June 24, 2015

Cyber-Attacks: Threats, Regulatory Reaction and Practical Proactive Measures to Help Avoid Risks

I. Cybersecurity; Its Importance and Relevance – How We Got to Where We Are Today

In the past few months, the White House, Home Depot, JP Morgan, Hard Rock Hotels, Tesla, the St. Louis Federal Reserve, the Internal Revenue Service and many other institutions have suffered well-publicized cybersecurity breaches.[1] In fact, very recently the Office of Personnel Management — the agency that manages background checks, pension payments and job training for the federal government — announced that it suffered a cyber-attack in which it believes that hackers stole the personal information of more than 4 million federal employees.[2] In a recent survey of more than 800 information technology (IT) security professionals across 19 industries in seven countries, more than half of the respondents said they will "likely" be victim to a successful cyber-attack this year, and almost three quarters of the respondents disclosed that they fell victim to successful cyber-attacks in the prior year.[3] In fact, the Depository Trust and Clearing Corporation recently disclosed in its 2015 *Systemic Risk Barometer Study* that almost half of the respondents listed cybersecurity as their top concern, and more than three quarters listed it among their top five overall concerns.[4]

As a result, it is often said that there are only two types of financial services firms: those that have experienced cybersecurity breaches and addressed them, and those that have experienced cybersecurity breaches and are unaware.[5]

Cybersecurity is multifaceted, and what it entails differs for every financial services firm. The risks of a cybersecurity breach, in addition to significant reputational harm, include loss of proprietary and confidential customer data, trade secrets and employee information; the resulting costs of mitigation (voluntary and as mandated by law); impairment of operations;

[1] *See* http://thehill.com/policy/cybersecurity/238127-white-house-state-dept-cyberattacks-linked, http://money.cnn.com/2014/09/08/technology/security/home-depot-breach/, http://www.cnbc.com/id/102644470, http://www.bloomberg.com/news/articles/2015-04-25/tesla-hacked-on-twitter-media-relations-e-mail-accounts, http://http://www.nytimes.com/2015/05/20/technology/st-louis-fed-confirms-hacking-attack.html, *see also* infra note 17. Most recently, a popular online dating service has sustained a highly publicized cybersecurity breach, causing an embarrassing disclosure of patrons' sexual proclivities. *See* http://money.cnn.com/2015/05/22/technology/adult-friendfinder-hacked/index.html.

[2] *See* http://www.politico.com/story/2015/06/personal-data-of-4-million-federal-employees-hacked-118655.html.

[3] *See* "2015 Cyber Threat Defense Report."

[4] *See* the 2015 first quarter "Systemic Risk Barometer Results Overview."

[5] *See* remarks of Robert S. Mueller, III, Director Federal Bureau of Investigation at the RSA Cyber Security Conference, San Francisco, CA (March 1, 2012), *see also* Bits Blog, "Hacked vs. Hackers: Game On" (Dec. 2, 2014).

For more information, please contact any of the following members of Katten's **Financial Services**, **Privacy, Data and Cybersecurity**, or **Litigation and Dispute Resolution** practices.

Alan J. Brudner
+1.212.940.6362
alan.brudner@kattenlaw.com

Wendy E. Cohen
+1.212.940.3846
wendy.cohen@kattenlaw.com

Gary DeWaal
+1.212.940.6558
gary.dewaal@kattenlaw.com

David Y. Dickstein
+1.212.940.8506
david.dickstein@kattenlaw.com

Doron S. Goldstein
+1.212.940.8840
doron.goldstein@kattenlaw.com

Dina Wegh
+1.212.940.6704
dina.wegh@kattenlaw.com

and litigation and regulatory actions. Various financial regulators recently have commenced enforcement actions utilizing tangentially related cybersecurity theories of liability. Analyzing some of these actions can give insight into the types of issues concerning financial regulators today.

This Advisory discusses various financial regulators' public views and initiatives relevant to cybersecurity as well as relevant disciplinary actions, and assimilates this information into a checklist of practical steps firms may take to protect themselves against cyber-attacks, as well as to minimize their potential liability. However, it is important to recognize that different measures are appropriate for each firm.

Actions by Industry Regulators in Recent Years

i. SEC

Rule 30 of Securities and Exchange Commission (SEC) Regulation S-P, known as the "Safeguards Rule," mandates that investment advisers, broker-dealers and investment companies create and maintain reasonably designed written policies and procedures to protect the security and confidentiality of customer records and information.[6] Citing Regulation S-P, the SEC has charged brokerage executives with failing to protect confidential information about their customers. In three separate cases, individuals charged under Regulation S-P settled with the SEC and paid fines between $15,000 and $20,000, as well as consented to orders that required them to cease and desist from committing any violations of the provisions charged.[7] The charges included violations of the law by transferring customers' private data without giving the customers a chance to opt out and ignoring red flags from security breaches at the plaintiffs' respective firms.

In additional actions brought by the SEC under Regulation S-P, the SEC found liability where a broker-dealer's written policies and procedures were too short and vague,[8] and only provided limited guidance rather than a "complete set of . . . policies and procedures addressing administrative, technical and physical safeguards reasonably designed to protect customer records and information."[9] In another action, the SEC held a broker-dealer liable where its policies and procedures did not address what to do in the instance of a breach. In that case, the SEC fined the firm's chief compliance officer individually under a theory that he aided and abetted the violation because he did not remedy the inadequate procedures.[10] While the aforementioned actions were brought against broker-dealers, to the extent that they were enforced under Regulation S-P, they apply equally to investment advisers.[11]

To control for cyber-attacks and breaches at the exchange level, the SEC adopted Regulation System Compliance and Integrity (Regulation SCI) to govern the technology infrastructure of most self-regulatory organizations, certain alternative trading systems, plan processors and certain clearing agencies in the United States (collectively, SCI Entities).[12] In the event of a cyber-attack or other disruption, SCI Entities are required to take corrective action, and notify the SEC and affected members or participants.

---

6 *See* https://www.sec.gov/rules/final/34-42974.htm.

7 *See* http://www.sec.gov/news/press/2011/2011-86.htm.

8 Exchange Act Release No. 58515, Admin. Proc. File No. 3-13181, at 4 (Sept. 11, 2008) (finding that the firm violated Regulation S-P), *available at* http://www.sec.gov/litigation/admin/2008/34-58515.pdf.

9 Exchange Act Release No. 58515, Admin. Proc. File No. 3-13181, at 4 (Sept. 11, 2008) (finding that the firm violated Regulation S-P), *available at* http://www.sec.gov/litigation/admin/2008/34-58515.pdf.

10 Exchange Act Release No. 64220, Admin. Proc. File No. 3-14328, at 3 (April 7, 2011) (finding that the firm violated Regulation S-P), *available at* http://www.sec.gov/litigation/admin/2011/34-64220.pdf.

11 In addition to Regulation S-P, the SEC also could bring actions against investment advisers for having inadequate information securities programs based on other federal securities laws including the following: (1) violations of Rule 204A-1 (the Code of Ethics Rule) under the Investment Advisers Act of 1940, as amended (Advisers Act). *See Investment Adviser Codes of Ethics*, Investment Advisers Act Release No. 2256 (July 2, 2004), where the SEC stated that the Code of Ethics Rule will renew investment advisers' "attention to their fiduciary and other legal obligations, and [increase] their vigilance against inappropriate behavior by employees;" (2) breaches of Regulation S-ID: Identity Theft Red Flags rules, *see Identity Theft Red Flag Rules*, Investment Advisers Act Release No. 3582 (April 10, 2013); (3) breaches of an investment advisers' fiduciary duties. *See Compliance Programs of Investment Companies and Investment Advisers*, Investment Company Act Release No. 26299 (Dec. 17, 2003) at n. 22 where the SEC stated an "adviser's fiduciary obligation to its clients includes obligations to its clients from being placed at risk as a result of the adviser's inability to provide advisory services."

12 *See* http://www.sec.gov/rules/final/2014/34-73639.pdf.

ii. CFTC and NFA

Similar to Regulation S-P above, all National Futures Association (NFA) Members must comply with federal privacy laws and the Commodity Futures Trading Commission's (CFTC) regulations applying those laws to futures firms.[13] Accordingly, and parallel to the Regulation S-P requirements, NFA Members must have written policies and procedures that describe their protections for customer records and information. The procedures must be reasonably designed to "(1) keep customer records and information secure and confidential, (2) protect against any anticipated hazards to the security or integrity of those records and (3) protect against unauthorized access to or use of the records or information."[14]

In *In Re Interbank FX, LLC*, the CFTC sanctioned Interbank for failing to adopt policies and procedures that address the administrative, technical and physical safeguards for the protection of customer records as required under Regulation 160.30 of Title V of the Gramm-Leach-Bliley Act.[15] The sanctions included a fine of $200,000 and an order that Interbank undertake to implement and maintain a comprehensive security program to address the protection of private customer data.

iii. FINRA

National Association of Securities Dealers (NASD) Rule 3010 requires that each Financial Industry Regulatory Authority- (FINRA) regulated firm create and maintain a system with written policies and procedures to supervise the activities of each registered representative or associated person to ensure compliance with applicable securities laws and regulations. Accordingly, FINRA cites Regulation S-P and NASD Rule 3010 to bring enforcement actions against Member firms. In one instance, a Member firm agreed to pay a $150,000 fine for failing to adequately maintain safeguards to detect and report breaches of private customer information.[16]

In another example, in March 2015, citing NASD Rule 3010, FINRA fined a Member firm, OptionsXpress, $150,000 for permitting an identity thief to illicitly transfer funds.[17] FINRA held OptionsXpress liable because its written supervisory policies and procedures to review transfers of funds from customer accounts to outside bank accounts were deemed inadequate.[18] FINRA charged OptionsXpress for not sufficiently following up on red flags in connection with transactions that appeared on an internal exception report that identified potentially suspicious conduct. As a result of the unauthorized activity, in March and April 2012, the relevant customer sustained losses totaling $443,000 that the firm ultimately reimbursed. Among the ignored red flags, the identity thief, pretending to be the OX customer, (i) contacted the OX customer service center and was not able to correctly answer security questions; (ii) called the OX customer service center using Skype, evidencing a heavy Eastern European accent, and did not appear to understand English, even though the actual customer lived in Illinois; and (iii) repeatedly accessed the customer's account from a Texas IP address (when the customer was living in Illinois) with numerous failed efforts to reset the account security personal identification number.

On May 5, 2015, citing Regulation S-P and NASD Rule 3010, FINRA fined a Member firm $225,000 when one of its employees left his unencrypted work computer in a public restroom and private customer information was placed at risk. The firm's policies and procedures did not provide for the encryption of laptops because firm management believed that, due to the low number of issued work computers, encryption was not necessary.[19]

iv. FTC

Rule 314 of the Federal Trade Commission (FTC) rules (FTC Safeguards Rule) also requires financial institutions to adopt comprehensive information security programs to protect customer information. While Rule 30 of Regulation S-P governs protection

---

[13] *See* infra note 35.

[14] *See* https://www.nfa.futures.org/NFA-compliance/publication-library/regulatory-requirements-guide.pdf.

[15] *In re Interbank FX, LLC*, CFTC Docket No. 09-11 (CFTC filed June 29, 2009).

[16] Letter of Acceptance, Waiver and Consent No. 2010022554701, at 2, 5 (April 9, 2012), *available at* http://disciplinaryactions.finra.org/Search/ViewDocument/31594.

[17] Approximately 100,000 taxpayers recently were subject to a similar identity theft fraud perpetrated by criminals on the US Internal Revenue Service. *See* http://www.nytimes.com/2015/05/28/business/irs-data-breach-may-be-sign-of-more-personalized-schemes.html.

[18] *See* http://disciplinaryactions.finra.org/Search/ViewDocument/38882.

[19] *See* http://disciplinaryactions.finra.org/Search/ViewDocument/51064.

of individual "customer" privacy data, the FTC Safeguards Rule is the federal information security protection regulation that requires private investment fund advisers to adopt procedures to protect the information of private investment fund investors.[20] Private investment funds, but not their underlying investors, are deemed "clients" under the Advisers Act. Since the funds are not individuals, Rule 30 does not apply. Conversely, the FTC Safeguards Rule applies to "customers" of *financial institutions*. The FTC could view the individual investors in such funds as "customers" of the funds. Consequently, the FTC's enforcement of the FTC Safeguards Rule is relevant to private investment fund managers. The FTC has brought numerous cases to enforce the FTC Safeguards Rule, and could try to bring similar actions against private investment funds for information security breaches.[21]

v. State Requirements

In addition to federal law and regulations, to date, 47 states and the District of Columbia, Puerto Rico, Guam and the US Virgin Islands have privacy laws, which require entities to promptly notify individuals whose information was compromised or thought to be compromised, and the majority of them provide a private right of action.[22]

vi. DOJ

In April 2015, the US Department of Justice (DOJ) released a 15-page document titled "Best Practices for Victim Response and Reporting of Cyber Incidents."[23] In addition to practical advice about incident response planning, the DOJ suggests notifying the relevant authorities promptly in the event of a breach because, among other things, the knowledge and experience of agencies such as the DOJ and FBI in dealing with particular types of breaches and particular criminal parties may be valuable in getting more quickly and accurately to the bottom of what happened in a particular instance.

II. Cybersecurity – The Current Regulatory Environment

Background

As a result of the increased volume and scope of cyber-attacks in recent years, various regulators and even the President of the United States,[24] have published cybersecurity "best practices." While the SEC, FINRA, CFTC and NFA have yet to enact specific regulations imposing cybersecurity requirements (other than Regulation SCI in the securities industry), cybersecurity is a growing concern of each of these regulatory bodies and, as elaborated below, more regulatory initiatives likely are forthcoming.[25] Additionally, the National Institute of Standards and Technology (NIST), a non-regulatory agency of the US Department of Commerce with a mission to promote industrial innovation and competitiveness, developed a cybersecurity framework that includes "a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks."[26] The framework, which all firms, including financial services firms, are strongly encouraged to use,[27] provides a structure to create, guide, assess and/or improve comprehensive cybersecurity programs, and is a helpful tool for

---

[20] *See* 16 CFR part 314, *Standards for Safeguarding Customer Information*.

[21] *See* e.g., In the Matter of Nationwide Mortgage Group Inc., (finding that Nationwide Mortgage Group violated the safeguards rule by failing to conduct privacy risk assessments), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2005/04/050415dod9319.pdf.

[22] *See* http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[23] *See* http://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf.

[24] *See* Executive Order 13636.

[25] The NFA is expected to enact requirements regarding cybersecurity for Members by the end of 2015, *see* "Testimony of Daniel J. Roth, President and CEO of the NFA before the Subcommittee on Commodity Exchanges, Energy, and Credit of the Committee on Agriculture of the U.S. House of Representatives." Additionally, the CFTC has incorporated cyber concerns into its regulations and is looking at private companies that run major exchanges and clearinghouses to determine if they are adequately testing their cyber protections, *see* "Testimony of Chairman Timothy G. Massad before the U.S. Senate Committee on Appropriations, Subcommittee on Financial Services and General Government."

[26] *See* "Framework for Improving Critical Infrastructure Cybersecurity."

[27] *See* https://www.whitehouse.gov/the-press-office/2014/02/12/launch-cybersecurity-framework, http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf, http://www.natlawreview.com/article/where-are-we-now-nist-cybersecurity-framework-one-year-later.

firms in developing their cybersecurity policies. Moreover, the federal government as well as a majority of states have enacted cybersecurity laws.[28]

i. The SEC Makes Cybersecurity a Priority

In 2014 and 2015, the SEC's Office of Compliance Inspections and Examinations (OCIE) included cybersecurity in its examination priorities. In 2014, OCIE listed "information technology" as an area that would continue to be examined, and included "cybersecurity" in a list of items on which its staff would focus with respect to the core risks of trading.[29] In 2015, OCIE's examination priorities include cybersecurity as a market-wide risk that will be scrutinized by the SEC.[30]

A few months after OCIE released its 2014 exam priorities, the SEC hosted a roundtable on cybersecurity.[31] In her opening remarks at the roundtable, SEC Chairman Mary Jo White opined that the threats on cybersecurity are global and pose a grave risk to our economy. Chairman White also stated that such risks are "first on the Division of Intelligence's list of global threats, even surpassing terrorism."[32] Panelists at the roundtable included government officials, service providers, investors and academics, all of whom shared their perspective on evaluating and addressing cybersecurity challenges.[33] Many of the panelists referenced the utility of the NIST framework,[34] but cautioned that the framework should not be viewed as a one-size-fits-all approach for dealing with cybersecurity risks.

At the SEC roundtable, cyber-attack perpetrators were categorized as follows:

- those seeking to steal national security secrets or intellectual property;
- organized criminals seeking to steal people's identity and money;
- terrorists desiring to attack a firm's infrastructure;
- "hacktivists" attempting to make a social statement by stealing information and publishing it to embarrass organizations or extort them; and
- insiders or people whose employment was terminated on bad terms.

The roundtable also identified the primary methods used to carry out cyber-attacks, including:

- the destruction of data or hardware;
- denial of service;
- theft of information, money or identity; and
- ransomware, which encrypts files until a ransom is paid.

ii. The CFTC Makes Cybersecurity a Priority

On February 26, 2014, the CFTC's Division of Swap Dealer and Intermediary Oversight issued recommended best practices for futures commission merchants, commodity trading advisors, commodity pool operators, introducing brokers, retail foreign exchange dealers, swap dealers and major swap participants.[35] The best practices highlight the steps registrants should take to secure the financial information of their customers in compliance with rules regarding customers' privacy, security and confidentiality under the Gramm-Leach-Bliley Act.

---

[28] *See* supra note 22, see also *Federal Information Security Modernization Act of 2014*.

[29] OCIE, "Examination Priorities for 2014" (Jan. 9, 2014).

[30] OCIE, "Examination Priorities for 2015" (Jan. 13, 2015).

[31] *See* a transcript of the Cybersecurity Roundtable.

[32] *Id.*

[33] SEC Press Release, "SEC Announces Agenda, Panelists for Cybersecurity Roundtable."

[34] *See* Supra note 26.

[35] Division of Swap Dealer and Intermediary Oversight, "Gramm-Leach-Bliley Act Security Safeguards" (Feb. 26, 2014).

Recognizing that cybersecurity is a growing problem, the CFTC addressed cybersecurity in its Information Technology Strategic Plan 2014-2018[36] and included funding to address the threat in its proposed budget for the 2016 fiscal year.[37] Moreover, CFTC Chairman Timothy Massad recently testified before the US House Committee on Agriculture and said, "Cybersecurity is perhaps the single most important new risk to market integrity and financial stability." He elaborated that the CFTC has responded to the significant risk of cybersecurity by, among other things, modernizing its Core Principles[38] and requiring exchanges, clearinghouses and swap execution facilities to maintain system safeguards and risk management programs.[39]

Similar to the SEC, CFTC staff held a roundtable on cybersecurity and system safeguards testing.[40] The roundtable, which included participants from the private sector and government agencies, was comprised of four panels that addressed (i) the need for testing, vulnerability and penetration assessments; (ii) key controls testing; and (iii) business continuity and disaster recovery testing. The CFTC is expected, at some point this year, to draft a new rule on cybersecurity preparedness, system safeguards and testing for at least some of its registrants.

Discussions at the different panels at the CFTC roundtable seem to suggest that the expected new rule may rely on existing cybersecurity best practices, and it seems the rule likely will address issues such as the frequency with which testing should be performed and the suggested method of defining the scope of each test. Additionally, CFTC Commissioner Sharon Bowen recently stated that her attendance at the roundtable led to her interest in the Bank of England's use of the CBEST program to deliver targeted, intelligence-led cybersecurity tests to significant market players.[41] This interest led her to sponsor a Market Risk Advisory Committee on June 2, 2015, to provide an overview of the CBEST program.[42]

iii. FINRA Makes Cybersecurity a Priority

Like the SEC, FINRA included cybersecurity in its 2014 and 2015 examination priorities. In its 2014 exam priorities, FINRA said that "[it] continues to be concerned about the integrity of firms' infrastructure and the safety and security of sensitive customer data."[43] Additionally, FINRA noted that, with respect to monitoring such infrastructures, "FINRA's evaluation of such controls may take the form of examinations and targeted investigations."[44] Within a month of publishing the 2014 exam priorities, FINRA sent sweep letters asking various firms about their approach to handling cybersecurity.[45] In its 2015 exam priorities, FINRA listed "outsourcing" as a priority, and noted that its exams would specifically focus on what brokers are doing to make sure that their third-party vendors are in compliance with security regulations.

Regulators Identify Prevalent Weaknesses in Existing Cybersecurity Infrastructures

On April 15, 2014, a few weeks after the SEC's cybersecurity roundtable,[46] OCIE published a National Exam Program risk alert, entitled *OCIE Cybersecurity Initiative*.[47] In the risk alert, OCIE announced that it would be conducting cybersecurity

---

[36] *See* the CFTC's Information Technology Strategic Plan.

[37] *See* the CFTC's budget for fiscal year 2016.

[38] The Core Principles were established by the Dodd-Frank Wall Street Reform and Customer Protection Act and they set out requirements with which designated contract markets, swap execution facilities, derivatives clearing organizations and others must comply.

[39] *See* a transcript of the speech.

[40] *See* a transcript of the "CFTC Staff Roundtable on Cybersecurity and System Safeguarding."

[41] *See* "Statement of Commissioner Sharon Bowen before the Market Risk Advisory Committee" (June 2, 2015).

[42] *See* http://www.cftc.gov/ucm/groups/public/@aboutcftc/documents/file/mrac060215presentations_cbest.pdf.

[43] *See* FINRA 2014 Examination Priorities.

[44] *Id.*

[45] *See* FINRA Targeted Exam Letter.

[46] *See* supra note 31.

[47] *See* National Exam Program risk alert, "OCIE Cybersecurity Initiative."

examinations of more than 50 registered broker-dealers and investment advisers. However, the risk alert mainly consisted of a sample cybersecurity document request, the intent of which was to "empower compliance professionals in the industry with questions and tools they can use to assess their firms' level of preparedness, regardless of whether they are included in OCIE's examinations."[48] Additionally, in its 2015 exam priorities, FINRA said that it also will be conducting reviews of specific firms to determine their approaches to handling cybersecurity.[49, 50]

The purpose of these examinations was to help the various regulators (1) understand the types of threats firms face; (2) increase the regulators' understanding of firms' risk tolerance, exposure and major areas of vulnerabilities in their IT systems; (3) understand firms' approaches to managing these threats; and (4) share observations and findings with Member firms.

In general, these examination concluded that many of the examined firms (1) have adopted written information security policies; (2) conduct periodic risk assessments to identify cybersecurity threats, vulnerabilities and potential business consequences; (3) stated that they have experienced cyber-attacks directly or through one or more of their vendors; (4) identified best practices through information-sharing networks; (5) incorporated requirements relating to cybersecurity risk into their contracts with vendors and business partners; (6) made use of encryption in some form; and (7) confronted certain common principal risks, including hackers penetrating systems for account manipulation to destroy data, insiders or other authorized users abusing their access for personal purposes or to place time bombs or engage in other destructive activities, and non-nation states or terrorist groups entering systems to wreak havoc.[51]

Despite the somewhat encouraging results from the various examinations and surveys, the SEC and FINRA have made it clear that the threat of cyber-attacks is growing, the attacks are getting more sophisticated and financial services firms are not doing enough.

Regulators' Cybersecurity "Best Practices" For Financial Services Firms

To help financial services firms create and implement effective cybersecurity frameworks, various financial services regulators have published best practices for such firms. The best practices released by the SEC,[52] CFTC[53] and FINRA,[54] as well as the NIST framework,[55] all comprise similar ideas, including that effective programs should:

- designate a specific senior employee with privacy and security management oversight responsibilities (it is important to have a specific person who will be accountable for lapses in oversight and implementation of policy);
- identify foreseeable cybersecurity risks (it is impossible to identify all possible breaches, as cyber-attacks are always evolving; however, to mitigate damage, it is necessary to control for those that are identifiable);
- implement policies and procedures to avoid, detect and respond to cybersecurity breaches (once foreseeable cyber-attacks are identified, it is imperative to create policies to avoid security breaches);
- make sure staff is trained to detect and react to cybersecurity breaches;
- test cybersecurity policies regularly and, because cyber-attacks are always evolving, frequently update cybersecurity policies; and
- conduct vendor due diligence (financial regulators are making it increasingly clear that financial services firms will be liable for cyber-attacks as a result of improper controls at third-party service providers).

---

48 *Id.*

49 *See* FINRA 2015 Examination Priorities.

50 Similarly, the New York State Department of Financial Services conducted studies to determine how the banking sector is dealing with cybersecurity, *see* http://www.dfs.ny.gov/about/press2014/pr140505_cyber_security.pdf, and to determine how banking organizations are addressing cybersecurity risks associated with third-party vendors, *see* http://www.lexology.com/library/detail.aspx?g=7317437a-83c0-4477-888c-9292e4d02659.

51 *See* https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf, *see also* http://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.

52 SEC Guidance Update, Cybersecurity, *available at* http://www.sec.gov/investment/im-guidance-2015-02.pdf.

53 *See* supra note 35.

54 *See* FINRA "Report on Cybersecurity Practices."

55 *See* supra note 26.

III. Minimizing Litigation Exposure

Even with the best cybersecurity program, it is possible, if not probable, that a cyber-attack will occur and proprietary firm information, including customer data, will be compromised.

Once a breach has been detected, a firm will need to coordinate its review and response on several pressing fronts: identifying the cause of the incident and its extent; taking appropriate steps to prevent ongoing or future harm, such as suspending accounts, changing account numbers or passwords, or halting the use of certain systems; notifying regulators or other government officials; notifying and dealing with law enforcement; and notifying customers or others whose data has been compromised, as well as other parties who need to know, such as vendors and clearing firms.

A data breach must be viewed as a significant event unless and until the firm has determined otherwise. Accordingly, it must be treated as such — the firm must quickly take steps to: identify, collect and preserve evidence; analyze what happened, what data was misappropriated, and what systems were breached; determine, if possible, who was responsible; and determine if the system is still at risk. As quickly as possible, the firm also will want to determine how it can prevent or minimize further damage and prevent additional intrusions.

A firm also should have appointed a single individual to coordinate a response to a cyber-attack. In the event of a cyber-attack, this person should immediately take the leadership role in responding to the incident.

The firm also will need to ensure that internal personnel who need to know — legal and compliance, IT, operations, senior management and potentially media relations — are alerted to the issue. Retaining outside counsel at the outset can maximize the protections against future discovery afforded by the attorney-client privilege and work product doctrine, which may prove helpful in later litigation. The firm also will likely want to retain, or have its outside counsel retain, a data forensics firm to help in determining the cause, scope and potential remediation of the problem.

If the firm is a FINRA Member and customer information has been compromised, the SEC, CFTC and FINRA should be notified promptly.[56]

In addition, if customer confidential personally identifiable information (PII) has been stolen, a majority of the states and US territories have laws in place requiring a company to notify its customers.[57] These laws also contain provisions requiring that the state's attorney general or other responsible officials also be notified. These disclosures are generally required to be made as expediently as possible and without unreasonable delay, with exceptions for the needs of law enforcement as well as if the firm is taking measures necessary to determine the scope of the breach and restore the reasonable integrity of the system that suffered the breach.

Not surprisingly, data breaches have led to quite a bit of litigation by customers, clients or parties whose information was misappropriated. Many of the reported class actions have settled, and others are in early stages, so it is difficult to make general pronouncements.

However, one issue — standing — has emerged as having particular relevance in cybersecurity and data breach litigation. A party is permitted to bring a lawsuit in the federal courts only if he has suffered an actual or "concrete and imminent" injury; fear of a future theoretical harm is insufficient.[58] On this basis, several — but not all — federal courts have dismissed data breach cases

---

[56] *See* supra note 35, *see also* http://www.finra.org/industry/issues/customer-information-protection. FINRA's "Checklist for Compromised Accounts" sets forth a helpful list of issues to consider if a firm discovers that a customer's account has been compromised. *See* http://www.finra.org/industry/firm-checklist-compromised-accounts. These include, among others:

- taking action to monitor, limit or temporarily suspend activity in the account pending resolution of the situation;
- alerting others in the firm to be mindful of unusual activity in other accounts;
- appointing a central person or department to serve as a central contact for questions;
- identifying, if possible, the root cause of the intrusion; and
- if the firm is not self-clearing, notify the clearing firm.

[57] *See* supra note 22.

[58] *U.S. Const. Art. III; Clapper v. Amnesty Int'l, USA*, 568 U.S., 133 S. Ct. 1138 (2013).

where PII, such as credit card numbers or bank account information, was stolen but not yet misused.[59] On the one hand, courts have suggested that the taking of credit card information is not, in and of itself, an injury cognizable in court, and that cardholders would typically be reimbursed even if their cards had been misused. On the other hand, plaintiffs' lawyers have stretched to argue that products or services would not have been purchased or certain merchants would not have been patronized but for the implicit representation that their security systems met industry standards. Some statutes seem to provide for a remedy even in the absence of concrete harm if the elements of the statute are proven; the US Supreme Court has agreed to consider this issue in a case that will be argued in the fall of 2015.[60] The bottom line is this: The faster and more effectively a firm acts to prevent harm from a data breach, the stronger the argument that firm will have to dismiss future civil litigation at an early stage. Of course, acting quickly and effectively also will reduce the recoverable damages even if it doesn't stop the lawsuit in its tracks, and it also will also help the firm address its reputational and public relations concerns.

IV. Going Forward – What Does the Future Hold?

A significant cyber-attack has the potential to materially impair the operations or even, in a worst-case scenario, the survival of a private investment fund and its managers. Given this risk, and considering that various regulators have put cybersecurity at the top of their lists of examination and enforcement priorities, fund managers — regardless of the nature of their investment portfolios — must create, implement and enforce cybersecurity frameworks. Because cybersecurity is a complex process and because no two firms are the same, no single cybersecurity framework will be effective for all firms. Therefore, in implementing a specific cybersecurity framework, each manager must analyze its particular structure and operations, and should also consider the following:

- *An Effective Assessment of Internal and External Cybersecurity Threats Includes the Following Elements:*
  - ➢ allocating sufficient funding for cybersecurity protection and recognizing that the amount of funding necessary to do so sufficiently is likely to be sizeable;
  - ➢ developing a clear, detailed and comprehensive understanding of the firm's assets, business needs and capabilities in order to identify information that hackers and cyber-attackers might find valuable, and determine what needs to be protected;
  - ➢ conducting threat risk workshops to better understand the types of threats against which a firm needs to protect, and the business impact associated with a variety of different threat scenarios, which can help determine areas that require additional focus;
  - ➢ participating in information sharing networks to receive timely information on the most recent types of cybersecurity threats. This way firms can make themselves aware of new cyber-attacks to determine if they are relevant to the firm's business model; and
  - ➢ being aware that cyber-attacks often occur from within their organization by unhappy, ignorant or recently fired employees, and taking appropriate precautions.
- *Appropriate Policies and Procedures May Be Developed After:*
  - ➢ considering "Defense in Depth" when establishing their policies. Defense in Depth is a concept of using multiple layers of security protection at once. The idea is to provide redundancies in the event that one control fails or is inadequate on its own;[61]
  - ➢ preparing written information security policies to establish a "best practices" information security program tailored to the firm's specific business model, and that identifies which policies should be regularly reviewed, evaluated and updated as new threats are perceived and business models change;

---

[59] *See* e.g., *Green v. eBay Inc.*, No. 14-1688 (E.D. La. 2014)(eBay user information, including credit card numbers and bank account information); *Storm, et al. v. Paytime Inc. and Holt, et al. v. Paytime Inc.*, No. 1:14-cv-01138 (E. D. Pa. 2014)(social security and bank account numbers).; *Remijas v. The Neiman Marcus Group LLC*, No. 14-3122 (N.D. Ill. 2014)(appeal argued, 7th Cir. 2015); *In re Barnes & Noble Pin Pad*, 12-cv-08617 (N.D. Ill. 2013); *but see* In re Adobe Systems, Inc. Privacy Litigation, No. 13-CV-05226 (N.D. Cal.)(credit card information of 38 million users); *Resnick v. AvMed, Inc.*, 693 F. 3d 1317 (11th Cir. 2012)(monthly premiums paid by plaintiffs sufficient to confer standing because inclusive of data security costs).

[60] *Spokeo, Inc. v. Robins*, No. 13-1339 (U.S.)(whether Congress has the authority to pass legislation that provides a private right of action to redress as statutory violation in the absence of injury).

[61] *See* https://www.nsa.gov/ia/_files/support/defenseindepth.pdf.

- identifying a key senior- or executive-level employee to be responsible for cybersecurity and ensuring that he or she has sufficient authority and funding to make necessary improvements to the cybersecurity frameworks;
- conducting periodic gap analysis/risk assessments to determine where the firm has vulnerabilities;
- retaining cybersecurity consultants to periodically test the firm's vulnerabilities;
- drafting documented procedures for internal and external communications following a security breach, including with employees, clients, service providers, regulators and other stakeholders (e.g., media) that must or should be notified if a data breach occurs, including and within required timeframes;
- conducting regular staff training to educate personnel about the firm's cybersecurity practices and common types of cyber-attacks in case electronic safeguards fail to catch threats;
- establishing and adopting incident response planning so that there is no panic after a breach has occurred;
- implementing an automated process to systematically collect, review and evaluate all relevant information from every source (e.g., exchange requests, exceptions from automated or other surveillance, financial issues) and automatically generate exception reports that identify potentially problematic activity or access that may evidence a cyber-attack. Too often red flags are missed because of process issues, including failure to review incidents in a systematic manner; and
- maintaining control over all electronic devices (e.g., smartphones and laptops) outside the office and only using encrypted wireless connections.

- *Cybersecurity Evaluation of Third-Party Service Providers Includes the Following Elements:*
  - *Vendor Diligence*. Vendor selection, procurement, contracting and continued monitoring are all critical. In addition, it is imperative (i) that there are no policy and practice mismatches between a hired vendor and the management firm; and (ii) to accurately identify all vendors that have access to proprietary data as well as the data that those third parties can access. If a firm experiences a cyber-attack as a result of a third-party vendor's failure, the firm may be held liable, particularly if it cannot demonstrate that it used due care in selecting and retaining said vendor;
  - *Back-Up*. Investment management firms should frequently secure and back up data, and should ensure that third-party vendors make use of back-up systems to maintain electronic and hard copies of data;
  - *Restricted Access*. Vendors' access to systems and data should be restricted to only allow necessary access;
  - *Terms of Third-Party Vendor Agreements*. Agreements with third-party vendors should expressly address cybersecurity and include requirements with respect to (i) the maintenance of at least industry-minimum standard cybersecurity protections; (ii) the notification of the firm in case of breaches; (iii) responsibility for costs in case of a breach, including a requirement that the vendor maintain cyber liability insurance, where possible; (iv) the conditions and use of subcontractors; (v) certification by a third party that the vendor's cybersecurity policies and practices meet industry standards and/or audit rights; and (v) access to the third-party vendor's policies to ensure compliance; and
  - *Due Diligence*. Managers should perform due diligence/risk assessments with respect to a vendor's use of subcontractors, and firms should keep written records of their diligence.
- *To Enlist Staff and Client Buy-In Through Training and Education, Managers Should Ensure That Their Employees:*
  - regularly receive training on cyber-attacks and the firm's cybersecurity policies and procedures. Employees often innocently enable cyber-attacks by not recognizing and opening pernicious emails. Firms should ensure that their employees are trained to spot breaches, alert a previously identified reporting person in the event that they become aware of a breach and implement the firm's policies and procedures;
  - have a personal stake in the firm's cyber-attack preparedness; and
  - are monitored to ensure their compliance with the firm's cybersecurity policies and procedures, including rewarding those who follow the policies and disciplining those who don't.
- *To Limit the Damage: Reporting, Responding and Litigating If a Breach Occurs; Investment Management Firms Should Consider the Following:*

- *Notification*. Ensure that if a cyber-attack occurs, (i) if appropriate, law enforcement is promptly notified; (ii) all government entities and other persons required to be notified are notified within the required timeframes; (iii) clients and vendors are timely notified of any breach; and (iv) as appropriate, ensure media contacts are alerted in an effort to minimize adverse publicity;
- *Accord Breaches Appropriate Significance*. Make sure security breaches are taken seriously and that best efforts to limit damages are taken. While it may be difficult or impossible to stop a security breach right away, it is imperative that firms act as expediently as possible, document the steps they take to fix the breach, and keep forensic records to provide assistance in determining the source and scope of the breach and to strengthen the defense against litigation;
- *Ensure Client Access to Account Funds*. Take steps necessary to ensure clients are able to access their funds and securities when a cyber-attack occurs; and
- *Cyber Insurance*. Consider utilizing cyber insurance to help mitigate the economic consequences of a cybersecurity breach. Cyber insurance is a relatively new type of insurance, and the scope of coverage can vary widely by policy and carrier. Firms should consider policies that will reimburse them for the costs of an investigation to determine whose data was breached, litigation costs arising from the breach, costs arising from extortion as a result of stolen data and costs associated with public relations.

V. Conclusion

It is not a question of if an investment management firm will experience a cyber-attack, but rather a question of when and how. It is imperative that investment managers plan for these attacks, so that when a breach occurs, the manager can minimize damage and demonstrate to relevant regulators that they have acted with due care. It is important to understand that having a sufficient cybersecurity framework in place is a process and not a result, and as technology continues to evolve, the cybersecurity framework of each firm needs to evolve accordingly.