THE EVOLVING LANDSCAPE OF DATA PRIVACY AND CYBER SECURITY IN THE FINANCIAL SERVICES INDUSTRY

Craig Nazarro[*]
Matt White[**]
Eric Setterlund[***]

INTRODUCTION

The regulation of data privacy and cyber security in the financial services sector is in its infancy. This is partly due to the fact that the regulation of financial services is fragmented with multiple regulators covering varying risks, across different entities, serving a variety customers. These regulators include the Federal Reserve Board of Governors (the "Federal Reserve" or "The Fed"), Federal Deposit Insurance Corporation ("FDIC"), Office of the Comptroller of the Currency ("OCC"), Securities and Exchange Commission ("SEC"), Financial Industry Regulatory Authority ("FINRA"), Consumer Financial Protection Bureau ("CFPB"), and the Financial Crimes Enforcement Network ("FinCEN"), among others, as well as additional state agencies covering traditional commercial banking, consumer lending, investment banking, and broker dealer activity. This article will review the standards that are currently being utilized by both the prudential regulators, the CFPB, as well as the New York Department of Financial Services, and the best practices that those in the commercial banking and consumer lending spaces should implement including review of the FFIEC's Cyber Security tool. This article will also address the same expectations in the regulation of the securities and investment space, with a discussion of examination trends and an overview of recent enforcement actions. Finally, following this article's discussion of compliance on the front end, it will conclude with best practices to implement

---

[*] Of Counsel, Baker, Donelson, Craig Nazzaro advises lenders and servicers on all regulatory and compliance issues that impact the consumer lending industry, and defends them against charges of liability and any regulatory violations.

[**] Attorney, Baker, Donelson, Bearman, Caldwell & Berkowitz, P.C.; J.D., The University of Florida Levin College of Law; B.A. English, The University of Florida. The author would like to thank his wife Sarah for standing beside him throughout his career and for all of the love and support that made that career possible.

[***] Attorney, Baker, Donelson, Bearman, Caldwell & Berkowitz, P.C.; J.D., The University of Memphis Cecil C. Humphreys School of Law; B.A. Medieval Studies, The University of Tennessee. The author would like to thank his wife and daughter for their unending support.

in the event of a breach, and how implementing best practices prior to a breach will help in limiting regulatory, reputational, and litigation liability following a breach.

I. REGULATION PRIORITIES OF THE FFIEC

Within commercial banking data privacy and cybersecurity pose a risk to both an institution's consumers as well as the institution's safety and soundness. Given this fact, the CFPB, FDIC, The Fed and the OCC all have interests in promoting metrics, controls and standards to enhance the protection of information.

The Comptroller at the OCC has repeatedly highlighted the risk of cyber threats to financial institutions, going as far to call cyber threats the foremost risk facing banks today[1] while the FDIC has said Information Security is critical to their ability to carry out its mission of maintaining stability and public confidence in the nation's financial system.[2]

The FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB), and to make recommendations to promote uniformity in the supervision of financial institutions.[3] To this end they publish various resources to focus on. The FFIEC Information Security booklet is one of these resources. The booklet is part of many that comprise the FFIEC's "IT handbook". There are eleven (11) such booklets—booklets covering a variety of issues including: Audit functions, Business Continuity planning, Development and Acquisition, E-banking, Outsourcing technologies as well as other topics. However, the Information Security booklet speaks directly to the process by which a financial institution protects sensitive information.

Special focus should be paid to the updated Appendix A which was published as guidance for a regulator's field examiners to assess the level of

---

[1] Thomas J. Curry, Comptroller of the Currency, Remarks before the New England Council, Boston Massachusetts (Jul. 24, 2015) (transcript available from the Office of the Comptroller of the Curency).

[2] FDIC, FDIC CYBERSECURITY, https://www.fdic.gov/about/governance/cybersecurity.html (last updated February 22, 2017).

[3] FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, https://www.ffiec.gov/, (last modified Aug. 3, 2016).

security risks to an institution's information systems and the adequacy of its information security program's integration into overall risk management. The following 11 objectives are listed for said examiners within the appendix, but objectives 2-10 can be used as internal guidance to assess an institution's program:[4]

(1) Determine the appropriate scope and objectives for the examination.
(2) Determine whether management promotes effective governance of the information security program through a strong information security culture, defined information security responsibilities and accountability, and adequate resources to support the program.
(3) Determine whether management of the information security program is appropriate and supports the institution's ITRM process, integrates with lines of business and support functions, and integrates third-party service provider activities with the information security program.
(4) As part of the information security program, determine whether management has established risk identification processes.
(5) Determine whether management measures the risk to guide its recommendations for and use of mitigating controls.
(6) Determine whether management effectively implements controls to mitigate identified risk.
(7) Determine whether management has effective risk monitoring and reporting processes.
(8) Determine whether management has security operations that encompass necessary security-related functions, are guided by defined processes, are integrated with lines of business and activities outsourced to third-party service providers, and have adequate resources (e.g., staff and technology).
(9) Determine whether management has an effective information security program.
(10) Determine whether assurance activities provide sufficient confidence that the security program is operating as expected and reaching intended goals.
(11) Discuss corrective action and communicate findings.

In an effort to help institutions' management identify their risks and determine their preparedness, in 2015 the FFIEC released what is known as the

[4] FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, FFIEC INFORMATION TECHNOLOGY EXAMINATION HANDBOOK, INFORMATION SECURITY, 1 57–74 (2016).

'Cyber Security Basement Tool' which is comprised of a set of definable metrics that can provide a baseline as to where an institution sits. The assessment tool was designed to provide a measurable and repeatable process to assess an institution's level of cybersecurity risk and preparedness.[5] It consist of two parts:

(1) Inherent Risk Profile
(2) Cybersecurity Maturity

To define an Inherent Risk Profile, an institution must incorporate the type, volume and complexity of their operations and threats directed at the institution without including any mitigating controls. From this, an institution is able to assign one of five risk levels (Least, Minimal, moderate, Significant, Most) to five different categories:[6]

- Technologies and connection types
- Delivery channels
- Online/mobile products and technology services
- Organizational characteristics
- External threats

After determining the Inherent Risk Profile, the institution transitions to the Cybersecurity Maturity part of the Assessment to determine the institution's maturity level within each of the following five domains[7]:

- Domain 1: Cyber Risk Management and Oversight
- Domain 2: Threat Intelligence and Collaboration
- Domain 3: Cybersecurity Controls
- Domain 4: External Dependency Management
- Domain 5: Cyber Incident Management and Resilience

There are narratives which describe the controls within each of these domains that would place an organization in one of five statuses (Baseline, Evolving, Intermediate, Advanced or Innovative). Once completed, one can review an institution's Inherent Risk Profile in relation to its Cybersecurity Maturity results for each domain to determine whether they are aligned. If they

---

[5] FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, CYBERSECURITY ASSESSMENT TOOL, USER'S GUIDE, 1, 1 (2015).

[6] *Id*.

[7] *Id*. at 5.

are not aligned, an institution can then decide what actions are needed either to affect the inherent risk profile or to achieve a desired state of maturity.

An institution is not currently required to utilize the Cyber Security tool and, if it does utilize it, it is not required to report the results. However as with any self-assessment, if an institution does utilize it, it must provide the results if asked by its primary regulator. The use of this tool cannot only limit regulatory liability by showcasing that an institution is doing all that it can to implement a sound approach to data privacy and cyber security, but it also may have the effects of limiting litigation liability in the event of breach, as the institution will be able to show that it was prudent in its data privacy and cybersecurity practices which can limit damages in a lot of cases.

II. THE CFPB EFFORTS TO REGULATE THROUGH ENFORCEMENT

The CFPB began their regulation of the data protection space with an enforcement action. In a press release announcing the action, the CFPB cited its authority under UDAAP to bring a claim against an entity called Dwolla, Inc., explaining, "rather than setting 'a new precedent for the payments industry' as asserted, Dwolla's data security practices in fact fell far short of its claims. Such deception about security and security practices is illegal."[8] Under the Dodd-Frank Wall Street Reform and Consumer Protection Act (DoddFrank Act), all covered persons or service providers are legally required to refrain from committing unfair, deceptive, or abusive acts or practices (collectively, UDAAPs) in violation of the Act.[9] An act or practice is deceptive when:

(1) The act or practice misleads or is likely to mislead the consumer;
(2) The consumer's interpretation is reasonable under the circumstances; and
(3) The misleading act or practice is material.[10]

One would think that it was the *statements* that were illegal, not the *practices*, but when you review the consent order it becomes readily apparent the CFPB was focused on Dwolla's policies and procedures—not their marketing material.

---

[8] Press Release, CONSUMER FIN. PROT. BUREAU, CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices (Mar. 2, 2016), https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/.

[9] Consumer Fin. Prot. Bureau, CFPB Bull. 2013–07, Prohibition of Unfair, Deceptive, or Abusive Acts or Practices in the Collection of Consumer Debts (2013).

[10] *Id*. at 3 (citing CFPB Exam Manual at UDAAP 5).

The consent order addresses the marketing violations by mentioning that Dwolla is enjoined from "misrepresenting, or assisting others in misrepresenting, expressly or by implication, the data-security practices implemented". The Bureau then quickly moves to a lengthy discussion on how Dwolla must change their data protection *procedures*. The order fined Dwolla only $100,000, but required the company to:

(1) Adopt and implement reasonable and appropriate data-security measures to protect consumers' personal information;
(2) Establish, implement and maintain a written, comprehensive data security plan that is reasonably designed to protect the confidentiality, integrity and availability of sensitive consumer information;
(3) Adopt and implement reasonable and appropriate data-security policies and procedures;
(4) Designate a qualified person to coordinate and be accountable for the data-security program;
(5) Conduct data-security risk assessments twice annually and evaluate and adjust the data security program as needed;
(6) Conduct regular, mandatory employee training;
(7) Develop, implement and update, as required, security patches to fix any security vulnerabilities identified in any web or mobile application; and
(8) Develop, implement and maintain an appropriate method of customer identity authentication.

This has been the CFPB's only attempt to regualte a covered entity on a data priavcy issue, infact prior to this enforcement action, most of the industry belived data privacy issues to be handled by the FTC or the prudential reguators and the fine levied was small in proportions to the enforcement actions the CFPB levies against the industry. One has to wonder what might happen if the Bureau tries this on a larger scale, attempting to levy a fine in the millions—will an institution challenge the CFPB's authority in the space? And is this order the CFPB's attempt to position itself as a primary authority on data protection and cybersecurity?

III. THE NEW YORK DEPARTMENT OF FINANCIAL SERVICES' CYBERSECURITY RULE

States have begun to regulate the data privacy and cybersecurity practices of the financial services industry as well. The New York Department of Financial Services (NYDFS) released the self-proclaimed "first in the nation"

rule entitled "Cybersecurity Requirements for Financial Services Companies" to require effective cybersecurity measures to protect consumers and ensure the safe and sound operation of Department-regulated entities. The proposed rule has since been revised and the final rule became effective on March 1, 2017.[11]

The final rule was narrowed in scope from the proposed rule, but still creates cause for concern in multiple areas. In part the rule covers:

(1) A very broad definition of "covered entity"—which includes "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law".[12]

(2) Unconventional definition of nonpublic information—it is very broad and states that the term, "shall mean all electronic information that is not Publicly Available Information" and is:

(A) Business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity;[13]

(B) Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records;[14]

(C) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to

[11] N.Y. Comp. Codes R. & Regs. tit. 23, § 500.00 (2017).
[12] N.Y. Comp. Codes R. & Regs. tit. 23, § 500.01(c) (2017).
[13] N.Y. Comp. Codes R. & Regs. tit. 23, § 500.01(g)(1) (2017).
[14] N.Y. Comp. Codes R. & Regs. tit. 23, § 500.01(g)(2) (2017).

any individual, or (iii) payment for the provision of health care to any individual.[15]

(3) Strict audit trail requirements.[16]

(4) A mandate for a Chief Information Security Officer (CISO)—which can include a "qualified individual" to serve as CISO for the entity and may either be a company employee or an external vendor.[17]

(5) Annual certifications[18]

IV. REGULATION IN THE SECURITIES AND INVESTMENT SECTOR

Financial industry regulators have identified cybersecurity as one of the most significant risks that brokerage and investment advisory firms face.[19] Accordingly, regulators in this sector will continue to focus on firms' supervision and risk management related to cybersecurity, technology management, and data quality and governance. As discussed below, these areas have been identified as key issues by both the SEC and FINRA.

A. The SEC's Focus on Cybersecurity

The SEC annually issues guidance concerning its regulatory priorities for the coming year. This year, the SEC Office of Compliance Inspections and Examinations ("OCIE") issued its Examination Priorities for 2017 on January 12, 2017.[20] Among its identified examination priorities is cybersecurity.[21] This is not surprising as the OCIE has included cybersecurity as a priority since 2014.

In regulating cybersecurity and data protection issues, the SEC has a variety of regulatory tools at its disposal. These tools include Reg SCI

---

[15] N.Y. Comp. Codes R. & Regs. tit. 23, § 500.01(g)(3) (2017).

[16] *See* N.Y. Comp. Codes R. & Regs. tit. 23, § 500.06 (2017).

[17] N.Y. Comp. Codes R. & Regs. tit. 23, § 500.04 (2017).

[18] *See* N.Y. Comp. Codes R. & Regs. tit. 23, § 500.17 (2017).

[19] *See, e.g.*, Press Release, Sec. and Exch. Comm'n, SEC Names Christopher Hetner as Senior Advisor to the Chair for Cybersecurity Policy (June 2, 2016) (quoting SEC Chair Mary Jo White stating "Cyber attacks are a constant threat to our markets[.] . . . With the cyber field steadily evolving and expanding, it is imperative we continue to enhance our coordinated approach to cybersecurity policy across the SEC and engage at the highest levels with market participants and governmental bodies concerning the latest developments in this area.").

[20] Off. of Compliance Inspections and Examinations, Sec. and Exch. Comm'n, Examination Priorities for 2017 (2017).

[21] *Id.* at 4 ("Cybersecurity. In 2017, we will continue our initiative to examine for cybersecurity compliance procedures and controls, including testing the implementation of those procedures and controls.").

(Systems, Compliance and Integrity);[22] Reg S-P (Safeguards for the Protection of Customer Records and Information);[23] Reg SDR (Security-Based Swap Data Repository);[24] Reg S-ID (Identity Theft Red Flags);[25] Exchange Act Rule 15c3-5 (Market Access);[26] and Investment Company Act Rule 38-1 and Investment Advisers Act Rule 206(4)-7 (Compliance Rules).[27] These regulations provide the SEC with wide latitude in requiring companies to enact adequate policies, procedures, and practices related to cybersecurity and data compliance.

As noted above, regulation of cybersecurity in the financial services sector generally is relatively new. The SEC's regulation of these issues is no exception. The SEC's principle regulatory efforts in this arena began in March 2014, when the SEC sponsored a Cybersecurity Roundtable.[28] Thereafter, in April 2014, the OCIE announced the implementation of its Cybersecurity Initiative.[29] The initiative would undertake to examine more than 50 registered broker-dealers and registered investment advisers on each entity's cybersecurity governance, identification and assessment of cybersecurity risks, protection of 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 experiences with certain cybersecurity threats.[30]

In February 2015, the OCIE announced the results of this initiative.[31] This announcement revealed that the OCIE examined 57 registered broker-dealers and 49 registered investment advisers to better understand how firms address

---

[22] 17 CFR Parts 240, 242, and 249.

[23] 17 C.F.R. § 248.30 (2017).

[24] 17 C.F.R. §§ 232, 240, 249 (2017).

[25] 17 C.F.R. 248 (2017).

[26] 17 C.F.R. § 240.15c3–5 (2017).

[27] 17 C.F.R. §§ 270.38a1, 275.206(4)–7 (2017).

[28] *See* Press Release, Mary Jo White, Chair, Opening Statement at SEC Roundtable on Cybersecurity (Mar. 26, 2014) (underscoring the importance of technology, including cybersecurity preparedness to the integrity of the market system and customer data protection.), http://www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541286468; *see also* Press Release, Luis A. Aguilar, Commissioner, The Commission's Role in Addressing the Growing Cyber-Threat, (Mar. 26, 2014) (emphasizing the importance for the SEC to gather information and consider what additional steps it should take to address cyber-threats.),: http://www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541287184.

[29] *See* Off. of Compliance Inspections and Examinations, Sec. and Exch. Comm'n, National Exam Program Risk Alert Vol. IV, Issue 2, OCIE Cybersecurity Initiative (2014).

[30] *Id.* at 2.

[31] Off. of Compliance Inspections and Examinations, Sec. and Exch. Comm'n, National Exam Program, Risk Alert Vol. IV, Issue 4, Cybersecurity Examination Sweep Summary (2015).

the legal, regulatory and compliance issues associated with cybersecurity.[32] In the examinations, the staff collected and analyzed information from the selected firms relating to their practices for: identifying risks related to cybersecurity; establishing cybersecurity governance, including policies, procedures, and oversight processes; protecting firm networks and information; identifying and addressing risks associated with remote access to client information and funds transfer requests; identifying and addressing risks associated with vendors and other third parties; and detecting unauthorized activity. In addition to reviewing documents, the staff held interviews with key personnel at each firm regarding its: business and operations; detection and impact of cyber-attacks; preparedness for cyber-attacks; training and policies relevant to cybersecurity; and protocol for reporting cyber breaches.[33] The OCIE survey found that 88 percent of broker-dealers and 74 percent of advisers have experienced cyber attacks, either directly or through a vendor.[34] Moreover, 54 percent of broker dealers and 43 percent of advisers reported receiving fraudulent emails seeking to transfer client funds, and several of these reported losses relating to the fraudulent emails.[35] The announcement also contained observations focusing on how firms identify cybersecurity risks; establish cybersecurity policies, procedures and oversight processes; protect their networks and information; and detect unauthorized activity.[36]

Following up on its February alert, the OCIE issued another risk alert on cybersecurity in September 2015.[37] This alert announced that the OCIE would be conducting a second round of cybersecurity exams, which would involve more testing to assess the implementation of firm procedures and controls and further assess cybersecurity preparedness in the securities industry, including firms' ability to protect broker-dealer customer and investment adviser client information.[38] The second round exams would focus on: (1) Governance and risk assessment; (2) Access rights and controls; (3) Data loss prevention; (4) Vendor management; (5) Training; and (6) Incident response.[39] The OCIE has continued to conduct examinations of broker-dealers and investment advisers

---

[32] *Id.* at 1.
[33] *Id.*
[34] *Id.* at 2.
[35] *Id.*
[36] *Id.* at 2–5.
[37] Off. of Compliance Inspections and Examinations, Sec. and Exch. Comm'n, National Exam Program, Risk Alert Vol. IV, Issue 4, OCIE's 2015 Cybersecurity Examination Initiative (2015).
[38] *Id.* at 2–3.
[39] *Id.*

in these areas since that time, and its 2017 Examination Priorities Letter indicates these examinations will continue throughout 2017.[40]

B. FINRA's Focus on Cybersecurity

Similar to the OCIE, FINRA annually issues guidance concerning its regulatory and examination priorities for the coming year. This year, FINRA issued its Regulatory and Examination Priorities Letter for 2017 on January 4, 2017.[41] Among its identified examination priorities is cybersecurity.[42] While the SEC has included cybersecurity as an annual priority since 2014, cybersecurity has been a regular theme in FINRA's annual Regulatory and Examination Priorities Letters since 2007.

Much of FINRA's regulatory authority over cybersecurity and data privacy-related matters is the same as that of the SEC. However, FINRA's regulatory actions to date demonstrate that it primarily reviews compliance with Regulation S-P,[43] which requires firms to adopt written policies and procedures to protect customer information against cyber attacks and other forms of unauthorized access; Regulation S-ID,[44] which outlines a firm's duties regarding the detection, prevention and mitigation of identity theft; and the Securities Exchange Act of 1934,[45] which requires firms to preserve electronically stored records in a non-rewriteable, non-erasable format.

FINRA's regulation over these issues began much like the SEC's, with surveys and reviews of firm practices related to cybersecurity and data privacy.

---

[40] *See supra* note 2.

[41] Fin. Industry Reg. Authority, 2017 Annual Regulatory and Examination Priorities Letter (2017).

[42] *Id.* at 6 ("Cybersecurity threats remain one of the most significant risks many firms face, and in 2017, FINRA will continue to assess firms' programs to mitigate those risks. FINRA recognizes there is no one-size-fits-all approach to cybersecurity, and we will tailor our assessment of cybersecurity programs to each firm based on a variety of factors, including its business model, size and risk profile. Among the areas FINRA may review are firms' methods for preventing data loss, including understanding their data (*e.g.*, its degree of sensitivity and the locations where it is stored), and its flow through the firm, and possibly to vendors. FINRA may assess controls firms use to monitor and protect this data, for example, through data loss prevention tools. In some instances, we will review how firms manage their vendor relationships, including the controls to manage those relationships. The controls should be informed by a number of factors, including a clear understanding of any customer or employee personally identifiable information or sensitive firm information to which vendors have access. We may also examine firms' controls to protect sensitive information from insider threats. The nature of the insider threat itself is rapidly changing as the workforce evolves to include more employees who are mobile, trusted external partnerships and vendors, internal and external contractors, as well as offshore resources.").

[43] 17 CFR §248.30.

[44] 17 CFR §§248.201–202.

[45] 17 CFR §240.17a-4(f).

In 2010 and 2011, FINRA conducted on-site reviews of firms of varying sizes and business models to assess how firms control critical information technology and cyber risks.[46] In June 2011, FINRA conducted a survey of 224 firms to better understand industry information technology and cybersecurity practices and issues that may impact investor protection or market integrity.[47] Then, in 2014, FINRA launched a targeted sweep to explore cybersecurity. FINRA expressed four primary objectives: (1) to better understand the types of threats that firms face; (2) to increase its understanding of firms' risk appetite, exposure and major areas of vulnerabilities in their information technology systems; (3) to better understand firms' approaches to managing these threats; and (4) to share observations and findings with firms.[48]

In February 2015, FINRA issued its report on cybersecurity practices, which detailed the results of its survey and sweep, and provides what FINRA believes to be principles and effective practices for firms to consider in developing cybersecurity programs.[49] The report focused on best practices and considerations regarding several key areas, including: cybersecurity governance and risk management; cybersecurity risk assessment; technical controls; incident response planning; vendor management; staff training; cyber intelligence and information sharing; and cyber insurance.[50] FINRA's report concluded that the top three threats in these areas identified in its 2011 survey and 2014 sweep were: hackers penetrating systems; insiders compromising firm or client data; and operational risks.[51] Accordingly, FINRA's report intended to present an approach to cybersecurity to combat these risks that was grounded in risk management principles.[52] FINRA noted, however, that while the principals and practices addressed in the report should be considered by all firms, there is no one-size-fits-all approach to cybersecurity.[53]

---

[46] *See* FINRA, Report on Cybersecurity Practices (2017).

[47] *Id.* at 1.

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] *Id*. at 4.

[52] *Id.* at 1.

[53] To further assist small firms in establishing cybersecurity programs designed to identify, assess and detect cybersecurity threats; protect assets from cyber intrusions; and plan for a response when a compromise occurs, FINRA launched its Small Firm Cybersecurity Checklist in 2015. *See* FINRA, Checlist for a Small Firm's Cybersecurity Program (2016).

C. Exemplar Regulatory Actions

In addition to other regulators discussed throughout this article, the SEC and FINRA have brought numerous actions against firms they believe have violated rules and regulations related to cybersecurity and data privacy. Discussed below are actions in several areas where FINRA and the SEC have been particularly focused.

1. Violations Resulting from a Cyber-Breach

One June 8, 2016, the SEC fined a firm $1 million for allegedly failing to protect customer information, some of which was likely hacked and offered for sale online.[54] The misappropriated data included personally identifiable information ("PII"), such as customers' full names, phone numbers, street addresses, account numbers, account balances and securities holdings.[55] The SEC alleged that the firm used web "portals" for employees to access customer information without effective authorization modules to restrict access solely to employees with legitimate business needs, and that it failed to audit or test the relevant authorization modules.[56] Factually, the SEC alleged that from 2011 to 2014, a then-employee impermissibly accessed and transferred data regarding approximately 730,000 accounts to his personal server, which was ultimately hacked by third parties.[57] Following the hack of the personal server, the SEC alleged that it was likely that portions of the confidential data were posted on the Internet along with offers to sell larger quantities.[58] As a result of this conduct, the firm was alleged to have violated Rule 30(a) of Reg. S-P, the "Safeguards Rule" which requires, among others, every broker-dealer and investment adviser registered with the Commission to adopt written policies and procedures reasonably designed to: (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. Announcing the settlement of the charges, the SEC's Director of its Enforcement Division stated that "[g]iven the dangers

---

[54] Morgan Stanley Smith Barney LLC, Exchange Act Release No. 78021, 2016 SEC LEXIS 2142 (ALJ June 8, 2016) (cease-and-desist order).

[55] *Id.* at 2.

[56] *Id.* at 2–3.

[57] *Id.* at 5.

[58] *Id.* at 2.

and impact of cyber breaches, data security is a critically important aspect of investor protection. We expect SEC registrants of all sizes to have policies and procedures that are reasonably designed to protect customer information[.]"[59] The former-employee separately agreed to an industry and penny stock bar with the right to apply for reentry after five years, and was criminally convicted for his actions and received 36 months of probation and a $600,000 restitution order as a result of his conduct.[60]

2. Failing to Establish Adequate Policies and Procedures

On September 22, 2015, the SEC settled with a firm for $75,000 for allegedly failing to establish adequate cybersecurity policies and procedures in advance of a breach that made PII of approximately 100,000 individuals, including thousands of the firm's clients, vulnerable to theft.[61] The firm's web server was alleged to have been attacked in July 2013 by an unknown hacker who gained access and copy rights to the data on its server, rendering the PII vulnerable to theft.[62] The SEC alleged that the firm failed to adopt written policies and procedures reasonably designed to safeguard customer information in violation of Rule 30(a) of Reg. S-P.[63] For example, the SEC alleged the firm failed to conduct periodic risk assessments, implement a firewall, encrypt PII stored on its server or maintain a response plan for cybersecurity incidents.[64] Notably, there were no allegations of financial harm to any customers as a result of the attack, and the SEC noted that the firm retained a cybersecurity firm to review the incident, provided notice of the breach, and offered free identity monitoring to every affected individual.[65] Nevertheless, the SEC's Co-Chief of its Enforcement Division's Asset Management Unit stated that "as we see an increasing barrage of cyber attacks on financial firms, it is important to enforce the safeguards rule even in cases like this when there is no apparent financial harm to clients . . . [therefore] [f]irms must adopt written policies to protect their clients' private information

[59] Press Release, SEC, SEC: Morgan Stanley Failed to Safeguard Customer Data (June 8, 2016), https://www.sec.gov/news/pressrelease/2016-112.html.

[60] *Id.*

[61] R.T. Jones Capital Equities Management, Inc., Investment Advisers Act Release No. 4204, 2015 Lexis 3909 (ALJ September 22, 2015) (cease-and-desist order).

[62] *Id.* at 2.

[63] *Id.*

[64] *Id.* at 3.

[65] *Id.*

and they need to anticipate potential cybersecurity events and have clear procedures in place rather than waiting to react once a breach occurs."[66]

Addressing similar concerns, on May 15, 2015 FINRA fined a firm $225,000 for allegedly failing to have written supervisory procedures that were reasonably designed to protect confidential customer and proprietary information in violation of Rule 30(a) of Reg. S-P, after an employee lost a laptop computer that contained unencrypted financial and personal information of customers.[67] Specifically, FINRA alleged that the personal and confidential information of 352,551 customers was placed at risk when an Information Technology employee of the firm inadvertently left an unencrypted laptop in a restroom and it was lost.[68] At the time the unencrypted laptop was lost, the firm's written supervisory procedures provided for the adoption of Information Security Policy and Standards containing policies relative to data management, access controls, confidentiality and integrity, infrastructure, acceptable use, threat and vulnerability management and education and awareness; however, the firm's Information Security Policy and Standards allegedly did not require encryption of laptop hard drives, and only belatedly required laptop encryption.[69] While there were no allegations that the data was ever stolen or used, FINRA found that the information was put "at risk" and the firm's written supervisory procedures were insufficient.[70]

3. Books & Records Violations (SEA Section 17(a), Rule 17a-3, FINRA Rule 4511)

On December 21, 2016, FINRA fined 12 firms a total of $14.4 million for alleged significant deficiencies relating to the preservation of broker-dealer and customer records in a format that prevents alteration.[71] FINRA alleged that for prolonged periods, the firms failed to maintain electronic records in "write once, read many" ("WORM") format, which prevents the alteration or

---

[66] Press Release, SEC, SEC Chargers Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach (September 22, 2015), https://www.sec.gov/news/pressrelease/2015-202.html.

[67] Sterne, Agee & Leach, Inc., FINRA Letter of Acceptance Waiver and Consent No. 2014041619501 (2015).

[68] *Id.* at 2–3.

[69] *Id.* at 2–3.

[70] *Id.*

[71] *See* Press release, FINRA, FINRA Fines 12 Firms a Total of $14.4 Million for Failing to Protect Records From Alteration (December 21, 2016), https://www.finra.org/newsroom/2016/finra-fines-12-firms-total-144-million-failing-protect-records-alteration.

destruction of records stored electronically.[72] FINRA alleged that each of the 12 firms had WORM deficiencies that affected millions, and in some cases, hundreds of millions, of records pivotal to the firms' brokerage businesses, spanning multiple systems and categories of records.[73] In announcing the settlements, FINRA's Executive Vice President and Chief of Enforcement stated "[t]hese disciplinary actions are a result of FINRA's focus on ensuring that firms maintain accurate, complete and adequately protected electronic records. Ensuring the integrity of these records is critical to the investor protection function because they are a primary means by which regulators examine for misconduct in the securities industry."[74]

In light of these actions, firms can expect a continued regulatory focus on these areas and should be prepared to regularly audit their policies and procedures in these areas to ensure compliance with the regulators' concerns.

V. DATA BREACH PREVENTION AND PREPARATION

In the current digital age, it is not a question of whether an organization will experience a significant security incident, *but when*. Indeed, the likelihood of a company experiencing a significant event is almost certain—whether it is a service outage or a breach of personal identifying information.[75] Although by

---

[72] *Id.*

[73] *Id.*

[74] *Id.*

[75] For the less initiated, "breach" is a term of art involving the unauthorized access, disclosure, or use of "personally identifiable information"—usually defined to mean first name and last name of a consumer plus information that if known to a malicious actor could result in identity theft. A breach is *a type* of a security incident, and all breaches are security incidents. Not all security incidents are breaches, however. The difference between the two is significant because a breach requires consumer notification unless it can be demonstrated that there is a low risk of harm to the consumer. *See, e.g.*, Alaska Stat. § 45.48.010 et seq.; Ariz. Rev. Stat. § 44-7501; Ark. Code § 4-110-101 et seq.; Cal. Civ. Code § 1798.29, 1798.80 et seq.; Colo. Rev. Stat. § 6-1-716; Conn. Gen. Stat. § 36a-701b; Del. Code Ann. tit. 6 § 12B-101et seq.; D.C. Code § 28-3851 et seq.; Fla. Stat. § 501.171; Ga. Code § 10-1-910 et seq.; H.R.S. § 487N-1 et seq.; Idaho Code § 28-51-104 et seq.; 815 Ill. Comp. Stat. 530/5,530/10, 530/12, 530/15,530/20, 530/25; Ind. Code § 4-1-11 et seq.; § 24-4.9-1 et seq.; Iowa Code § 715C.1-2; Kan. Stat. § 50-7a01 et seq.; KY Rev. Stat. §365.732; La. Rev. Stat. § 51:3071 et seq.; 10 Me. Rev. Stat. § 1346 et seq.; Md. Code Com. Law § 14-3501 et seq.; Mass. Gen. Laws 93H § 1et seq.; Mich. Comp. Laws § 445.63, 72 et seq.; Minn. Stat. § 325E.61; Miss. Code § 75-24-29; Mo. Rev. Stat. § 407.1500; Mont. Code § 30-14-1701 et seq.; Neb. Rev. Stat. § 87-801et seq.; Nev. Rev. Stat. § 603A.010 et seq.; N.H. Rev. Stat. § 359-C:19 et seq.; N.J. Stat. § 56:8-163; N.Y. Gen. Bus. Law § 899-aa; N.C. GEN. STAT. §§ 75-61, 75-65; N.D. Cent. Code § 51-30-01et seq.; Ohio Rev. Code § 1349.19; 24 Okla. Stat. § 161 et seq.; Or. Rev. Stat. §§ 646A.600,646A.602, 646A.604,646A.624, 646A.626; 73 Pa. Stat. § 2301 et seq.; 10 L.P.R.A. St § 4051 et seq.; R.I. Gen. Laws § 11- 49.2-1et seq.; will be repealed effective June 26, 2016 and replaced by § 11- 49.3-1, et seq.; S.C. Code § 39-1-90; Tenn. Code § 47-18-2107; Tex. Bus. & Com. Code §§ 521.002, 521.053; Utah Code §§ 13-44-101, 13-44-202, 13-44-301; 9 V.S.A. §§ 2430, 2435; Va. Code

no means all-inclusive, the following are some tips to prevent and prepare for data breaches.

A. Appropriately Identify Assets

"[W]ithout a thorough understanding of the IT infrastructure . . . any future attempts to increase security may be, at best, ineffective or, at worst, detrimental to the basic business functions of the organization."[76] Thus, a company must identify what types of data it possesses, which employees have access to the data, and how employees access the data. Identifying the type of data is a critical step because certain types of data are subject to various regulations—possibly more than one—and those regulations usually require specific safeguards. It is also important to know who has access to data because a necessary requirement under most regimes is limiting access to data on a need-to-know basis, which in turn limits exposure.[77]

B. Implement an Ongoing Risk Assessment Process

An organization is not capable of warding off every single threat—especially those that are unknown. And regulators understand this. What regulators require, however, is an ongoing process that works to identify, assess, and control risk. The greatest penalties are, and will be, levied against those companies that fail to assess and control risk.[78] Accordingly, an ongoing risk assessment process is necessary.

1. The Risk Assessment Process

The assessment process gives a business the ability to identify and assess the risk to its assets, which, in turn, allows a business to focus its attention and

§ 18.2-186.6 § 32.1-127.1:05; Wash. Rev. Code § 19.255.010 et seq.; W. VA. Code § 46A-2A-101et seq.; Wis. Stat. § 134.98; Wyo. Stat. § 40-12-501 et seq.; *see also* 45 CFR §§ 164.400–414; 70 Fed. Reg. 15736–15754 (March 29, 2005).

[76] Peter P. Swire & Kenesa Ahmad, FOUNDATIONS OF INFORMATION AND DATA PROTECTION 79 (2012).

[77] For example, the "minimum necessary" standard in HIPAA requires covered entities to take reasonable steps to limit the use or disclosure of protected health information. 45 CFR §§164.502(b), 164.514(d).

[78] Press Release, Fed. Trade Comm'n, Student Lender Settles FTC Charges That It Failed to Safeguard Sensitive Consumer Information and Misrepresented Its Security Practices (March 4, 2008), https://www.ftc.gov/news-events/press-releases/2008/03/student-lender-settles-ftc-charges-it-failed-safeguard-sensitive; U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, Resolutions Agreements and Civil Money Penalties, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ (last visited April 6, 2017) (various settlements for failure to assess or implement safeguards).

resources on threats representing the *greatest total risk*. There are multiple risk assessment methodologies, but this process generally involves the following:

- Identifying all reasonably foreseeable internal and external threats to the information assets;
- Assessing the likelihood that the threat will materialize;
- Evaluating the potential damage that will result if the threat materializes; and
- Assessing the sufficiency of the policies, procedures, and safeguards in place to guard against the threat.[79]

Many consultants are available to assist with this process and should be considered.

2. Take Action Based on the Assessment and Implement Safeguards

After a company has identified its greatest total risk, it must then take action to mitigate that risk. This is done by implementing reasonable physical, technical, and administrative safeguards. An example of a physical safeguard is a lock on a door or filing cabinet, or security cameras. Technical safeguards refer to the technological measures to protect your information, such as encryption, two-factor authentication, passwords, and firewalls. And last but not least, there are administrative safeguards, which are the management measures that companies should put in place to ensure that employees are properly handling data. These safeguards include policies and procedures, training and enforcement protocols, and segregation of duties.

It is important to emphasize that every company should have documented policies in procedures in place. Such policies and procedures create expectations regarding the use of data, and all employees should be routinely trained regarding the company's specific policies and procedures to ensure a thorough understanding of those expectations. Often companies might have active procedures in place, but they are not well-documented. This is a problem because the procedures will likely not be consistently understood or followed.

Once employees have been trained in a company's policies and procedures, the company must then implement measures to ensure that employees are

[79] Jill D. Rhodes & Vincent I. Polley, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 51 (2013).

complying with the policies. This includes a sanction policy for employees who violate established protocol.

Periodic security reminders should also be sent to employees regarding their security obligations or known threats, such as phishing emails targeting employees. Sending periodic reminders, through email, greatly increases employee awareness of their security responsibilities and results in employees being more cautious. These measures also increase the chance that employees will report suspicious behavior and perhaps avoid some malicious attacks, like phishing.

C. Destroy What You Don't Need

Another way to mitigate your company's risk is to destroy data that is no longer needed for business purposes. This requires the implementation of an effective information governance program, which identities and deletes data that is no longer necessary. Such a program is critical for companies that quickly accumulate massive amounts of personally identifiable information.[80] The accumulation of unnecessary sensitive data only increases a company's exposure should a breach occur.

Information governance programs vary—they can be manual, automated, or both. Manual governance programs are not practical for companies with large amounts of data, however. Manual programs require that every employee be (1) assigned tailored responsibilities and (2) trained in their specific responsibilities. Additionally, this is an ongoing process, meaning that employees will be constantly doing this. Simply put, it is just too time consuming. Automated governance programs involve applications that analyze data and take action based on a company's policies. Automatic deletion of read emails past a certain date is a common automated process. Advanced automated solutions now also employ artificial intelligence to analyze content and make retention decisions. Ultimately, a governance program must be tailored to fit—there is no one-size-fits-all solution.

[80] As a practical matter, the more data that is accumulated and not deleted, the less likely it is that the data will be viewed, analyzed, used, or understood, which means the data will have very little value for your company.

D. Develop an Incident Response Program—And Routinely Test It.

It is crucial that companies develop and test their incident response plans. Adequate response plans include, but are not limited to, the following characteristics:

- **Approval from the C-Suite—**Approval and sponsorship from upper management is critical for success.
- **Appointment of Proper Personnel & Assignment of Responsibilities**—In addition to the company's privacy and security officer(s), the right employees need to be chosen to make up the response team and they need to have clearly designated roles. This allows the team to quickly assemble—each with a clearly assigned role—to respond to the incident.
- **Establish Clear Internal and External Lines of Communication, including Escalation**—Team members need to know who to contact both inside and outside the company. For internal communications, an appropriate chain of command needs to be established as not every incident rises to the level of requiring an "all-hands-on-deck" approach. Indeed, some trivial matters will simply need to only be documents. For external communications, companies should include in the policy the contact information for their insurance providers, outside forensics investigators, PR firms, and law enforcement personnel, if necessary.
- **Set Methodology and Approach**—The appropriate methodology for investigating and responding to an incident needs to be set. This includes assessing what state and federal laws are at play, especially for determining whether an incident rises to the level of a reportable "breach."[81]
- **Checklists—**To ensure consistent treatment of incidents, it is preferable to develop checklists for investigation and remediation. This will create a road map for your company to both respond to an incident, as well as remediate an incident.

Finally, it is important for an institution to routinely test its incident response plan. This should be done through routine tabletop exercises, which involve an institution's team responding to scripted, announced—or unannounced—"incidents." For example, a team may be told that ransomware has attacked their information system. The team will have to work through and appropriately respond to the incident as if it is actually happening. Tabletop exercises can be a valuable tool to assess a team's readiness, as well as identify

[81] *See supra* note 1.

gaps in an instituion's plan and increase awareness throughout the organization.

E. Consider Cyber Insurance

Finally, to defray the costs associated with significant incidents and breaches, companies should consider purchasing cyber insurance. Cyber insurance covers common first-party claims (*e.g.*, incident response/crisis management and identity theft response, cyber extortion, data asset recovery and restoration, and business interruption caused by cyber security events.) and third-party claims (*e.g.*, claims from third-parties arising from a breach in network security or transmission malware or claims related to a company's failure to properly handle or protect personal information). However, the exclusions in the policy can greatly affect the handling of a claim. Companies will also need to carefully consider limitations of liability and applicable retentions to ensure that they are appropriately covered should an incident occur.