks.[13]

More thought, attention, and resources are being devoted to cybersecurity than ever before. The government has issued extensive guidance addressing cybersecurity, and lawmakers are working to enhance the ability of the public and private sectors to defend against and respond to the cyber threat. The purpose of this memo is to outline the threat, the applicable legal and regulatory framework, and key steps to mitigate the legal and business risks posed by the brave new cyber world. This memo also examines two recent developments of particular relevance to the financial industry: a July 2015 Government Accountability Office ("GAO") Report on cybersecurity at banks and other depository institutions, and the Cybersecurity Assessment Tool recently developed by the Federal Financial Institutions Examination Council ("FFIEC").

As described below, it is essential that businesses—particularly those that collect and transmit business and customer data online—conduct periodic risk assessments; undertake comprehensive preventative measures to fortify defenses; develop effective employee training and education, policies, and controls; and design robust incident response plans to ensure maximum preparedness in the event of a breach. Although the risk of a cyber incident cannot be eliminated, companies can meaningfully mitigate the risk and resulting harm by preparing for an incident before it occurs.

The Nature and Sources of the Threat

According to a February 2015 worldwide threat assessment by the United States intelligence community, "[c]yber threats to US national and economic security are increasing in frequency, scale, sophistication, and severity of impact."[14] The Director of National Intelligence has predicted that "[r]ather than a 'Cyber Armageddon' scenario that debilitates the entire US infrastructure," it is more likely that there will be "an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time."[15] Corporations across a broad spectrum of industries often find themselves the targets of these low-to-moderate level cyberattacks, which can manifest in many different forms.

Likely Business Targets

The financial industry consistently has been one of the sectors most likely to be the target of a cyberattack. According to the 2015 IBM Cyber Security Intelligence Index, the finance industry had the highest incident rate across surveyed industries in 2013 and 2014, accounting for approximately one-quarter of the private-sector incidents observed by IBM during each of those years.[16] That finding is consistent with those of other cybersecurity providers and researchers. Verizon, for example, reported that among private

industries, the financial services industry was second only to the information industry in the number of cyberattacks,[17] and Mandiant identified financial services as one of the top three most targeted industries, together with retail and business and professional services.[18]

The Sources of External Threats

The primary sources of external threats to companies and organizations are: "(1) nation states with highly sophisticated cyber programs (like Russia or China), (2) nations with lesser technical capabilities but possibly more disruptive intent (such as Iran or North Korea)," (3) individual or organized cybercriminals who typically act for financial gain, and (4) so-called "hacktivists" who are motivated by ideological objectives.[19]

There is evidence that large banks are "more likely to be targeted by nation-states and hacktivists," while smaller depository institutions, which typically have less sophisticated defense mechanisms, are more commonly targeted by financially-motivated cybercriminals.[20] Financially-motivated cybercriminals traditionally have sought banking credentials, credit card or other personal information from a variety of businesses, but the type of information being targeted—as well as the means of monetizing that information—is expanding. Recently, the DOJ announced the indictment of nine people in a large-scale, international scheme to hack into business newswires, steal yet-to-be published press releases containing confidential financial information, and then illegally trade on the basis of that stolen information.[21] Along similar lines, Mandiant recently profiled the activities of a sophisticated group of cybercriminals who have been targeting confidential M&A information from public companies, presumably to engage in insider trading.[22] In addition, the Director of the FBI expressed growing concern about terrorist groups looking to carry out a cyberattack.[23]

The Blurring of State and Non-State Actors

The lines between state-sponsored and other cyber actors have blurred, as the techniques and motives of cybercriminals and state actors have increasingly overlapped.[24] State actors have expanded beyond traditional espionage and have also "undertaken offensive cyber operations against private sector targets" to advance political, foreign policy or economic objectives, or to seek "retribution for perceived wrongs."[25] North Korea, for example, launched a highly destructive attack against Sony Pictures Entertainment in apparent retaliation for its planned release of a satirical film depicting the assassination of Kim Jong-un.[26] It is widely suspected—although the U.S. has officially declined to confirm—that China was behind the recent OPM hack, which resulted in the theft of sensitive information for millions of federal employees and potentially compromised the identities of intelligence officers secretly stationed abroad.[27] China has also been linked to both a prolonged intrusion at *The New York Times*[28] and the seizing of millions of electronic records held by U.S. health insurer Anthem.[29] Five Chinese military hackers were charged with economic espionage last year for allegedly hacking into the networks of private entities in America to steal information "that would be useful to their competitors in China, including state-owned enterprises."[30] Then-Attorney General Eric Holder described it as "the first ever charges against a state actor for this type

of hacking."[31] It can sometimes be difficult to distinguish between state and non-state actors within the same country when those "varied actors actively collaborate, tacitly cooperate, condone criminal activity that only harms foreign victims, or utilize similar cyber tools."[32]

The Range of External Attacks

The range of objectives motivating cyberattackers has resulted in a range of different types of attacks against businesses. In 2012 and 2013, for example, dozens of financial institutions were subjected to coordinated and sustained distributed denial-of-service, or DDoS, attacks.[33] Those attacks caused disruptions to online banking functions, but resulted in no reported losses of personal information, suggesting a lack of any pecuniary motive.[34] Some government officials and security researchers attributed the attacks to the government of Iran, suggesting the attacks may have been "in retaliation for economic sanctions and online attacks by the United States,"[35] while others have attributed the DDoS attacks to a group of hacktivists in Iran.[36]

In the summer of 2014, one of the largest U.S. banks suffered a data breach that compromised account information belonging to over 80 million households and small businesses.[37] It was reported that customer email addresses, home addresses, and telephone numbers were compromised, but that no customer funds were taken.[38] The DOJ announced arrests this summer of several individuals in the U.S. and abroad who reportedly were linked to this breach.[39]

In two of the largest financially-motivated cyberattacks, in 2013 and 2014, Target and Home Depot were victims of data breaches that involved the theft of credit card data of more than 40 million customers and 56 million customers, respectively.[40] And aside from these large-scale attacks, banks routinely experience so-called "account takeovers" in which cybercriminals surreptitiously obtain victims' banking credentials and then direct wire transfers or other withdrawals from the victims' accounts.[41] The methods used to obtain the victims' banking credentials vary, but often include phishing emails or luring victims into unwittingly installing malware on their computers that enables the perpetrator to steal their banking information.[42]

More recently, healthcare companies—which maintain extensive records of personal information—have become victims of the so-called mega-breaches that had been affecting the retail sector. In February 2015, for example, Anthem, "the second-largest health insurer in the United States," announced that hackers stole information regarding tens of millions of its customers from a database containing up to 80 million customer records.[43]

The Tools of External Attacks

The methods of carrying out these attacks vary in their degree of sophistication. Although certain actors, particularly state-sponsored actors, have become increasingly more sophisticated, phishing and other relatively unsophisticated methods remain common, and employee errors and supply-chain

vulnerabilities continue to be responsible for many cyber incidents. The recently-indicted hackers who allegedly stole press releases in order to trade on inside information used phishing emails, among other methods, to infiltrate the networks of the business wires.[44]

Another factor contributing to and compounding the cyber threat is the proliferation of widely-available hacking tools, which increasingly enable virtually anyone, anywhere in the world, to carry out cyberattacks. The DOJ announced criminal charges last year in a case involving the sale of malware to thousands of people around the world who, for only $40, could surreptitiously take over a victim's computer and then spy on their victims through their web cameras, steal files and account information, log victims' key strokes, and utilize the infected computers to carry out DDoS attacks.[45]

Threats From Within

Aside from these sources of external threats, insiders present another source of risk, accounting for more than 50% of cyber incidents by some estimates.[46] Data breaches caused by insiders often can be more inadvertent than malicious.[47]

Further highlighting the vulnerabilities created by employees, data collected from sanctioned tests involving the distribution of over 150,000 phishing emails "showed that nearly 50% of users open e-mails and click on phishing links within the first hour" of receiving them.[48] This has important implications for the design of cybersecurity programs, reinforcing the need to incorporate effective employee training and education into any cybersecurity program. This is addressed in more detail below.

Financial, Legal and Other Implications of Cyber Incidents

The direct financial costs resulting from a significant cyber incident can be substantial. Target, for example, reported that as of May 2, 2015, it had incurred $256 million in data-breach expenses since its 2013 data breach in which hackers stole the credit card information of millions of customers.[49] Sony estimated that the breach of its PlayStation Network, which compromised the information of millions of users, would cost the company more than $170 million,[50] and the Sony Pictures Entertainment hack in connection with the film "The Interview" was projected to cost the company hundreds of millions of dollars, including lost revenue from the decision to pull the film's release from theaters.[51]

Victim companies also face litigation risks and intangible and less-quantifiable harms, including reputational damage, loss of consumer confidence, disruption of business operations, destruction of files, drops in stock price, and even the potential for embarrassment—such as when personal emails are released to the public by hackers.[52]

Private Litigation Risks

In the wake of a significant cyber incident, companies—and their directors and officers—can face a flurry of private lawsuits from a range of different constituencies: individual consumers whose personal information has been compromised, shareholders alleging failures by the board and senior leadership in preparing for and/or responding to cyberattacks, and other third-parties potentially affected by a breach, such as banks and credit card companies.

Target, for example, faced dozens of lawsuits after the data breach that compromised the credit/debit card and other personal information belonging to as many as 100 million consumers. As in other breach cases, the consumer-plaintiffs asserted violations of state consumer protection and state data-breach statutes, as well as common law claims of negligence, breach of implied contract, bailment, and unjust enrichment.[53] The plaintiffs' factual allegations related to the company's conduct pre- and post-breach, including, for example, that Target allegedly failed to (1) "take adequate and reasonable measures to ensure its data systems were protected," (2) "take available steps to prevent and stop the breach from ever happening," (3) "disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard customers' financial account and personal data," and (4) "provide timely and adequate notice of the Target data breach."[54]

The multi-district consumer litigation was consolidated in the District of Minnesota, and in March 2015, following the denial of the defendant's motion to dismiss, the District Court preliminarily approved a settlement of the consumer litigation.[55] The proposed settlement requires Target to pay $10 million to consumers who used credit or debit cards at Target during the relevant time period and to implement various security measures to protect customer data, including: appointing a chief information security officer, creating metrics to track and maintain information security, and offering security training to its employees.[56]

According to published reports, Target subsequently reached a proposed $19 million settlement to reimburse financial institutions for the costs they incurred from the breach, such as reimbursing fraudulent charges and reissuing credit and debit cards.[57] The financial institutions had alleged violations of a Minnesota credit-card statute, negligence, and negligent representation by omission for failing to disclose information-security weaknesses. The settlement was derailed in May of this year, however, after failing to receive the required 90% participation rate from issuers.[58] In August, Target reached a settlement with Visa Inc. and the banks that issue Visa cards for up to $67 million.[59] Another group of financial institutions was recently certified as a class in federal court in the District of Minnesota, allowing other financial institutions the opportunity to join the suit against Target.[60]

Derivative shareholder litigation against Target's directors remains pending.[61] The shareholder plaintiffs have asserted claims for, among other things, breach of fiduciary duty, waste of corporate assets, and

gross mismanagement, and like the consumer plaintiffs, they rely on allegations concerning the defendants' supposed pre-breach failure to insure adequate safeguards and their post-breach response.[62]

Risks of Enforcement Proceedings or Public Inquiries

In addition to private lawsuits from these various constituencies, companies that are victims of a cyber incident can also face investigations and enforcement actions from a wide array of federal and state regulators and law enforcement agencies, as discussed in greater detail below. Cybercrime creates a somewhat unique situation in which a company that is a victim of an attack may at the same time be viewed by regulators as a subject of a government investigation. In the case of a significant breach, the possibility also exists that a company may be the subject of a Congressional inquiry and its executives could be called to testify.[63]

Risks to Senior Leadership

The recent wave of cyberattacks also has placed great pressure on organizations to hold management accountable for perceived lapses. Last year, Target's board of directors ousted the company's CEO following its data breach, marking the first time a CEO has been removed due to a cyber incident.[64] In addition, Institutional Shareholder Services ("ISS") took the unusual step of recommending that Target shareholders vote against seven of the ten directors (focusing on those who served on the audit and corporate-responsibility committees) for taking insufficient steps to ensure that Target's systems were fortified against security threats.[65] And the director of the OPM was forced to resign this summer in the wake of a massive data breach that compromised the personal information of more than 20 million federal employees.[66]

These consequences have served to reinforce the warning from one SEC Commissioner that "boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril."[67]

Regulatory Requirements and Enforcement Priorities

A wide variety of federal and state regulators and law enforcement agencies are increasingly directing their attention toward cybersecurity. The DOJ, SEC, Financial Industry Regulatory Authority ("FINRA"), Federal Communications Commission ("FCC"), U.S. Department of Health & Human Services ("HHS"), Federal Trade Commission ("FTC"), a number of state attorneys general, and federal bank regulators have enhanced their emphasis on cybersecurity and, in many cases, specifically identified cybersecurity as a priority. Organizations across sectors should therefore expect both increased rulemaking and enforcement activity.

The U.S. Department of Justice and Federal Law Enforcement Agencies

A number of federal agencies charged with law enforcement and prosecution have increasingly focused on cybersecurity and have dedicated significant resources to pursuing and prosecuting cybercrime. The

Criminal Division of the DOJ created the Cybersecurity Unit within the Computer Crime and Intellectual Property Section in December 2014 "to serve as a central hub for expert advice and legal guidance regarding how the criminal electronic surveillance and computer fraud and abuse statutes impact cybersecurity."[68] In April 2015, the Cybersecurity Unit released its recommended Best Practices for Victim Response and Reporting of Cyber Incidents "to assist organizations in preparing a cyber incident response plan and, more generally, in preparing to respond to a cyber incident."[69] The Cybersecurity Unit also is "helping to shape cyber security legislation" and "engag[ing] in extensive outreach to the private sector to promote lawful cybersecurity practices."[70] In addition to the Cybersecurity Unit, many U.S. Attorney's Offices across the country have allocated resources to investigating and prosecuting cybercrime.

The FBI has identified cybersecurity as one of the agency's top three priorities, and has instituted a "set of technological and investigative capabilities and partnerships" to assist in its efforts to combat cybercrime, including: a Cyber Division, "[s]pecially trained cyber squads at FBI headquarters and in each of [the] 56 field offices," cyber action teams, 93 Computer Crimes Task Forces, and partnership with other federal agencies such as the Department of Defense and Department of Homeland Security.[71] The U.S. Secret Service, within the Department of Homeland Security ("DHS"), maintains a national network of more than 35 Electronic Crimes Task Forces with a "focus on identifying and locating international cyber criminals connected to cyber intrusions, bank fraud, data breaches, and other computer-related crimes."[72]

Federal prosecutors have recently brought a number of significant criminal cases targeting cybercrimes. Federal prosecutors announced charges last month against nine stock traders and computer hackers who allegedly reaped as much as $100 million in illegal insider-trading profits "by conspiring to use information stolen from thousands of corporate press statements before their public release."[73] A month earlier, the DOJ announced that it had dismantled a major computer hacking forum called Darkode and charged 12 people associated with the forum.[74] Domestic law enforcement efforts to combat cybercrime have benefitted from an extraordinary degree of international cooperation rarely seen in other contexts. The Darkrode case, for example, was part of a coordinated effort by law enforcement authorities from 20 different countries, representing "the largest coordinated international law enforcement effort ever directed at an online cyber-criminal forum."[75] Similarly, the U.S. Attorney's Office in Manhattan brought charges last year in connection with the sale and use of "Blackshades" malware as part of a global law enforcement operation involving more than 90 arrests and other law enforcement actions in 19 countries.[76]

U.S. Securities & Exchange Commission

While SEC officials have at various times hinted at the prospect of additional cyber-related enforcement actions, the director of the SEC's Chicago Regional Office recently emphasized that "[c]ybersecurity . . . is an area where we have not brought a significant number of cases yet, but is high on our radar screen."[77] He pointed to two areas in particular on which the SEC is focused: cybersecurity controls and cyber-related disclosures.[78]

SEC Guidance for Public Companies

On the disclosure side, the SEC's Division of Corporation Finance (the "Corp Fin Division") has issued "disclosure guidance" to aid public companies in their cyber-related disclosures.[79] The guidance first addresses the potential disclosure of cybersecurity as a significant risk factor. In determining whether the risk rises to that level, companies should consider "prior cyber incidents and the severity and frequency of those incidents," as well as "the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption."[80] Where the cyber threat constitutes a material risk, the company should describe the type and severity of the risk, and should "avoid generic 'boilerplate' disclosure."[81] In some cases, that may require the disclosure of actual known or threatened cyber incidents.[82]

The Corp Fin Division's disclosure guidance also provides that if the costs or other consequences related to actual or potential cyber breaches "represent a material event, trend, or uncertainty," they should be addressed in a public company's MD&A section.[83] This too may require the disclosure of actual cyber incidents where, for example, the resulting costs are likely to be material or have led to a material increase in cybersecurity spending.[84] Since the SEC's disclosure guidance was first issued, the Corp Fin Division has issued a number of comment letters to public companies regarding their cybersecurity disclosures,[85] and speculation has emerged that the SEC is considering regulations requiring more specific disclosures surrounding cyber incidents.[86]

SEC Guidance for Registered Entities

Aside from the Corp Fin Division's disclosure guidance for public companies, the SEC addressed cybersecurity for regulated entities through the Division of Investment Management (the "IM Division"), which regulates investment companies, variable insurance products, and federally registered investment advisers,[87] and the Office of Compliance Inspections and Examinations ("OCIE"), which "administer[s] the SEC's nationwide examination and inspection program" for registered entities, including broker-dealers, transfer agents, investment advisers, investment companies, the national securities exchanges, and clearing agencies.[88]

The IM Division issued cybersecurity guidance that outlined steps for registered investment companies and registered investment advisers to consider.[89] The guidance recommends that these registered entities conduct periodic assessments; develop a strategy that is designed to prevent, detect, and respond to cybersecurity threats—including instituting preventative security measures and creating an incident response plan; and implement the strategy through written policies and procedures and training. [90] The guidance also recommends that funds and advisers assess the cybersecurity measures in place at relevant third-party service providers.[91]

On the examination front, OCIE announced the launch of a Cybersecurity Examination Initiative by issuing a Risk Alert in April 2014.[92] The 2014 Risk Alert offered a useful roadmap for the types of questions firms can expect to face during an examination. The Alert included, for example, a sample exam letter requesting information about past cyber incidents, cybersecurity governance, protection of firm networks and information, risks associated with remote customer access and funds transfer requests, risks associated with vendors and other third parties, detection of unauthorized activity, and methodology for identifying best practices.[93]

About 10 months later, in February 2015, OCIE released a follow-up Risk Alert providing summary observations from its examinations of 57 registered broker-dealers and 49 registered investment advisers conducted under the 2014 Initiative.[94] The 2015 Risk Alert provides data points from the OCIE's examinations that can be used to inform cybersecurity policies and practices.

For example, OCIE found a gap, particularly among investment advisers, when it comes to the level of scrutiny applied to cybersecurity at third-party vendors. While most of the examined firms performed risk assessments on a firm-wide basis, only 32% of the advisers required cybersecurity assessments of vendors with access to their networks, and even fewer (24%) incorporated requirements relating to cybersecurity risk into their contracts with vendors and business partners.[95] As cybercriminals have increasingly looked to exploit vulnerabilities at third-party vendors as a backdoor into companies' networks, companies should not overlook the need to apply the same type of rigor to outside vendors that they do to their own networks.[96] Efforts to fortify internal defenses are wasted if attackers can simply achieve the same result by taking advantage of weaknesses in cybersecurity at third-parties.

The 2015 Risk Alert also reported that over half of the examined broker-dealers (54%) and just under half of the examined advisers (43%) had received fraudulent emails seeking to transfer client funds.[97] A number of firms that experienced losses as a result of such fraudulent emails said that those losses were the result of employees not following identity authentication procedures.[98] These findings further highlight the importance of employee education and training as part of an effective cybersecurity program.

In September 2015, OCIE issued a new Risk Alert outlining the areas on which OCIE intends to focus in its second round of cybersecurity examinations, a process "which will involve more testing to assess implementation of firm procedures and controls."[99] The areas include governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response.[100]

SEC Rulemaking and Enforcement Activity

The SEC also has implemented rules that relate directly or indirectly to cybersecurity and have been—and likely will increasingly be—the basis for enforcement actions. The principal such regulation is Rule 30 of Regulation S-P (referred to as the "Safeguard Rule"), which requires that brokers, dealers, investment companies, and registered investment advisors develop and implement written policies and procedures

reasonably designed to "(a) [i]nsure the security and confidentiality of customer records and information; (b) [p]rotect against any anticipated threats or hazards to the security or integrity of customer records and information; and (c) [p]rotect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."[101] The Safeguard Rule has been the basis for enforcement actions against firms and individual executives for cybersecurity deficiencies,[102] and can be expected to serve as the basis for future enforcement actions as regulatory scrutiny of cybersecurity practices increases.

In fact, just last week, the SEC relied to the Safeguard Rule to deliver on its earlier statement that cybersecurity is an area "high on [the SEC's] radar screen."[103] The SEC announced charges against a St. Louis-based investment adviser that, according to the SEC, had "failed to establish the required cybersecurity policies and procedures in advance of a breach that compromised the personally identifiable information (PII) of approximately 100,000 individuals, including thousands of the firm's clients."[104] The SEC expressly acknowledged that no evidence existed of financial harm to any of the firm's clients, but determined that enforcement proceedings were nevertheless appropriate in light of the "increasing barrage of cyber attacks on financial firms."[105] Among the firm's alleged failures were that it "failed to conduct periodic risk assessments, implement a firewall, encrypt PII stored on its server, or maintain a response plan for cybersecurity incidents."[106]

In addition, in November 2014, the SEC adopted Regulation Systems Compliance and Integrity ("Regulation SCI"), which requires certain key market participants, including registered national securities exchanges and clearing agencies, to take steps designed to reduce the occurrence of data breaches and improve resiliency in the event of a breach.[107] Regulation SCI provides a framework for these entities to implement policies and procedures to help ensure operational capability, take appropriate corrective action when systems issues occur, provide notifications and reports to the SEC regarding systems problems and systems changes, inform members and participants about systems issues, conduct business continuity testing, and conduct annual reviews of their automated systems.[108]

Financial Industry Regulatory Authority

The SEC has not been the only source of guidance for broker-dealers. Earlier this year, FINRA issued detailed guidance to address the threat of a cyber incident.[109] FINRA's guidance provides specific recommendations for ensuring each of the following: risk assessments, a governance framework, technical controls and preventative measures, incident response plans, training of employees, and intelligence sharing. Like the SEC, FINRA has relied on the Safeguard Rule to bring enforcement actions in the wake of a data breach. FINRA fined a regulated firm for failing to protect confidential customer information after international hackers obtained information regarding approximately 192,000 customers,[110] and recently entered into a settlement with another firm that faced an information security threat after an unencrypted laptop containing sensitive information about hundreds of thousands of clients was left unattended in a restroom.[111]

Federal Communications Commission

The FCC encourages communications companies to practice "proactive and accountable self-governance within mutually agreed parameters" with respect to cybersecurity, and facilitates the improvement of cyber-risk management and corporate accountability in the communications sector through the Communications Security, Reliability and Interoperability Council.[112] The FCC also has prioritized enforcement actions in cyber breach cases. In April of this year, the agency entered into a consent decree with AT&T after nearly 280,000 customers' personal data was compromised.[113] In what the FCC called the "largest privacy and data security enforcement action to date," AT&T agreed to pay a $25 million penalty, hire a senior compliance office, conduct a privacy risk assessment and adopt various other reforms.[114] Companies in the communications sector should expect the FCC to continue its enforcement attention on perceived cybersecurity lapses in the future.

Department of Health & Human Services

The Health Insurance Portability and Accountability Act ("HIPAA") Security Rule established "national standards for protecting the confidentiality, integrity, and availability of electronic protected health information," and HHS's Office of Civil Rights ("OCR") is charged with the administration and enforcement of HIPAA's Privacy and Security Rules.[115] In May 2014, two health care organizations entered into a settlement with the HHS OCR for $4.8 million after allegedly failing to adequately secure "thousands of patients' electronic protected health information" that was "held on their network," in the largest HIPAA settlement to date.[116]

Federal Trade Commission

The FTC has been particularly active in the area of cybersecurity, bringing over 50 civil actions against companies related to the protection of personal information, using its authority under the Gramm-Leach-Bliley Act ("GLBA"), Section 5 of the FTC Act (which prohibits unfair or deceptive practices), and the Fair Credit Reporting Act.[117] The United States Court of Appeals for the Third Circuit recently upheld the FTC's authority to bring suits under Section 5 of the FTC Act based on "unfair or deceptive" cybersecurity practices.[118] The Third Circuit ruled that the alleged conduct—breaches of a hotel chain's data which resulted in over $10.6 million in fraudulent charges—did not "fall[] outside the plain meaning of 'unfair.'"[119] This decision may embolden the FTC to increasingly prioritize data security and privacy issues in its enforcement initiatives.

The FTC's relatively sweeping—and potentially expanding—authority to regulate cybersecurity issues is further evidenced by its issuance of the Health Breach Notification Rule in 2009, which requires certain businesses that are "not covered by HIPAA to notify their customers and others if there's a breach of unsecured, individually identifiable electronic health information."[120] The agency began enforcing the rule in February 2010.[121]

State Attorneys General

Forty-seven states, the District of Columbia, Puerto Rico, and the Virgin Islands have laws requiring notification of security breaches involving personal information, and a number of state attorneys general have been active in this area. About 15 state attorneys general, led by Illinois and Connecticut, are reportedly investigating a 2014 cyber breach at a major financial institution.[122] As lawmakers consider enacting federal legislation that sets nationwide guidelines for customer notification in the case of a data breach, the "[a]ttorney generals from all 47 states with data breach notification laws are urging Congress not to preempt local rules with a federal standard," arguing that the states currently play an "important role" in protecting consumers from cyberattacks.[123]

Federal Bank Regulators

The federal bank regulators—the Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve System ("FRB"), the Federal Deposit Insurance Corporation ("FDIC"), and the National Credit Union Administration ("NCUA")—have responsibility for ensuring the safety and soundness of the institutions they oversee, protecting federal deposit insurance funds, promoting stability in financial markets, and enforcing compliance with applicable consumer protection laws. These regulators individually and collectively have prioritized cybersecurity and have been working with industry and interagency organizations to improve financial institution cybersecurity.

Financial Stability Oversight Council

The Financial Stability Oversight Council ("FSOC"), established by the Dodd-Frank Act to "identify risks to the [country's] financial stability," "promote market discipline," and "respond to emerging threats to the stability of the U.S. financial system," has addressed the issue of cybersecurity.[124] Earlier this year, FSOC—whose members include the heads of each of the bank regulators—released its annual report, in which it identified cybersecurity as requiring "heightened risk management and supervisory attention." The report warned that "recent cyber attacks have heightened concerns about the potential of an even more destructive incident that could significantly disrupt the workings of the financial system."[125] The FSOC advised that "[m]itigating risks to the financial system posed by malicious cyber activities requires strong collaboration among financial services companies, agencies, and regulators."[126]

Individual Bank Regulators

Each of the individual bank regulators have also emphasized the importance of cybersecurity. In its Spring 2015 Semiannual Risk Perspective, for example, the OCC identified cybersecurity as one of its top supervisory concerns, and a priority for the next twelve months.[127] The report noted that, consistent with guidance from the other regulators, the OCC's bank examinations "will include assessments of data and network protection practices, business continuity practices, risks from vendors, and compliance with any new guidance."[128] A senior representative of the Federal Reserve Bank of New York emphasized that

"cybersecurity is a 'new normal.' It is going to become part of our vocabulary in nearly every exam we conduct, conversation we have with senior management, and conversation about the future of financial services."[129] Benjamin Lawsky, who recently stepped down as the Superintendent of the New York Department of Financial Services, called cybercrime "a huge threat to our financial system" and predicted that there would be "a lot of action around cybersecurity and the regulation in that area."[130]

Federal Financial Institutions Examination Council

The banking regulators have collaborated and coordinated on cybersecurity through the FFIEC, a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions and to make recommendations to promote uniformity in the supervision of financial institutions. Two key forms of guidance issued by the FFIEC are the Information Technology Examination Handbook and the Cybersecurity Assessment Tool, which was released this summer and discussed in detail below.

The FFIEC's IT Examination Handbook, first published in 1980, "comprises 11 booklets addressing topics such as electronic banking, information security, and outsourcing technology services."[131] FFIEC has updated the Handbook, and the FFIEC and individual regulators have issued guidance to address particular threats facing the industry, such as DDoS attacks, account takeovers, advanced persistent threats, and credit/debit card breaches.[132] There are now more than 150 examples of cybersecurity guidance applicable to the banking and finance sector.[133]

Gramm-Leach-Bliley Act

Financial institutions also are subject to certain regulations and interagency guidance issued pursuant to the GLBA. Section 501(b) of GLBA mandated that the bank regulators issue information security standards for financial institutions to safeguard sensitive customer information. Member agencies of the FFIEC did so by issuing the Interagency Guidelines Establishing Information Security Standards (the "Security Guidelines"). Under the Security Guidelines, each financial institution must develop and maintain an effective information security program tailored to the complexity of its operations, and service providers that have access to its customer information are required to take appropriate steps to protect the security and confidentiality of this information.[134] The Security Guidelines require each financial institution to identify and evaluate risks to its customer information, develop a plan to mitigate the risks, implement the plan, test the plan, and update the plan when necessary. Each financial institution must also report to its board "at least annually" on its information security program and compliance with the Security Guidelines.[135] The standards set forth in the Security Guidelines are consistent with the IT Examination Handbook and other guidance from the FFIEC member agencies. The Security Guidelines afford the FFIEC agencies enforcement options if financial institutions do not establish and maintain adequate information security programs.[136]

Pursuant to its authority under the GLBA, the FTC issued the Safeguards Rule, requiring certain non-bank financial institutions under the FTC's jurisdiction to have an information security plan that "contains administrative, technical, and physical safeguards" to "insure the security and confidentiality of customer information; protect against any anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer."[137]

Financial institutions should endeavor to follow regulatory guidance to ensure best practices in cybersecurity and to mitigate their regulatory risk. In addition, being responsive to this guidance is essential because private plaintiffs are likely to rely on any deviation from the regulatory guidelines as purported evidence of inadequate cybersecurity in the wake of a cyber incident. In one case, for example, the United States Court of Appeals for the First Circuit determined that a bank's security procedures were not "commercially reasonable" based in part on the bank's failure to adhere to FFIEC guidance.[138]

Best Practices for Boards and Senior Management

The frequency and scope of recent cyberattacks and the corresponding increased costs and harm demonstrate that the cyber threat is one of the most significant business risks facing financial institutions and other businesses. As a result, cybersecurity is a governance issue that requires attention from directors and senior leadership. In a recent study, "79 percent of C-level US and UK executives surveyed sa[id] executive level involvement is necessary to achiev[e] an effective incident response to a data breach and 70 percent believed board level oversight is critical."[139] Below is a summary of some of the key practices for boards and senior management to consider.

Board Oversight

As one SEC Commissioner stated, "ensuring the adequacy of a company's cybersecurity measures needs to be a critical part of a board of director's [*sic*] risk oversight responsibilities."[140] Senior management and the board should consider whether a committee of the board (such as the Audit Committee or a Risk Committee) or the full board should have primary oversight responsibility for cybersecurity. In any case, the board should be briefed regularly about cyber risks and efforts to address and mitigate those risks. External advisers, including those with the requisite technical expertise, can be enlisted as necessary to help directors understand the risks and a company's preparedness to respond to those risks. The board should also consider whether particular members of management should be tasked with overseeing cybersecurity and reporting to the board on cybersecurity matters.

The National Association of Corporate Directors ("NACD") addressed the role of boards relating to cybersecurity and identified the following five principles: (1) "[d]irectors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue;" (2) "[d]irectors should understand the legal implication of cyber risks as they relate to their company's specific circumstances;" (3) "[b]oards should have adequate access to cybersecurity expertise, and

discussions about cyber-risk management should be given adequate time on the board meeting agenda on a regular basis;" (4) "[d]irectors should set an expectation that management establish an enterprise-wide cyber-risk management framework with adequate staffing and budget;" and (5) "[b]oard-management discussion of cyber risks should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach."[141]

For financial institutions, the recently-released FFIEC Assessment Tool (discussed in detail below) provides a useful mechanism to evaluate the alignment between an institution's inherent risks and its cybersecurity preparedness. The FFIEC also released an overview for CEOs and directors along with the Assessment Tool that, among other things, lists questions for management and directors to consider and guide their discussions when using the Assessment Tool.[142] Although a valuable resource, the Assessment Tool "is intended to complement, not replace, an institution's risk management process and cybersecurity program."[143]

Periodic Risk Assessments

Periodic risk assessments should be conducted to develop a meaningful understanding of the key cyber risks facing the organization. It is impossible to design a program tailored to a particular company's risks and operations without first understanding those risks and how they impact the company's business. Accordingly, the board and senior leadership should be briefed regularly on the institution's cyber risks and the measures in place to mitigate those risks. The risk assessments should identify the company's most sensitive and valuable information and assets, and the company's senior leadership should understand where and how that information is stored, and the ways in which it is protected. Those assets should be afforded the greatest level of security protection.

Preventative Measures: Technology, Controls and Compliance

The board and senior management should ensure that the company has implemented sufficient preventative measures and controls and that they are being periodically reviewed and updated as necessary. Technology is, of course, a critical component of defending against a cyberattack, and companies should follow the best practices outlined in the applicable regulatory guidelines. Technological measures, however, cannot be relied on exclusively. Employees remain a significant source of potential vulnerability that cybercriminals continue to exploit, and therefore, an effective cybersecurity program must incorporate employee training and education and information-security controls. Notwithstanding the risk from insiders, this aspect of cybersecurity is often neglected. In one survey, for example, only 50 percent of respondents said they conduct periodic security awareness and training programs, and the same number said they offer security training for new employees.[144]

Although many companies have developed robust compliance programs in areas ranging from anti-bribery to anti-money laundering to insider trading, compliance efforts on the information-security side are often lagging, even though the risk to the overall organization from non-compliance by a single

employee may be potentially greater in the cyber area. New hires and existing personnel should all be trained on the importance of cybersecurity, educated as to the risks and their individual roles in protecting the company against those risks, and advised of the company's information-security policies. Compliance with information-security policies should be monitored, just as employees' compliance with securities trading or other more traditional areas of compliance are routinely monitored.

Employee training should be provided periodically and updated as necessary, and employees should be required to sign regular cyber-compliance certifications. The importance of information security needs to be emphasized, and the message should come from the top of the organization to instill a strong culture of information security throughout the organization. Basic policies and protocols that reduce risks should include requiring encryption, limiting the use of personal devices, using strong passwords that must be changed periodically, and controlling remote access through multifactor authentication.

Taking these steps to enhance cybersecurity can present a difficult balance for companies because each enhanced security measure typically imposes an additional burden on employees. It could become convenient for employees to bypass these measures, so it is critically important that information-security policies be prioritized, and that the proper tone is set by management. Further, there are effective measures that impose a relatively low burden and yet, surprisingly, still are not implemented by many sophisticated organizations until after they are victimized. In the wake of the OPM hack, for example, the White House announced a "Cybersecurity Sprint" designed to improve cybersecurity at federal agencies over a 30-day period, and that effort has included basic measures that had not been widely implemented. As one example, in just the first 10 days of the Sprint, federal civilian agencies reportedly were able to increase multifactor authentication—an effective and not burdensome measure—by 20 percent.[145]

Moreover, given the increased awareness of the severity of the risk among the general public, there is reason to be optimistic that employees will have at least a modestly increased tolerance for some additional burdens in order to fortify their companies' cybersecurity.[146]

As the nature of the cybersecurity threat evolves, and additional risks or vulnerabilities are identified, cybersecurity policies and protocols must be updated accordingly. For example, the need for increased oversight and scrutiny of third-party vendor relationships has become evident as cybercriminals have increasingly exploited weaknesses in vendor security to bypass a company's cybersecurity. The Target breach is perhaps the most high-profile example, but the DOJ's recent announcement of a massive insider trading ring that relied on the hacking of business newswires further highlights the risks associated with providing network access or sensitive data to third-party vendors. Management should require appropriate vendor management controls, including diligence, monitoring and contractual protections.

Information Sharing with Government and Industry Peers

A comprehensive cybersecurity program should include a mechanism for sharing information with public and private partners to enhance access to actionable cyber-threat intelligence that can be used to better detect and respond to threats. As discussed below in the context of the GAO Report, the financial sector is among the leaders in this effort. Although lawmakers and regulators are exploring ways to improve cyber information sharing, institutions must continue working collaboratively to remove barriers to more robust sharing and to find innovative ways to enhance the effectiveness of their information sharing. Information sharing is also an important tool for smaller institutions, which tend to have less sophisticated defense mechanisms and fewer IT resources; by helping them focus their limited resources, cyber-threat intelligence can be particularly important to those institutions.

Review and Satisfaction of Applicable Legal and Regulatory Requirements

The legal and regulatory framework governing cybersecurity is fragmented and evolving. Companies must navigate a maze of domestic and international cyber-related laws and regulations that apply in both the pre-breach and post-breach context. Companies have legal, regulatory and often contractual obligations to safeguard information and, following a breach, to make certain disclosures to customers, regulators, or other third-parties. In the post-breach context, for example, 47 states, the District of Columbia, Puerto Rico, and the Virgin Islands have laws requiring notification of security breaches involving personal information, and industry-specific laws and regulations impose independent notification obligations. As discussed above, public companies also have public disclosure obligations, and SEC-regulated entities are subject to separate SEC regulations concerning the safeguarding of information. Senior leadership should understand not only the business risks associated with the cyber threat but also the legal and regulatory risks and requirements. Management should ensure ongoing compliance with those requirements and, as discussed below, oversee the company's preparedness to satisfy its legal, regulatory, and contractual obligations in the event of a breach. Just as advance planning can mitigate the business risks, it can also mitigate the legal and regulatory exposure from a cyberattack.

Incident Response and Business Continuity Plan

Because no defense system is impenetrable, it is critical not only to ensure adequate preventative measures, but to have a comprehensive incident response and business continuity plan that can quickly be implemented in the event of a breach. In the wake of an attack, companies face a host of challenges and must make difficult and time-sensitive decisions, typically with incomplete information and in a chaotic environment. The way in which companies respond can directly impact the extent of the resulting harm, including financial loss, reputational harm, and civil and regulatory liability—all of which can be mitigated through advance planning and maximum preparedness.

Some of the key issues that typically arise following a breach are: (1) assessing the scope of the attack, determining what, if anything, has been taken, and ensuring that any intruders are completely removed from the network. This is a process that is usually far more difficult and time-consuming than most organizations anticipate, which further compounds the challenge of responding to an attack because the scope of the breach typically cannot be determined quickly, meaning that companies will have to make difficult decisions despite lacking key facts and critical information; (2) quickly restoring and ensuring continuity of business operations with minimal disruption, even in the case of destructive malware; (3) complying with domestic and international statutory and regulatory disclosure requirements, and determining when and to whom disclosures should be made, as well as what should be disclosed; (4) deciding if and when to notify law enforcement authorities and, if so, dealing with the day-to-day interactions with those authorities as they conduct investigations; and (5) handling internal communications and external public relations with consumers, shareholders and other affected third-parties.

Given the range of issues that arise, a comprehensive response requires an integrated approach involving the participation not only of senior leadership but of representatives from a number of different internal constituencies, such as IT, legal, compliance, and investor relations, as well as outside technical, legal, and PR advisors. Companies should not put themselves in the position of confronting these difficult questions for the first time, or scrambling to determine who should be responsible for what, in the chaotic aftermath of a cyber incident. Companies need to consider each of these issues in advance of an attack. The response plan should provide clearly delineated lines of responsibility for each of the significant issues likely to arise following a breach and should be tested through tabletop exercises before an incident occurs.

The risk of a cyberattack cannot be eliminated. But the impact can be mitigated through careful planning, and it is therefore essential that boards and senior leadership take the steps necessary to put their companies in the best position to limit the resulting harm should an incident take place.

Recent Developments Affecting Financial Institutions

Recognizing the unique threats facing the industry, the GAO and FFIEC each released cybersecurity resources this summer specifically tailored to financial institutions. We examine both the GAO Report and the FFIEC Cybersecurity Assessment Tool in detail below.

The GAO Report on Cybersecurity at Banks and Other Depository Institutions

In July of this year, the GAO released a report on cybersecurity at banks and other depository institutions.[147] The report principally examined (1) how bank regulators oversee depository institutions' efforts to mitigate cyber threats, and (2) how government agencies share cyber threat information with the banking sector. The report's key conclusions were: first, while bank regulators focus their cybersecurity examinations on risks *within* individual institutions, the regulators need to collect and analyze data from IT examinations on trends *across* the industry; and second, notwithstanding fairly robust sharing of cyber-threat information among financial institutions, obstacles still remain, and banks are seeking more usable threat information from their government counterparts.

Bank regulators take an institutional, risk-based approach to their cybersecurity examinations. Accordingly, the scope of an IT examination at any particular institution is determined based on an assessment of that institution's internal and external risks. To assess those risks, examiners look at an institution's safeguards and protections against threats to customer information, the likelihood and effects of identified threats and vulnerabilities, and the sufficiency of policies and procedures to control risks.

Hiring and training a sufficient number of examiners with the requisite expertise to conduct sophisticated examinations poses a serious challenge for regulators. To put the problem in perspective, the FDIC is the primary regulator for over 4,000 institutions, and has only "60 premium IT examiners who are highly skilled in conducting IT examinations;" the OCC is the primary regulator for more than 1,500 institutions, and has "100 dedicated IT specialist examiners;" the NCUA "regulates more than 6,200 credit unions" and has "40 to 50 subject-matter IT examiners" and 16 IT specialists; and the Federal Reserve "regulates more than 5,500 institutions" and has approximately 85 IT examiners with information security or advanced IT expertise.[148]

Faced with these resource constraints, regulators generally have not used IT experts for examinations of medium and small institutions, meaning that "examiners with little or no IT expertise are performing IT examinations at smaller institutions."[149] This allocation of limited resources is understandable, but concerning, especially given that the discrepancy in sophistication of examiners parallels the disparity in information-security resources across such institutions. Smaller institutions, not surprisingly, tend to devote fewer resources to information security. One large bank said it planned to deploy over 1,000 people to focus on cybersecurity,[150] and following a significant breach last year, that bank's CEO announced that the bank would double its $250 million annual spending on cybersecurity.[151] By contrast,

some community banks do not have any dedicated IT security personnel.[152] This may leave smaller financial institutions more vulnerable to cyberattacks, perhaps explaining why cybercriminals appear increasingly to be targeting smaller financial institutions.[153]

The principal deficiency identified in the GAO Report, however, was the failure of regulators to aggregate data from individual examinations to identify trends across the industry: "Although each regulator described collecting some information across examinations to assist its oversight, the regulators did not have standardized methods for collecting examination data that could allow them to readily analyze trends in specific information security problems across institutions."[154]

The failure stems in part from the methods by which regulators collect information from individual institutions. In particular, the information is not collected in formats that would facilitate such aggregation and analysis. The regulators, for example, do not have standardized methods for categorizing IT deficiencies. The deficiencies identified at particular institutions generally were not broken into fields or categories that differentiated the types of problems found at different institutions, and thus the regulators are not able to identify trends in specific types of deficiencies across institutions. In addition, although banks have obligations to disclose to their regulators data breaches that compromise sensitive customer information, the information collected by the regulators is not centrally compiled and analyzed. The GAO found that the regulators "varied in the extent to which they could provide data on actual incidents at their regulated institutions."[155]

The GAO Report concluded that these flaws have hindered the regulators from identifying broader IT issues affecting their regulated entities and thus impede their ability to better target their IT risk assessments. This is not the first time—and cybersecurity is not the first area—in which the GAO has observed this deficiency in how regulators collect and analyze information. In a January 2000 report, the GAO observed "that neither the Federal Reserve nor OCC collected aggregated information on the risks that examiners identified during examinations."[156] As an example of the potential benefits of such an approach, the January 2000 report concluded that by aggregating examination data, regulators would have been better positioned to recognize the industry-wide exposure to Long Term Capital Management and appreciate the potential disruption to the markets of its collapse.[157] And in 2009, the GAO "found that bank regulators' oversight of institutions' anti-money laundering activities could be improved by aggregating information about deficiencies."[158]

The second key conclusion of the GAO Report was that improvements are needed in the way cyber-threat information is shared among the financial sector and disseminated from the government to the private sector. While the government has been engaged in a campaign to encourage the private sector to share more information with the government, the GAO Report identifies deficiencies in the flow of information *from* the government *to* the private sector.

The financial industry has developed sophisticated information-sharing mechanisms and established a model that other industries have sought to emulate. The Financial Services Information Sharing and Analysis Center ("FS-ISAC"), for example, has become a key resource for cyber-threat information for financial sector institutions. The FS-ISAC was established in 1999 and is the operational arm of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security ("FSSCC"). The FS-ISAC facilitates the sharing of information pertaining to physical and cyber threats, vulnerabilities, incidents, potential protective measures and practices. It has over 5,000 members worldwide, and when it learns of an attack or has other information to share, it follows a protocol in which different color-coded alerts indicate who can access the information.[159] During the OCIE examination sweep, broker-dealers identified the FS-ISAC as "adding significant value,"[160] and banks have reported that a high level of trust has developed among the FS-ISAC members and that the FS-ISAC was valuable in responding to the financial-sector DDoS attacks.[161] The DDoS attacks showcased the "sector's capacity . . . , through the FS-ISAC, [to] act collectively to respond to major attacks and minimize their capacity to cascade through the sector."[162]

The financial sector has also developed and implemented innovations to facilitate more robust information sharing. For example, to help alleviate concerns about exposing competitive weaknesses by revealing breaches to competitor institutions, the FS-ISAC removes identifying data to obscure the identity of the breached institution.[163] Although some reluctance to share information for this reason remains, this approach has reduced the concern. The FS-ISAC has also deployed an automated system called Soltra Edge, which was developed in conjunction with DHS, the Depositary Trust, and Clearing Corporation, for efficiently disseminating alerts to member institutions.[164]

The government is also an important source of cyber threat information for financial institutions. In nearly 70 percent of all breaches, organizations first learn of the breach from the government or some other external source.[165] The primary government sources of cyber information for the financial sector are Treasury, DHS, Secret Service, and the FBI. Treasury's Financial Sector Cyber Intelligence Group ("CIG"), for example, monitors and analyzes intelligence on cyber threats to the financial sector and disseminates that information to industry participants. The CIG facilitates the sharing of classified information and also responds to requests for information from financial institutions, either individually or through the FS-ISAC. Law enforcement agencies, like the FBI Cyber Division and the Secret Service's Electronic Crimes Task Forces, often share threat information directly with financial institutions or through the use of Private Industry Notification Reports addressing particular threats. And representatives of financial institutions are often provided temporary security clearances so they can receive threat briefings from the FBI or other agencies.

Although the financial industry has developed extensive information-sharing arrangements both within the private sector and between the private sector and government, the GAO Report identifies obstacles that remain and offers suggestions for improvements to the way in which the government disseminates

information to the industry. In particular, financial institutions have expressed frustration that the information they receive is often "repetitive," "not timely," and "lack[ing] sufficient details" to be actionable.[166]

By virtue of having multiple sources of information within government, banks often end up receiving the same information from multiple agencies.[167] That redundancy causes banks to waste resources trying to determine whether the information is new or duplicative. While this creates an unnecessary distraction of IT resources for banks of all sizes, it poses an even greater challenge for smaller institutions that are already grappling with limited information-security resources.

Banks also reported that for the information to be effective, it must be timely and specific.[168] The timeliness of information sharing can be critical in effectively defending against a cyberattack that quickly spreads from one institution to another. One report found that 75 percent of cyberattacks spread from victim 0 to victim 1 within 24 hours, and "[o]ver 40% hit the second organization in less than an hour."[169] As to the specificity of the information, the GAO Report determined that the information banks obtain from the government often lacks context or specific details necessary to enable banks to take steps to protect themselves. A representative of a financial institution offered this analogy: "receiving insufficiently detailed information [is] similar to telling the institution that it might be attacked by a criminal in a red hat. But saying that a criminal in a red hat, would go behind the building, and use a crowbar to force the door open would provide enough detail for the institution to better target its defenses."[170]

The government is already taking steps to reduce obstacles to better information sharing. Treasury, for example, is seeking to accelerate the declassification of financial cyber threat information, which should enable the sharing of more specific information. Deputy Treasury Secretary Sarah Bloom Raskin recently said that Treasury is focused on "getting information declassified very quickly and into the hands of people who need it," adding, "It makes no sense for the government to be sitting on this information."[171]

While the GAO Report focused mainly on potential improvements in the flow of information from government to the private sector, it also identified issues that continue to restrict complete sharing in the other direction. There is, for example, continuing concern within the private sector about potential liability resulting from the sharing of personal information with the government, as well as fears that the information may become classified (which, in turn, restricts further sharing of the information by the institution) or subject to public disclosure (through FOIA requests, for example).[172]

Congress and the White House have been working to alleviate these concerns as well. In February, President Obama issued Executive Order 13,691 on Promoting Private Sector Cybersecurity Information Sharing, which directs the Secretary of Homeland Security to "strongly encourage" the development of Information Sharing and Analysis Organizations ("ISAOs") to serve as focal points for cybersecurity collaboration.[173] The President also proposed legislation that would protect companies from lawsuits for sharing certain cybersecurity information

with the government.[174] Two pending bills in the House and one in the Senate seek to provide private companies protection from liability in order to encourage sharing of information with the government.[175]

The FFIEC Cybersecurity Assessment Tool

This summer, the FFIEC rolled out a Cybersecurity Assessment Tool (the "Assessment Tool") to give financial institutions a "repeatable and measurable process to inform management of their institution's risks and cybersecurity preparedness."[176] The Assessment Tool incorporates principles from the IT Handbook and the National Institute of Standards and Technology ("NIST") Framework.

The Assessment Tool is broken down into two parts. The first addresses an institution's Inherent Risk Profile, and the second addresses the company's Cybersecurity Maturity. It enables an institution to evaluate its level of risk in each of five enumerated risk categories, and its level of cybersecurity preparedness in each of five "domains." By comparing the institution's risk levels to its cybersecurity maturity levels, management can assess whether the degree of maturity is sufficiently aligned with its level of risk. If not, the Assessment Tool provides readily identifiable measures the company can take to reduce a particular risk or increase the maturity of a particular aspect of its cybersecurity.

The Inherent Risk Profile assigns one of five escalating risk levels (least, minimal, moderate, significant, or most) to each of five categories of risk: (1) technologies and connection types, (2) delivery channels, (3) online/mobile products and technology services, (4) organizational characteristics, and (5) external threats. For each category, the Assessment Tool lists different parameters that correlate to each risk level. For example, within the "technologies and connection types" category, one of the considerations is the number of personal devices allowed to connect to the corporate network. The institution determines its risk level by choosing the parameters that best describe the company's characteristics. The following table provides an example of the characteristics, or parameters, corresponding to each of the risk categories for "personal devices":[177]

	Risk Level				
	Least Risk	Minimal Risk	Moderate Risk	Significant Risk	Most Risk
Personal devices allowed to connect to the corporate network	None	Only one device type available; <5% of employees; e-mail access only	Multiple device types used; available to <10% of employees; e-mail access only	Multiple device types used; available to <25% of authorized employees; e-mail and some applications	Any device type used; available to >25% of employees; all applications accessed

After determining the Inherent Risk Profile, the institution turns to the Cybersecurity Maturity portion of the Assessment Tool to determine its maturity level within each of five "domains:" (1) "Cyber Risk Management and Oversight," (2) "Threat Intelligence and Collaboration," (3) "Cybersecurity Controls," (4) "External Dependency Management," and (5) "Cyber Incident Management and Resilience."[178] Within each domain, the Assessment Tool lists declarative statements that apply to each maturity level (baseline, evolving, intermediate, advanced, or innovative). The institution determines its maturity level by identifying which declarative statements best fit the current practices of the company. The Assessment Tool thereby allows a company to determine its maturity level within each of the five domains, but does not provide an overall enterprise-wide maturity level.

When the assessment is complete, management can assess the degree of alignment between its risk profile and its cybersecurity maturity. An institution's maturity level generally should go up as its risk profile rises. Because the risk profile and maturity levels will change over time, the Assessment Tool recommends that management reevaluate both periodically and be vigilant of planned changes (like new products or services or new connections) that may affect its risk profile.

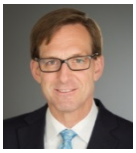
The Assessment Tool is a useful management oversight resource because it provides a method for comparing an institution's maturity level to its inherent risk profile. To the extent management is not satisfied with the level of maturity in relation to its risk profile, the characteristics of the different categories provide actionable steps that management can take either to reduce its risk level or to enhance its maturity level.

* * *

As discussed above, the cyber threat presents a growing business and legal risk for companies across a broad spectrum of industries and requires careful and current attention by senior corporate leadership.

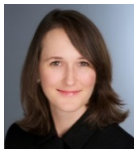
Paul, Weiss draws on an experienced team of attorneys across a range of practice areas to counsel our clients on cybersecurity challenges and strategies to manage the complex risks and consequences of cyber incidents.

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

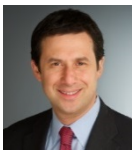


John F. Baughman
Partner
212-373-3021
jbaughman@paulweiss.com

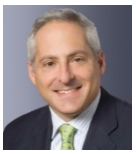
H. Christopher Boehning
Partner
212-373-3061
cboehning@paulweiss.com



Jessica Carey
Partner
212-373-3566
jcarey@paulweiss.com

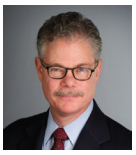


Roberto Finzi
Partner
212-373-3311
rfinzi@paulweiss.com



Michael E. Gertzman
Partner
212-373-3281
mgertzman@paulweiss.com

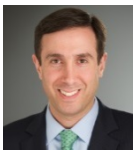
Brad S. Karp
Partner
212-373-3316
bkarp@paulweiss.com



Daniel J. Kramer
Partner
212-373-3020
dkramer@paulweiss.com

Lorin L. Reisner
Partner
212-373-3250
lreisner@paulweiss.com

Elizabeth M. Sacksteder
Partner
212-373-3505
esacksteder@paulweiss.com



Richard C. Tarlowe
Counsel
212-373-3035
rtarlowe@paulweiss.com

Associates Elana Rose Beale, Erin Smith Dennis, and Marina Indenbaum, as well as Law Clerk Kelly D. Tomlin, contributed to this client alert.

---

1 PwC, US Cybersecurity: Progress Stalled, Key Findings from the 2015 US State of Cybercrime Survey, PwC 3 (July 2015), https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf.

2 *NYSE Tweets—"The Issue We Are Experiencing Is An Internal Technical Issue And Is Not The Result Of A Cyber Breach,"* CNBC (July 8, 2015, 12:28 PM), http://www.cnbc.com/2015/07/08/reuters-america-nyse-tweets--the-issue-we-are-experiencing-is-an-internal-technical-issue-and-is-not-the-result-of-a-cyber-breach.html.

3 Press Briefing, Press Secretary John Earnest, Press Secretary, Office of the Press Secretary, White House (July 8, 2015), https://www.whitehouse.gov/the-press-office/2015/07/08/press-briefing-press-secretary-josh-earnest-7815.

4 *The Latest: NYSE Trading Resumes After Outrage*, THE ASSOCIATED PRESS, (July 8, 2015, 3:59PM), http://bigstory.ap.org/article/131d63c2119340618b3ca160d546e4ce/latest-nyse-halts-trading-because-technical-issues.

5 *Jeh Johnson: United, NYSE Problems Not Caused By 'Nefarious' Actor*, REUTERS, (July 8, 2015), http://www.reuters.com/video/2015/07/08/jeh-johnson-united-nyse-problems-not-cau?videoId=364876319.

6 Press Release, U.S. Dep't of Justice, Nine People Charged in Largest Known Computer Hacking and Securities Fraud Scheme, (Aug. 11, 2015), http://www.justice.gov/usao-nj/pr/nine-people-charged-largest-known-computer-hacking-and-securities-fraud-scheme [hereinafter Press Release, Dep't of Justice].

7 Press Release, U.S. Sec. & Exch. Comm'n, SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach, (Sept. 22, 2015), http://www.sec.gov/news/pressrelease/2015-202.html.

8 Colleen McCain Nelson & Byron Tau, OPM Director Katherine Archuleta Resigns After Massive Personnel Data Breach, Wall St. J., http://www.wsj.com/articles/opm-director-katherine-archuleta-resigns-after-massive-personnel-data-hack-1436547193 (last updated July 10, 2015, 7:10 PM).

9 Andy Greenberg, Hackers Remotely Kill a Jeep on the Highway—With Me in It, Wired, (July 21, 2015), http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway; David Gelles, Hiroko Tabuchi, and Matthew Dolan, Complex Car Software Becomes the Weak Spot Under the Hood, N.Y. Times, (Sept. 27, 2015), http://www.nytimes.com/2015/09/27/business/complex-car-software-becomes-the-weak-spot-under-the-hood.html.

10 Mike Spector & Danny Yadron, Regulators Investigating Fiat Chrysler Cybersecurity Recall, Wall St. J., http://www.wsj.com/articles/fiat-chrysler-recalls-1-4-million-vehicles-amid-hacking-concerns-1437751526 (last updated July 24, 2014, 8:37 PM).

11 Damien Paletta, FBI Director Sees Increasing Terrorist Interest in Cyberattacks Against U.S., Wall St. J., (July 22, 2015, 10:41 PM), http://www.wsj.com/articles/fbi-director-sees-increasing-terrorist-interest-in-cyberattacks-against-u-s-1437619297.

12 Ian McKendry & Tanaya Macheel, Regulators to Step Up Cybersecurity Activity: Lawsky, American Banker, (July 28, 2015), http://www.americanbanker.com/news/bank-technology/regulators-to-step-up-cybersecurity-activity-lawsky-1075715-1.html.

13 Michael Riley & Jordan Robertson, *Digital Misfits Link JPMorgan Hack to Pump-and-Dump Fraud*, BLOOMBERG BUSINESS, (July 21, 2015, 1:50 PM), http://www.bloomberg.com/news/articles/2015-

07-21/fbi-israel-make-securities-fraud-arrests-tied-to-jpmorgan-hack (last updated July 22, 2015, 8:09 AM); Matthew Goldstein, *4 Arrested in Schemes Said to be Tied to JPMorgan Chase Breach*, N.Y. TIMES, (July 21, 2015), http://www.nytimes.com/2015/07/22/business/dealbook/4-arrested-in-schemes-said-to-be-tied-to-jpmorgan-chase-breach.html.

14 James R. Clapper, Dir. of Nat'l Intelligence, S. Armed Forces Comm., Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community 1 (Feb.26, 2015), http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf [hereinafter Clapper, Worldwide Threat Assessment].

15 *Id.*

16 IBM, IBM 2015 Cyber Security Intelligence Index: Analysis of Cyber Attacks and Incident Data from IBM's Worldwide Security Services Operations, app. at 3 fig.2 (2015), http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03073usen/SEW03073USEN.PDF [hereinafter IBM 2015 Cyber Security Intelligence Index].

17 Verizon, 2015 Data Breach Investigations Report, 3 (2015), *available at* http://www.verizonenterprise.com/DBIR/2015 [hereinafter Verizon, 2015 Data Breach Investigations Report].

18 Mandiant, M-Trends 2015: A View From The Front Lines, FireEye 2 (2014), https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf [hereinafter Mandiant, A View From The Front Lines].

19 Worldwide Threat Assessment, *supra* note 14, at 2; see U.S. Gov't Accountability Office, GAO-15-509, Cybersecurity: Bank and Other Depository Regulators need Better Data Analytics and Depository Institutions Want More Usable Threat Information, at 9-11 (July 2, 2015), *available at* http://www.gao.gov/products/GAO-15-509 [hereinafter GAO-15-509].

20 GAO-15-509, *supra* note 19, at 13.

21 Press Release, Dep't of Justice, *supra* note 6.

22 Barry Vengerik et al., Hacking the Street? Fin4 Likely Playing the Market, FireEye (2014), https://www2.fireeye.com/rs/fireye/images/rpt-fin4.pdf.

23 Paletta, *supra* note 11.

24 See Mandiant, A View From The Front Lines, *supra* note 18, at 20-21; PwC, US Cybersecurity, *supra* note 1, at 4.

25 Worldwide Threat Assessment, *supra* note 14, at 1; see also Cyber Crime: Modernizing our Legal Framework for the Information Age: Hearing Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary (July 8, 2015) [hereinafter Testimony of Wm. Douglas Johnson], *available at* http://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Johnson%20Testimony.pdf (testimony of Wm. Douglas Johnson, American Bankers Association) ("Nation states are becoming more adept at compromising private and public computer systems for reasons ranging from retribution for perceived wrongs to espionage.").

26 Press Release, Fed. Bureau of Investigation, Update on Sony Investigation, (Dec. 19, 2014), https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

27 Mark Mazzetti & David E. Sanger, U.S. Fears Data Stolen by Chinese Hacker Could Identify Spies, N.Y. Times, (July 24, 2015), http://www.nytimes.com/2015/07/25/world/asia/us-fears-data-stolen-by-chinese-hacker-could-identify-spies.html?_r=0.

28 Nicole Perlroth, Hackers in China Attacked The Times for Last 4 Months, N.Y. Times, (Jan. 30, 2013), http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html.

29 David E. Sanger, Julie Hirschfeld Davis, & Nicole Perlroth, U.S. Was Warned of System Open to Cyberattacks, N.Y. Times, (June 5, 2015), http://www.nytimes.com/2015/06/06/us/chinese-hackers-may-be-behind-anthem-premera-attacks.html.

30 Press Release, U.S. Dep't of Justice, U.S. Charges Five Chinese Military Hackers For Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
31 *Id.* (quoting Holder).
32 Worldwide Threat Assessment, *supra* note 14, at 2.
33 GAO-15-509, *supra* note 19, at 11.
34 *Id.*
35 Nicole Perlroth & Quentin Hardy, Bank Hacking Was the Work of Iranians, Officials Say, N.Y. Times, (Jan. 8, 2013), http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html; see also Worldwide Threat Assessment, *supra* note 14, at 3.
36 GAO-15-509, *supra* note 19, at 11, 13.
37 JPMorgan Chase & Co., Current Report (Form 8-K) (Oct. 2, 2014) at 2, *available at* http://www.sec.gov/Archives/edgar/data/19617/000119312514362173/d799478d8k.htm.
38 *Id.*
39 Riley & Robertson, *supra* note 13; Goldstein, *supra* note 13.
40 Robin Sidel, Home Depot's 56 Million Card Breach Bigger Than Target's, Wall St. J., http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571 (last updated Sept. 18, 2014, 5:43 PM).
41 GAO-15-509, *supra* note 19, at 11-12.
42 *Id.*
43 Charles Riley, Insurance Giant Anthem Hit By Massive Data Breach, CNNMoney (Feb. 6, 2015, 10:52 AM), http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security.
44 Indictment, United States v. Turchynov, No. 2:15-cr-390 (D.N.J. Aug. 6, 2015), ECF No. 1; Indictment, United States v. Korchevsky, No. 1:15-cr-381 (E.D.N.Y. Aug. 5, 2015).
45 Press Release, U.S. Dep't of Just., Manhattan U.S. Attorney and FBI Assistant Director-In-Charge Announce Charges In Connection with Blackshades Malicious Software That Enabled Users Around The World to Secretly And Remotely Control Victims' Computers (May 19, 2014), http://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-and-fbi-assistant-director-charge-announce-charges-connection.
46 IBM 2015 Cyber Security Intelligence Index, *supra* note 16, at 6; Verizon Data Breach Investigations Report, *supra* note17, at 47.
47 IBM 2015 Cyber Security Intelligence Index, *supra* note 16.
48 Verizon Data Breach Investigations Report, *supra* note 17, at 13.
49 Target, Quarterly Report (Form 10-Q) (May 2, 2015) at 10, *available at* https://www.sec.gov/Archives/edgar/data/27419/000002741915000018/tgt-20150502x10xq.htm.
50 Dan Kaplan, Sony Expects to Spend at Least $171 million Over Breach, SC Mag., (May 23, 2011), http://www.scmagazine.com/sony-expects-to-spend-at-least-171-million-over-breach/article/203591.
51 Annie Lowrey, Sony's Very, Very Expensive Hack, N.Y. Mag., (Dec. 16, 2014, 5:47 PM), http://nymag.com/daily/intelligencer/2014/12/sonys-very-very-expensive-hack.html
52 Michael Cieply & Brooks Barnes, Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm, N.Y. Times, (Dec. 30, 2014), http://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html.
53 Complaint at 85-86, In re Target Corporation Consumer Data Security Breach Litigation, MDL No. 14-2522 (D. Minn. Aug. 25, 2014), ECF No. 182.
54 *Id.* at 1.

55 George Stahl, Target to Pay $10 Million in Class Action Over Data Breach, Wall St. J., (Mar. 19, 2015, 8:38 am), http://www.wsj.com/articles/target-to-pay-10-million-in-class-action-over-data-breach-1426768681.
56 *Id.*
57 Lisa Beilfuss, Target Reaches $19 Million Settlement with MasterCard Over Data Breach, Wall St. J., (Apr. 15, 2015, 6:17 PM), http://www.wsj.com/articles/target-reaches-19-million-settlement-with-mastercard-over-data-breach-1429136237.
58 Tina Orem, Target/MasterCard Settlement Deal Dead, Credit Union Times, (May 21, 2015), http://www.cutimes.com/2015/05/21/target-mastercard-settlement-deal-dead.
59 Shannon Pettypiece & Elizabeth Dexheimer, Target Reaches $67 Million Agreement with Visa Over Breach, Bloomberg Business, (Aug. 18, 2015, 5:59 PM), http://www.bloomberg.com/news/articles/2015-08-18/target-says-it-has-reached-settlement-with-visa-over-data-breach (last updated Aug. 18, 2015, 5:59 PM).
60 Tina Orem, Target Suit Wins Class Action Status, Credit Union Times, (Sept. 15, 2015), http://www.cutimes.com/2015/09/15/target-suit-wins-class-action-status.
61 See Collier v. Steinhafel, No. 0:14-CV-00266, 2014 WL 321798 (D. Minn. Jan. 29, 2014).
62 *Id.*
63 See, *e.g.*, Protecting Personal Consumer Information from Cyber Attacks and Data Breaches: Hearing Before the S. Comm. On Commerce, Sci., & Transp., (Mar. 26, 2014), *available at* https://corporate.target.com/_media/TargetCorp/global/PDF/Target-SJC-032614.pdf (written testimony of John Mulligan, Executive V.P. and C.F.O., Target); see also Under Attack: Federal Security and the OPM Data Breach: Hearing Before the S. Comm. on Homeland Security and Governmental Affairs, (June 25, 2015), *available at* https://www.opm.gov/news/testimony/114th-congress/under-attack-federal-cybersecurity-and-the-opm-data-breach.pdf (statement of Hon. Katherine Archuleta, Director, U.S. Office of Personal Management).
64 See Susan Taylor et al., Target's Decision to Remove CEO Rattles Investors, Reuters, (May 5, 2014, 5:32 PM), http://www.reuters.com/article/2014/05/05/us-target-ceo-idUSBREA440BD20140505.
65 Paul Ziobro & Joann S. Lublin, ISS's View on Target Directors Is a Signal on Cybersecurity, Wall St. J., http://www.wsj.com/articles/iss-calls-for-an-overhaul-of-target-board-after-data-breach-1401285278 (last updated May 28, 2014, 6:28 PM).
66 Nelson & Tau, *supra* note 9.
67 Commissioner Luis A. Aguilar, Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus, Cyber Risks and the Boardroom Conference, New York Stock Exchange (June 10, 2014), *available at* http://www.sec.gov/News/Speech/Detail/Speech/1370542057946.
68 U.S. Dep't of Just., Cybersecurity Unit, http://www.justice.gov/criminal-ccips/cybersecurity-unit (last updated May 26, 2015).
69 Cybersecurity Unit, Best Practices for Victim Response and Reporting of Cyber Incidents, U.S. Dep't of Just. (April 2015), http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf.
70 U.S. Dep't of Just., Cybersecurity Unit, http://www.justice.gov/criminal-ccips/cybersecurity-unit (last updated May 26, 2015).
71 See Cybersecurity Unit, Best Practices, *supra* note 69 at 5; Fed. Bureau of Investigation, FBI – Computer Intrusions, https://www.fbi.gov/about-us/investigate/cyber/computer-intrusions.
72 U.S. Dep't of Homeland Sec., Combating Cyber Crime, http://www.dhs.gov/topic/combating-cyber-crime (last updated Sept. 23, 2015).
73 Noeleen Walder, Jonathan Stempel, & Joseph Ax, Hackers Stole Secrets For Up to $100 Million Insider-Trading Profit: U.S., Reuters, (Aug. 12, 2015, 5:02 AM),

http://www.reuters.com/article/2015/08/12/us-cybercybersecurity-hacking-stocks-arr-idUSKCN0QG1EY20150812.

74 Press Release, Fed. Bureau of Investigations , Major Computer Hacking Forum Dismantled, (July 15, 2015), https://www.fbi.gov/pittsburgh/press-releases/2015/major-computer-hacking-forum-dismantled.

75 *Id.*

76 Press Release, U.S. Dep't of Just., Manhattan U.S. Attorney and FBI Assistant Director-In-Charge Announce Charges In Connection with Blackshades Malicious Software That Enabled Users Around The World to Secretly And Remotely Control Victims' Computers (May 19, 2014), http://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-and-fbi-assistant-director-charge-announce-charges-connection.

77 Sarah N. Lynch, U.S. SEC on the Prowl for Cyber Security Cases—Official, Reuters, (Feb. 20, 2015, 4:07 PM), http://www.reuters.com/article/2015/02/20/sec-cyber-idUSL1N0VU2AV20150220 (quoting David Glockner).

78 *Id.*

79 CF Disclosure Guidance: Topic No. 2, Cybersecurity, Div. of Corp. Fin., U.S. Sec. & Exch. Comm'n (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

80 *Id.*

81 *Id.*

82 *Id.*

83 *Id.*

84 *Id.*

85 See Letter from Mary Jo White, Chair, Sec. & Exch. Comm'n, to Hon. John D. Rockefeller IV, Chairman, U.S. S. Comm. on Commerce, Sci., & Transp., (May 1, 2013), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=7b54b6d0-e9a1-44e9-8545-ea3f90a40edf (stating that "the staff issued comments addressing cybersecurity matters to approximately 50 public companies of varying size and in a wide variety of industries"); see, *e.g.*, Letter from Karl Hiller, Branch Manager, to Ira M. Birns, Exec. Vice President and Chief Fin. Officer, World Fuel Services Corp. (Mar. 20, 2015), *available at* http://www.sec.gov/Archives/edgar/data/789460/000000000015016935/filename1.pdf; Letter from Mara L. Ransom, Assistant Dir., to Jon Kessler, President and Chief Fin. Officer, HealthEquity, Inc. (May 1, 2014), *available at* http://www.sec.gov/Archives/edgar/data/1428336/000000000014022132/filename1.pdf;Letter from Linda Cvrkel, Branch Chief, to Joseph Ceryanec, Chief Fin. Officer, Meredith Corp. (Feb. 6, 2014), *available at* http://www.sec.gov/Archives/edgar/data/65011/000000000014006410/filename1.pdf.

86 See, *e.g.*, Cory Bennett, SEC Weighs Cybersecurity Disclosure Rules, The Hill, (Jan. 14, 2015, 6:00 AM), http://thehill.com/policy/cybersecurity/229431-sec-weighs-cybersecurity-disclosure-rules.

87 Division of Investment Management, U.S. Sec. & Exch. Comm'n, http://www.sec.gov/divisions/investment/investment_about.shtml (last updated Aug. 1, 2013).

88 Office of Compliance Inspections and Examinations, U.S. Sec. & Exch. Comm'n, http://www.sec.gov/ocie (last updated Sept. 22, 2015).

89 Div. of Inv. Mgmt., U.S. Sec. & Exch. Comm'n, IM Guidance Update, No. 2015-02 (April 2015), *available at* http://www.sec.gov/investment/im-guidance-2015-02.pdf.

90 *Id.*

91 *Id.*

92 Office of Compliance Inspections & Examinations, U.S. Sec. & Exch. Comm'n, OCIE Cybersecurity Initiative, National Exam Program Risk Alert, Vol. IV, Issue 2 (Apr. 15, 2014), *available at* http://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf.
93 *Id.*
94 Office of Compliance Inspections & Examinations, U.S. Sec. & Exch. Comm'n, Cybersecurity Examination Sweep Summary, National Exam Program Risk Alert, Vol. IV, Issue 4 (Feb. 3, 2015), *available at* https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.
95 *Id.*
96 See Target Hackers Broke in Via HVAC Company, KrebsonSecurity, (Feb. 5, 2014), http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.
97 Cybersecurity Examination Sweep Summary, *supra* note 94.
98 *Id.*
99 Office of Compliance Inspections & Examinations, U.S. Sec. & Exch. Comm'n, OCIE's 2015 Cybersecurity Examination Initiative, National Exam Program Risk Alert, Vol. IV, Issue 8 (Sept. 15, 2015), *available at* http://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.
100 *Id.*
101 17 C.F.R. § 248.30(a).
102 See, *e.g.*, Order Instituting Admin. and Cease-and-Desist Proceedings, Pursuant to Sections 15(b) and 21C of the Sec. Exch. Act of 1934, Making Findings, and Imposing Remedial Sanctions and a Cease-and-Desist Order, In re Marc. A. Ellis, Sec. Exch. Act Release No. 64220, File No. 3-14328 (Apr. 7, 2011), *available at* http://www.sec.gov/litigation/admin/2011/34-64220.pdf; Letter of Acceptance, Waiver, and Consent, Dept. of Enforcement, Fin. Indus. Reg. Auth., No. 20080152998, In re D.A. Davidson & Co. (Apr. 9, 2010), *available at* http://www.securityprivacyandthelaw.com/uploads/file/4_9_2010%20FINRA%20Letter%20of%20Acceptance.pdf; Order Instituting Admin. and Cease-and-Desist Proceedings Pursuant to Sections 15(b) and 21c of the Sec. Exch. Act of 1934 and Sections 203(e) and 203(k) of the Inv. Advisers Act of 1940, Making Findings, and Imposing Remedial Sanctions and a Cease-and-Desist Order as To LPL Financial Corp., In re LPL Financial Corp., Sec. Exch. Act Release No. 58515, File No. 3-13181 (Sept. 11, 2008), *available at* http://www.sec.gov/litigation/admin/2008/34-58515.pdf.
103 See Lynch, *supra* note 77.
104 Press Release, U.S. Sec. & Exch. Comm'n, SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach (Sept. 22, 2015), http://www.sec.gov/news/pressrelease/2015-202.html.
105 *Id.*
106 *Id.*
107 See Sec. & Exch. Comm'n Release No. 34-73639, File No. S7-01-13, RIN 3235-AL43 (Nov. 19, 2014), *available at* http://www.sec.gov/rules/final/2014/34-73639.pdf.
108 *Id*; see also 17 C.F.R. § 242 (2015).
109 Fin. Indus. Regulatory Auth., Report on Cybersecurity Practices (Feb. 2015), https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.
110 News Release, Fin. Indus. Regulatory Auth., FINRA Fines D.A. Davidson & Co. $375,000 for Failure to Protect Confidential Customer Information (Apr. 12, 2010), http://www.finra.org/newsroom/2010/finra-fines-da-davidson-co-375000-failure-protect-confidential-customer-information.

111 News Release, Fin. Indus. Regulatory Auth., Disciplinary and Other FINRA Actions, at 11 (July 2015), http://www.finra.org/sites/default/files/publication_file/July_2015_Disciplinary_Actions.pdf.
112 Emily Field, FCC Head Says Companies Must Be Cybersecurity Leaders, Law360, (Apr. 22, 2015, 6:19 PM), http://www.law360.com/articles/646465/fcc-head-says-companies-must-be-cybersecurity-leaders.
113 Sue Reisinger, FCC Fines AT&T $25M: Agency's Largest Cyber Enforcement, Corporate Counsel, (Apr. 14, 2015), http://www.corpcounsel.com/id=1202723349349/FCC-Fines-AT38T-3625M-Agencys-Largest-Cyber-Enforcement?slreturn=20150816162248.
114 *Id.* (quoting the FCC).
115 HIPAA Administrative Simplification Statute and Rules, U.S. Dep't of Health & Human Services, http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html.
116 News Release, U.S. Dep't of Health & Human Services, Data Breach Results in $4.8 million HIPAA Settlements (May 7, 2014), http://www.hhs.gov/news/press/2014pres/05/20140507b.html.
117 Gigi Stevens, Cong. Research Serv., The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority 6 (Sept. 11, 2014), https://www.fas.org/sgp/crs/misc/R43723.pdf; see also *Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime: Hearing Before the S. Comm. on the Judiciary*, (Feb. 4, 2014), (statement of Chairwoman Edith Ramirez), *available at* https://www.ftc.gov/system/files/documents/public_statements/oral-statement-federal-trade-commission-privacy-digital-age-preventing-data-breaches-combating/2014-02-04_judiciary_opening_statement_final.pdf.
118 *See* FTC v. Wyndham Worldwide Corp., No. 14-3514, 2015 WL 4998121 (3d Cir. Aug. 24, 2015).
119 *Id.* at *7.
120 FED. TRADE COMM'N, FTC FACTS FOR BUSINESS: COMPLYING WITH THE FTC'S HEALTH BREACH NOTIFICATION RULE 1 (Apr. 2010), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus56-complying-ftcs-health-breach-notification-rule.pdf.
121 *Id.*
122 Matthew Goldstein, *State Attorneys General Press JPMorgan for More Details on Hacking*, N.Y. TIMES, (Jan. 14, 2015, 12:35 PM), http://dealbook.nytimes.com/2015/01/14/state-attorneys-general-press-jpmorgan-chase-for-more-details-on-hacking.
123 Cory Bennett, *State AGs Clash with Congress Over Data Breach Laws*, THE HILL, (July 7, 2015, 5:32 PM), http://thehill.com/policy/cybersecurity/247118-state-ags-warn-congress-against-preempting-data-breach-laws.
124 FIN. STABILITY OVERSIGHT COUNCIL, 2015 ANNUAL REPORT 102 (2015), *available at* http://www.treasury.gov/initiatives/fsoc/studies-reports/Documents/2015%20FSOC%20Annual%20Report.pdf.
125 *Id.* at 3.
126 *Id.* at 9.
127 OFFICE OF THE COMPTROLLER OF THE CURRENCY, SEMIANNUAL RISK PERSPECTIVE FROM THE NATIONAL RISK COMMITTEE, (Spring 2015), *available at* http://www.occ.gov/publications/publications-by-type/other-publications-reports/semiannual-risk-perspective/semiannual-risk-perspective-spring-2015.pdf.
128 *Id.* at 10.
129 Sarah Dahlgren, Exec. Vice President, Fed. Reserve Bank of N.Y., Remarks at the OpRisk North America Annual Conference, New York City (Mar. 24, 2015), *available at* http://www.newyorkfed.org/newsevents/speeches/2015/dah150324.html.
130 McKendry & Macheel, *supra* note 12.
131 GAO-15-509, *supra* note 19, at 19-20

132 *Id.* at 20-21.
133 *Id.* app. 2, at 55-59.
134 12 C.F.R. Pt. 30, App. B (2014).
135 *Id.*
136 *Id.*
137 15 U.S.C. § 6801(b).
138 *See* Patco Const. Co. v. People's United Bank, 684 F.3d 197, 213 (1st Cir. 2012) (holding that bank's security procedures were not "commercially reasonable" based, in part, on the bank's failure to implement FFIEC guidance).
139 PONEMON INSTITUTE, *2015 Cost of Data Breach Study: Global Analysis,* IBM 1 (May 2015), http://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.pdf.
140 Commissioner Luis A. Aguilar, *supra* note 67.
141 LARRY CLINTON, NAT'L ASS'N OF CORP. DIRECTORS, *Cyber-Risk Oversight, Director's Handbook Series* 4 (2014), *available at* https://na.theiia.org/standards-guidance/Public%20Documents/NACD-Financial-Lines.pdf.
142 FED. FIN. INST. EXAMINATION COUNCIL, *FFIEC Cybersecurity Assessment Tool, Overview for Chief Executive Officers and Boards of Directors* (June 2015), https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf.
143 Fed. Fin. Insts. Examination Council, *supra* note 142, at 2.
144 PWC, *US Cybersecurity*, *supra* note 1, at 10.
145 Press Release, Office of the Press Sec'y, Fact Sheet: Administration Cybersecurity Efforts 2015 (July 9, 2015), *available at* https://www.whitehouse.gov/the-press-office/2015/07/09/fact-sheet-administration-cybersecurity-efforts-2015.
146 Banks are positioned differently than most other companies because they have to defend against the threat on two fronts: (1) their own networks, and (2) fraudulent charges or transfers/withdrawals out of a customer's account when the *customer* has been the victim of a data breach elsewhere. Security measures that address the latter can impose additional burdens on customers, which raises other concerns, but it is fair to expect that they too will become more accustomed to—and more accepting of—some added inconvenience for the sake of enhanced security given the current climate.
147 GAO-15-509, *supra* note 19.
148 *Id.* at 24-25.
149 *Id.* at 45.
150 James O'Toole, *JPMorgan: 76 Million Customers Hacked,* CNN MONEY, (Oct. 3, 2014, 8:00 AM), http://money.cnn.com/2014/10/02/technology/security/jpmorgan-hack.
151 Emily Glazer, *J.P. Morgan CEO: Cybersecurity Spending to Double*, WALL ST. J., http://www.wsj.com/articles/j-p-morgans-dimon-to-speak-at-financial-conference-1412944976 (last updated Oct. 10, 2014, 5:57 PM).
152 GAO-15-509, *supra* note 19, at 1.
153 *See id.* at 13.
154 *Id.* at 27.
155 *Id.* at 28.
156 *Id.* at 29.
157 *Id.*
158 *Id.*
159 *Id.* at 33.
160 Cybersecurity Examination Sweep Summary, supra note 94, at 4.
161 GAO-15-509, *supra* note 19, at 34.

162 Testimony of Wm. Douglas Johnson, *supra* note 25.
163 GAO-15-509, *supra* note 19, at 34.
164 *Id.*
165 MANDIANT, A View From The Front Lines, supra note 18, at 1.
166 GAO-15-509, *supra* note 19, at 39.
167 *Id.*
168 *Id.*
169 VERIZON, *Data Breach Investigations Report*, *supra* note 17, at 10-11 (citing Risk Analytics data).
170 GAO-15-509, *supra* note 19, at 42.
171 *Treasury's Raskin Focusing on Improving Cyber Info-Sharing*, ABA BANKING JOURNAL, (July 14, 2015), http://bankingjournal.aba.com/2015/07/treasurys-raskin-focusing-on-improving-cyber-info-sharing (quoting Raskin).
172 GAO-15-509, *supra* note 19.
173 Exec. Order No. 13,691, 80 Fed. Reg. 9349 (Feb. 13, 2015).
174 Ellen Nakashima & Katie Zezima, *Obama to Propose Legislation to Protect Firms that Share Cyberthreat Data*, Wash. Post, (Jan. 12,2015), http://www.washingtonpost.com/politics/obama-proposes-legislation-to-protect-consumer-data-student-privacy/2015/01/12/539c4a06-9a8f-11e4-bcfb-059ec7a93ddc_story.html.
175 Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong., 1st Session (2015); Protecting Cyber Networks Act, H.R. 1560, 114thCong. 1st Session (2015); National Cybersecurity Protection Advancement Act, H.R. 1730, 114th Cong., 1st Session (2015).
176 Fed. Fin. Inst. Examination Council, *supra* note 142, at 1.
177 *Id.* at 11.
178 *Id.* at 19-57.