# Table of Contents

Overview .................................................. 1–4

Cybersecurity Project Report ........................................ 5–20

Addendum 1 – Sample Firm Cybersecurity Policy .................. 21–26

Addendum 2 – Data Classification ................................. 27–31

Addendum 3 – Selected Regulatory Enforcement Actions .......... 32–33

Addendum 4 – Cybersecurity and Resiliency Observations from SEC.. 34–45
Overview

The Financial Services Institute (FSI) is the only organization advocating solely on behalf of independent financial advisors and independent financial services firms. Since 2004, through advocacy, education, and public awareness, FSI has been working to create a healthier regulatory environment for 30,000 independent financial advisors and nearly 90 independent financial services firms that represent upwards of 160,000 affiliated financial advisors. FSI has been working to improve conditions for these members so they can provide affordable, objective financial advice to Main Street Americans.

FSI appreciates the hard work, significant efforts, and substantial time committed to drafting this white paper by the members of the FSI Cybersecurity Task Force (Task Force). The Task Force includes:

- Mark Quinn, Co-Chair, Cetera Financial Group
- Mike Pedlow, Co-Chair, Kestra Financial, Inc.
- Sam Attias, OS33
- David Boron, Triad Advisors, LLC
- Allen Eickelberg, Spire Investment Partners, LLC
- Morley Ivers, OS33
- Sam Johnson, Sagepoint Financial, Inc.
- Jason Lish, Advisor Group, Inc.
- Kevin Miller, Securities America, Inc.
- Summer Pretzer, Cetera Advisor Networks, LLC
- John Reinhardt, Atria Wealth Solutions
- Frank Smith, First Command Financial Planning, Inc.

FSI formed this Task Force to provide a resource for independent financial services firms to help them understand the cybersecurity requirements and expectations unique to this segment of the industry. The Task Force is comprised of experienced attorneys, compliance officers, and broker-dealer executives charged with developing a guide specific to the concerns of the independent broker-dealer (IBD) space.

This document provides a summary of the law and regulations related to cybersecurity, regulatory guidance and expectations along with information gained from enforcement actions in connection with cybersecurity incidents, and discussion of techniques that firms may wish to use in order to mitigate potential risks.
Scope of the Law

- **Federal Law and SEC Rules** Cybersecurity encompasses laws and regulations covering both data privacy and data security. Most providers of financial services are subject to the Gramm-Leach-Bliley Act of 2001, which requires firms to protect the privacy of customer information, disclose to customers how they use that information, and under what circumstances they share that information with third parties. In response, the SEC promulgated rules covering customer privacy and data security, including Regulation S-P and Regulation S-ID.

- **State Regulations** Many states have adopted laws or regulations governing data protection and privacy. The largest of note are New York and California.
  - In 2017, New York adopted legislation requiring financial services firms to implement a cybersecurity program designating a Chief Information Security Officer, adopting certain policies and procedures for the collection, use, and dissemination of customer information, training for employees and agents, and incident reporting. This law is overseen and enforced by the New York Department of Financial Services.
  - In 2018, California adopted the California Consumer Privacy Act, which created strict guidelines for the collection, use and sale of customer information. This law contains a general exemption for entities that are subject to the provisions of Gramm-Leach-Bliley.

- **Foreign Jurisdictions** The European Union adopted the General Data Protection Regulation in 2018, which contains extensive requirements regarding the collection, use and protection of customer information. If your firm does business anywhere in the EU, we recommend that you consult with counsel about how the GDPR might apply to your operations.

Guidance

- **SEC Guidance** to date has been fairly general, but has included the following:
  - **Cybersecurity Disclosure Standards**—Independent financial services firms must make accurate and timely disclosures of material events. Firms must make clear and expedient disclosures and are responsible for ensuring that they have appropriate disclosure tools in place.
  - **Cybersecurity and Resiliency Observations (included in addendums)**
  - **Oversight of Cyber Risks** Including outside actors such as cybercriminals, and inside actors who could be either malicious or negligent. Breached firms must disclose the extent of their risk oversight and its effect on their leadership structure.
  - **Chief Information Security Officers** should ensure that when reporting on cyber risks that their communications are:
    - Appropriate and relevant to their audience
    - Grounded in a business mindset
    - Based on complete and accurate data
    - Transparent about incomplete or unverified data
• FINRA’s Report on Selected Cybersecurity Practices (2018) provided prescriptive guidance to help firms understand and meet FINRA’s requirements in this area. The report outlined five areas of focus to help broker-dealers protect sensitive customer and firm data:
  ◦ Branch Controls, generally consisting of two parts:
    ■ Asset Inventory
    ■ Technical Controls
  ◦ “Phishing” or social engineering attacks
  ◦ Insider Threats
  ◦ Penetration Testing
  ◦ Mobile Devices

• The FINRA “Top 10 List” for Branch Offices identifies several specific items related to data protection that member firms must have to demonstrate that they have adequate safeguards in place to protect their data, including
  ◦ “Least Privileged” Access
  ◦ Vulnerability Scanning and Patch Management
  ◦ Data Loss Prevention
  ◦ Identity Management – Verification and Multi Factor Authentication
  ◦ Data Encryption
  ◦ Penetration Testing
  ◦ Incident Response
  ◦ Awareness and Training
  ◦ End-Point Management
  ◦ Risk Assessment

**Mitigation Techniques**

In an attempt to mitigate the complex threats associated with a cybersecurity breach, broker-dealers should consider the following:

- The use of software tools such as anti-virus/anti-malware protection for all electronic devices used to access client information
- The use of cloud-based services for laptops/mobile devices so they can be wiped remotely if lost or stolen
- The use of a written cybersecurity checklist and inventory of all devices used and to whom they are assigned
- Evaluate whether policies and procedures for the use of customer relationship management (CRM) programs are appropriate to the broker-dealer’s business model. Firms may wish to limit what information can be stored in these systems.
• Obtaining insurance coverage sufficient to address any financial damage firms may incur in connection with cybersecurity incidents or other breaches. Coverage should include:
  ◦ Reimbursement for damages suffered by clients or third parties as a result of unauthorized use of client data
  ◦ Reimbursement to the firm for costs incurred in recovering data lost to hackers or other unauthorized users, or replacement of equipment damaged as a result of intrusions
  ◦ Coverage for fines and penalties assessed by regulatory agencies for violations of applicable laws or rules (though there are often limits on the ability to obtain insurance for those costs).
  ◦ It is worth noting that insurance coverage may be compromised or nullified if the firm or individuals associated with it do not follow applicable procedures
INTRODUCTION

Modern businesses depend on electronic data to manage virtually all of their operations. This includes information about the firm itself, customers, suppliers, employees and other stakeholders, much of which is sensitive and must be protected. This is particularly true for providers of financial services such as banks, broker-dealers and investment advisers. Customers, regulatory agencies, and the public expect firms to take all reasonable steps to protect information relating to them and respond promptly and effectively in the event of breaches or other incidents. While the use of electronic data has greatly enhanced the ability of financial services providers to manage their business and provide value to their customers, it has created risks that did not previously exist. The value of electronic information has also created incentives for criminals or other bad actors to steal data for improper use or to disable systems that are critical to the functioning of a business.

FSI member firms and individual advisers have multiple interests to consider when managing data:

• The possibility of regulatory scrutiny;

• Financial exposure that can result if systems are compromised or customer information is misappropriate; and

• Risk to their reputations in the event of breaches or unauthorized use of customer data.

In this report, we will provide an overview of the law and regulations relating to cybersecurity applicable to broker-dealers and Registered Investment Advisers (RIAs). We will offer summaries of regulatory guidance and expectations, as well as perspective gained from enforcement actions taken by various regulators in connection with cybersecurity incidents. We will focus primarily on issues that are of specific interest to independent broker-dealers (IBDs), particularly with respect to adviser use of equipment or systems that are not owned or completely controlled by the firm. We will also discuss techniques that firms may wish to use in order to mitigate the risks that cybersecurity and data protection regulations may create.

SCOPE OF THIS REPORT—WHAT IS CYBERSECURITY?

The term “cybersecurity”, as applied to the securities industry, consists of two different but related topics: Data protection and data privacy. This report will cover both. The law relating to data privacy for financial services providers in the U.S. has been in existence for nearly 20 years and is fairly well-developed. Regulations relating to data protection are newer, not generally as comprehensive, and evolve rapidly at both the state and federal levels. We strongly encourage all broker-dealers and RIAs to be aware of this evolution and develop processes to monitor new or proposed legislation and regulatory guidance.

Standards relating to cybersecurity have been adopted by multiple government and quasi-government agencies worldwide. In this report, we will focus on standards applicable to broker-dealers, RIAs, and their associated persons who operate in the United States. We will offer limited comments on standards applicable to other types of entities, particularly corporate affiliates of broker-dealers and RIAs. We will also touch briefly on standards for firms operating in the European Union (EU). We recommend that if your firm has operations in the EU or other geographic regions outside the United States, you seek additional guidance from local counsel or experts regarding laws and regulations in those jurisdictions.
Many regulations applicable to broker-dealers and RIAs are “principles-based”. They set forth a set of general standards or considerations and leave design and implementation of processes, policies, and procedures to the firm, based on the nature and scope of its business. A global full-service investment bank with 25,000 employees is a fundamentally different enterprise than a domestic RIA with 10 employees and 200 clients. Section 15 of the Securities Exchange Act generally requires that supervisory processes for broker-dealers be “reasonable” in light of all of the circumstances. We will attempt to highlight areas in which the applicable regulations are prescriptive and mandate specific standards, as compared to those that allow firms more latitude in assessing their circumstances and what actions they wish to take with respect to cybersecurity.

ENTITIES SUBJECT TO REGULATION

Broker-Dealers

Broker-dealers are regulated by the SEC, FINRA, and most of the 50 states. As discussed in more detail below, each agency has different legal authority, standards, and expectations with respect to protection of data and limitations on the use of information relating to customers. The degree of sophistication of hackers and other bad actors has increased dramatically, and the level of concern from the public, legislators, and regulatory agencies is rising. One prominent study estimates that the number of data breaches experienced by large American companies has increased from 200 to approximately 1,400 incidents per year in the period from 2007 through 2018.

A commonly expressed view is that every business will eventually be subject to a cyber-attack of some kind. In light of that, firms must take steps to secure their systems and processes and be prepared to respond in the event of an incident. They should be able to demonstrate not only that they have complied with current legal requirements, but that they have taken reasonable steps to anticipate and mitigate threats to the security of their own data and that of their customers. The SEC and FINRA have each published guidance regarding their expectations with respect to broker-dealers, discussed in more detail below. In addition to the SEC and FINRA, many individual states have their own requirements with respect to data protection and privacy.

Registered Investment Advisers

RIAs are regulated by the SEC and most states. For the most part, SEC and state standards applicable to broker-dealers and RIAs are similar, but since RIAs are deemed to be fiduciaries with respect to services provided to customers, their duty of care in the absence of a specific standard may be higher than that applicable to broker-dealers.
The North American Securities Administrators Association (NASAA) has published a model rule covering privacy and information security applicable to state-registered RIAs.¹ The model rule has not been finalized or adopted by any state as of now, but can likely be viewed as indicative of the standards that many states will ultimately adopt.

**Parent Companies and Other Corporate Affiliates**

Many broker-dealers and RIAs are under common corporate ownership, either in conjunction with a business strategy or as part of a corporate group that includes entities such as insurance companies, banks, or other providers of financial services. Depending on the type of enterprise, each of these entities are subject to regulation by different government agencies, and not all of the standards applicable to them will apply to broker-dealers or RIAs. In many large, vertically-integrated financial services companies, information technology services and data protection are managed as a shared service by a single team or vendor on behalf of multiple subsidiaries. Broker-dealers and RIAs must meet the standards imposed on them by the SEC, FINRA, and the states, regardless of who actually provides services to them or their clients. If your firm is part of an affiliated corporate group or if you outsource any aspect of your cybersecurity program to a third party, you should be aware of the rules that may apply to different types of entities and take steps to ensure that shared services provided by an affiliate or contractor meet the requirements applicable to your type of regulated entity. FINRA has published guidance regarding review, selection, and monitoring of vendors and service providers.² Much of it is general in nature and not focused on data security, but it may be useful for firms as they consider this issue.

**APPLICABLE LAW AND REGULATION – MANY JURISDICTIONS**

Cybersecurity consists of laws and regulations that cover both protection and privacy of customer information. Privacy includes requirements to protect both the security and confidentiality of non-public personal information (NPI) regarding customers.

**Federal Law and SEC Rules**

Most providers of financial services, including broker-dealers and RIAs, are subject to the provisions of the Gramm-Leach-Bliley Act of 2001³, (GLBA). Among other things, GLBA requires covered firms to take steps to protect the privacy of customer information (Personally Identifiable Information, or PII), disclose to customers how they use PII, and under what circumstances they share it with affiliates or third parties.

In response to GLBA, the SEC adopted a series of rules creating standards covering customer privacy and data security. These include SEC Regulation S-P⁴ and Regulation S-ID.⁵

---

² See, for example, FINRA Notice to Members 05-48.
⁴ 17 CFR Section 248, et. seq.
⁵ 17 CFR Section 248.201.
Regulation S-P contains several elements, including:

- A requirement to provide all customers with written notice of the firm’s policies regarding disclosure of NPI or PII to third parties. The notice must generally be delivered at least annually to all customers. It must contain a summary of the information that the firm collects, under what circumstances it will be disclosed to third parties, and the rights of the customer to prevent disclosure of such information, specifically including the right to “opt out” of having information shared with third parties.

While Reg. S-P only requires broker-dealers and RIAs to provide customers the ability to opt-out of information sharing, several states go further and require that any customer whose NPI will be shared with unaffiliated third parties take affirmative action to “opt in”. 6

Also, note that under the provisions of Reg. S-P, NPI is considered to be the property of the firm, as distinct from the individual adviser. Thus, unless the privacy policy of the firm specifically allows individual advisers who leave the firm to take customer NPI with them, the firm may violate Reg. S-P if it allows departing advisers access to that information after their affiliation with the firm ends. 7

- A requirement to describe the policies of the firm with respect to protecting the confidentiality and security of customer information.

- The “Safeguards Rule” 8, which requires broker-dealers and RIAs to adopt written policies and procedures with regard to protection of customer NPI. The Safeguards Rule also requires broker-dealers and RIAs to protect against unauthorized access to consumer credit reports and to properly dispose of them under certain circumstances.

Regulation S-ID requires all broker-dealers and RIAs to establish an Identity Theft Prevention program, which must be designed to detect, prevent, and mitigate against damages caused by customer identity theft. The program must identify “red flags” or suspicious activity with respect to covered accounts and respond to them appropriately. It also requires that the Identity Theft Prevention program be monitored and updated periodically to reflect the firm’s evaluation of changes in risks to customers. It must include provisions for training of employees and oversight of vendors and other third parties that provide services to the firm. The program must be reviewed and approved by the Board of Directors or a similar group at each firm.

The provisions of Regulation S-ID requiring approval by the Board of Directors and ongoing review are both interesting and slightly unusual. They are intended to emphasize the importance of these issues to the firm and customers, and give the SEC authority to hold directors or members of senior management personally responsible in the event of violations.

State Regulations

Many states have adopted laws or regulations governing protection of customer information and data privacy. In general, state standards include restrictions on what types of client information may be collected by financial services providers, how and with whom that information may be shared, standards for how information is to be protected, and provisions relating to notification to regulatory authorities and customers when breaches are discovered. The National Conference of State Legislatures maintains a website that contains information about state cybersecurity regulations 9 and required notifications after breaches are detected. 10

---

7 See, for example, In the Matter of Next Financial INVESTMENT ADVISERS ACT OF 1940 Release No. 5163 / March 11, 2019 ADMINISTRATIVE PROCEEDING File No. 3-19066.
8 17 CFR Section 248.30.
A survey of the laws of all 50 states is beyond the scope of this report, but states that have adopted laws covering cybersecurity since 2017 include California, New York, South Carolina, Rhode Island, Nevada, and Vermont. The California and New York laws are particularly worthy of note. Both states have large populations and are often viewed as trendsetters for other states in many areas of law and regulation, particularly for financial services firms. It is likely that other states will follow their lead to some extent.

In 2017, the state of New York adopted cybersecurity legislation relating to many financial services firms. It requires all such firms to implement a cybersecurity program that includes designation of a Chief Information Security Officer (CISO), adoption of policies and procedures for collection, use, and dissemination of customer information, training for employees and agents, and reporting of incidents such as breaches.

The New York Department of Financial Services (DFS) has established a division that will oversee compliance with New York laws and presumably take enforcement action if violations of the law occur. The Superintendent of the DFS has recently stated that cybersecurity will be an area of emphasis for her staff and it is reasonable to expect further action in this area.

In 2018, the State of California adopted the California Consumer Privacy Act (CCPA), which becomes effective on January 1, 2020. It enhances privacy rights for California residents, and creates strict guidelines regarding the collection, use, and sale of customer information. The CCPA contains a general exemption for broker-dealers, RIAs, and other entities that are subject to the provisions of GLBA, but if your firm has customers who reside in California, you should review the provisions of the CCPA to see if your firm is subject to additional requirements. This is particularly true if you have corporate affiliates that collect or use data regarding your customers in ways that differ from the policies of your firm. We would also note that a number of amendments to the CCPA have been proposed. Particularly if your firm has substantial operations or customer presence in California, we recommend careful monitoring of possible changes to the law.

**Jurisdictions Outside of the United States**

Many countries in addition to the U.S. have adopted laws or regulations covering protection of customer information and cybersecurity. Of particular note is the General Data Protection Regulation (GDPR), which was adopted by the European Union in 2018. The GDPR contains extensive requirements regarding collection, use, and protection of customer information, as well as notification to authorities in the event of certain types of incidents. In particular, it includes provisions requiring companies to “forget” or delete information about customers upon their request.

The GDPR was created primarily to cover the operations of companies such as Facebook, Amazon, and Google, whose business models include sale of data about customers. Most financial services providers do not engage in this practice, but the provisions of the GDPR are so broad that they may apply in circumstances that firms would not otherwise expect. If your firm does business anywhere in the EU, we recommend that you consult with counsel or other experts knowledgeable about how the GDPR might apply to your operations. Several U.S.-based providers of financial services viewed the provisions of the GDPR as so problematic that they announced their intention to cease serving clients who reside in the EU.

Each firm should review its operations with a view to collection, use, and protection of customer data. As we have seen, the stakes for firms that experience breaches involving exposure of customer data can be severe. They may include costs of remediation or ancillary costs incurred by customers, regulatory fines and penalties, costs of restoring data compromised by hackers, and damage to the reputation of the firm. The damages accruing to a firm will always depend on the facts and circumstances surrounding a breach, but we will suggest that the stakes are getting bigger, not smaller.

---

12 [http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=].
THE SEC APPROACH

“Today, the importance of data management and technology to business is analogous to the importance of electricity and other forms of power in the past century.”

— SEC Statement and Guidance on Public Company Cybersecurity Disclosures

In February 2018, the SEC released updated guidance on cybersecurity disclosure for public companies. While not all of it is specifically applicable to broker-dealers and RIAs, it is representative of the SEC’s view as to what steps all companies should take and the level of significance that the SEC attaches to it. In 2019, the SEC Office of Compliance Inspections and Examinations (OCIE) has issued guidance on multiple occasions regarding its priorities in this area. However, financial services firms should be aware that the SEC only established its Division of Enforcement Cyber Unit in September of 2017. Cybercriminals have been in the game for much longer.

SEC rules and guidelines to date have been fairly general. Disclosure standards and impact for broker-dealers and CISOs include several parts, including the following:

Cybersecurity Disclosure Standards

SEC Chairman Jay Clayton has shared his aim to ensure that all regulated entities provide more complete information to investors about cyber risks and incidents. The main focus of the SEC guidance is that broker-dealers and RIAs must review their controls and procedures to ensure that their cybersecurity disclosure responsibilities are properly discharged. Referring to the increasing frequency, magnitude and cost of cyber incidents, the SEC has stated that public companies and regulated entities should “take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack.”

The SEC has also made it clear that if investors are kept in the dark about security incidents, not only should companies expect class action suits, they can expect action from the SEC, including investigations and possible enforcement action. In the agency’s words, the SEC “continues to monitor cybersecurity disclosures carefully.” With that in mind, broker-dealers and RIAs should be certain that they understand the importance of cybersecurity and that there is value in communicating to clients exactly what is being done to help protect their data.

The SEC has noted that the responsibility for clear and expedient disclosure falls squarely on the broker-dealer. The firm is responsible for ensuring that they have appropriate disclosure controls and procedures “to make accurate and timely disclosures of material events.” This helps investors grasp the impact of a cyber incident on the organization and its business, finances, operations and, of course, potential liability.

The issue of disclosure is further complicated by the need to detect incidents, properly handle the firm’s response, manage any necessary repair or recovery, and ensure that all clients are properly notified. The SEC has also advised organizations to provide specific information that is meaningful to investors in incident reports.

Impact for Broker-Dealers: Oversight of Cyber Risks

SEC guidance notes that cybercriminals and “threat actors” have different motives, ranging from financial gain to social or political goals such as “hacktivism”. Security incidents can also result from the actions of malicious or negligent insiders. In addition, the consequences of cyberattacks can take many forms, from lost business to reputational damage, strained relationships with suppliers and clients, fines, lawsuits and more.

13 See, for example, SEC Release Nos. 33-10459 and 34-82746 and https://www.sec.gov/spotlight/cybersecurity.
The SEC has emphasized that a breached firm must “disclose the extent of its various roles in the risk oversight of the company, such as how the board administers its oversight function and the effect this has on the broker-dealer’s leadership structure.” Given this clear statement, it would be extremely difficult for broker-dealers and RIAs to defend their conduct by stating that they have not received sufficient guidance from the SEC about expectations in this area.

**Impact for Chief Information Security Officers: Collaboration and Communication**

Directors and senior managers of regulated entities are in the crosshairs of the SEC, as are CISOs. Data security leaders should be prepared to implement mechanisms to discern the impact and potential materiality of cyber risks. For some CISOs, this will require increased collaboration and cooperation with Chief Risk Officers (CROs) and other professionals to determine more accurate, timely and objective ways to evaluate and communicate cyber risks. CISOs should aim to make sure that their communications are clear and effective when managing and reporting on cyber risks and ensure that their communications are:

- Appropriate and relevant to their audience
- Grounded in a business mindset
- Based on complete and accurate data
- Transparent about incomplete or unverified data

The updated SEC guidance has raised the bar and provided clear warnings about the responsibilities of broker-dealers and RIAs regarding cybersecurity disclosure.

**FINRA’S APPROACH TO CYBERSECURITY FOR MEMBER FIRMS**

**Guidance for Broker-Dealers**

Beginning in approximately 2014, regulators in the securities industry began to focus on cybersecurity as a distinct type of risk for broker-dealers and RIAs and established a set of standards, guidelines, and best practices for regulated firms. The SEC’s Office of Compliance Inspections and Examinations (OCIE) released their first Cybersecurity Initiative in April 2014. FINRA has generally followed the OCIE’s guidance, and over time has created its own views on cybersecurity.

As a self-regulatory organization (SRO), FINRA is not a government agency and does not enact laws, but it does have the authority to adopt rules that apply to all FINRA member firms and to enforce laws or regulations of other agencies such as the SEC. FINRA is also subject to oversight from the SEC, and the two organizations often work closely together when it comes to guidance for broker-dealers. FINRA rules generally do not apply to RIAs, except in circumstances where a broker-dealer is dually-registered as an RIA. In those instances, firms should be cognizant of the fact that FINRA rules and guidance may apply to advisory activities.

The SEC and FINRA have both been criticized for what had previously been viewed as the vague nature of their guidance to regulated firms. FINRA has largely changed that perception with the release of its 2018 Cybersecurity Report. The guidance provided in that report is generally prescriptive, giving broker-dealers an effective “how to” guide to implementing and managing cybersecurity controls. It is likely the SEC and FINRA will expand on this recent initiative to provide even more prescriptive guidance going forward.

---


FINRA'S REPORT ON SELECTED CYBERSECURITY PRACTICES (2018)

There are two main components to a cybersecurity program for a broker-dealer. The first centers on policies, procedures, and firm-driven initiatives. The second is based on technology. We will focus primarily on how technology can help firms meet the cybersecurity guidance issued by FINRA and will highlight certain technical aspects of the guidance itself.

FINRA has stated that the primary purpose of its 2018 guidance is to help broker-dealers protect “sensitive customer and firm data”. The report is split into five areas of focus, explaining the guidance and proposing solutions for member firms. They include:

- Branch Controls
- “Phishing”
- Insider Threats
- Penetration Testing
- Mobile Devices

Branch Controls

This section provides a practical guide on how to create, enforce and manage cybersecurity policies and procedures across all groups in a broker-dealer. It also provides a framework for managing the activities of branch offices that are owned or controlled by advisers who are independent contractors or not otherwise employees of the firm. Branch Controls generally consist of two separate parts: Asset Inventory and Technical Controls.

- **Asset Inventory** mandates that broker-dealers maintain a comprehensive and current list of all Information Technology (IT) assets that store or access sensitive information. The purpose of the inventory is to serve as a starting point to identify assets that can be vulnerable to being compromised. It is also useful in managing the lifecycle of IT assets. Many broker-dealers have reported that they were asked to produce real-time reports on IT assets during recent FINRA examinations. FINRA has developed an examination protocol specifically designed to cover cybersecurity. It has been active in this area for the past several years, and has indicated an intention to increase emphasis in the future.¹⁶ There are currently several versions of software commercially available that can account for IT assets in real time, as well as the security status of devices.

- The **Technical Controls** section is highly prescriptive in its guidance. This has generally come as a welcome development for broker-dealers because of the specificity it offers. The focus of the section is largely devoted to non-employees of the broker-dealer, such as advisers who are independent contractors. The highlights of the section include:
  - Password requirements and Multi-Factor Authentication
  - Minimum third-party vendor controls and requirements
  - Identity and access management for advisers and support staff
  - Encryption standards
  - Wireless security settings
  - Device security – Anti-Virus, Anti-Malware, and Encryption
  - Controlling adviser and support staff access to customer data

FINRA guidance generally applies to all individuals who have access to customer data, whether they are registered with FINRA or not. Thus, non-registered individuals who are employees of independent contractor advisers may also be subject to regulatory requirements. Advisers with employees who have access to customer data should be conscious of this and ensure that appropriate standards for such individuals are in place and followed.

**Phishing**

FINRA has chosen to make the prevention of “social engineering” attacks a main focus of their guidance. Some of the largest and most extensive breaches in the broker-dealer community in recent years have been a result of “phishing” or a similar scheme.

Phishing is an example of what has been described as “social engineering”. Social engineering is an attack methodology that relies heavily on human interaction and often involves manipulating people into deviating from normal security procedures and best practices in order to gain access to systems, networks, or physical locations to make improper use of electronic information for financial gain. Phishing is the practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. The objectives of these schemes are to trick or convince an employee to take action that will reveal or give access to sensitive information. Training, policies and procedures are methods that FINRA recommends in preventing and mitigating attacks. During FINRA’s audits of broker-dealers in 2019, phishing has been the most common inquiry in connection with cybersecurity examinations.

Some broker-dealers have implemented systems to control access to sensitive data based on users having completed training related to social engineering and/or phishing. FINRA has also suggested the following as possible control mechanisms:

- Implementing email scanning and filtering to prevent phishing communications from being received by users
- Simulated phishing campaigns designed to evaluate user awareness of phishing and related techniques
- Limitations on access to data through use of Multi-Factor Authentication (MFA) and Data Loss Prevention solutions
- Logging of all incidents and responses.

**Insider Threats**

FINRA has noted that individuals within an organization can significantly compromise sensitive firm or customer data. As such, it is necessary for broker-dealers to put technological and procedural controls in place to prevent and mitigate incidents or breaches that may result from unauthorized use of firms’ systems or data by individuals who otherwise authorized to use them. An insider could be an employee, an adviser, or a third party, such as a vendor. Any of these individuals may cause a breach either intentionally or inadvertently.
To address the possibility of Insider Threats, FINRA has recommended the following as possible mitigation techniques:

- Training for all individuals classified as Insiders
- Ongoing support and reminders from senior management of the firm regarding the importance of vigilance
- Technical Controls, including Identity and access management - Which individuals have access to which types of data? How can they access it? What are the password and authentication requirements?
- Data Loss Prevention (DLP) - Data should be classified as sensitive based on criteria adopted by the firm. Once it is identified as such, restrictions should be put in place to control movement of that data within and outside of the firm’s systems. For example, data labeled as PII may not be able to be downloaded onto a local device such as a disc writer or thumb drive, or may not be allowed to be printed. DLP-specific software should be considered to effectuate these policies
- Security Information and Event Management. (SIEM) - This is a relatively new technology which focuses on aggregating data from multiple IT assets and generating alerts based on what is defined as risky or dangerous activity. SIEM tools can provide real-time alerts so that organizations can take immediate action to limit exposure.

Technical Control recommendations represent relatively new ground for FINRA. These are tools or policies that many broker-dealers do not currently have in place, and it is likely that this area will get more focus during FINRA examinations in 2020 and beyond.

**Penetration Testing**

Ensuring the fortitude of computer networks at both the home office and branch level is viewed as essential by FINRA. Penetration testing, or “Pen testing” is a technique that has existed for many years and consists of hiring a third party to attempt to gain access to the firm’s IT systems or information to determine the effectiveness of its security program. The FINRA guidance discusses:

- Types of Pen tests that can be performed
- Frequency of testing
- Parameters of effective Pen tests
- Due diligence on third-party testers
- Managing results

As with Phishing, some firms are exploring solutions that prevent access to sensitive information based on the results of the Pen tests.

**Mobile Devices**

FINRA has dedicated an entire section to guidance relating to use of mobile devices such as cellphones and laptop/tablet computers. The rapid proliferation of these devices has proven challenging for broker-dealers in managing policies and access. Mobile devices have also become a material exposure point for data breaches given their potential for dual usage for both personal and business purposes. Use of these devices is a major theme in the FINRA guidance, which covers both home office, adviser and customer activity.
FINRA recommends several specific actions with respect to mobile devices, including:

- Establishment of policies for staff and advisors to protect sensitive firm data
- Standards for the use of personal devices for firm business
- Training for all staff and advisers
- Ensuring the integrity of passwords and “timeouts”, which effectively “lock” a device after a certain period of inactivity
- Ensuring that devices aren’t “Jailbroken”. Jailbreaking is an attack designed to remove manufacturer or carrier restrictions from a device. This usually involves running an attack on a user’s device to replace the manufacturer’s factory-installed operating system with software designed to give unauthorized users access to data or IT systems
- Enabling capabilities to “wipe” information from devices remotely

**Small Firms**

In addition to the sections mentioned above, FINRA provides specific guidance for Small Member Firms with respect to cybersecurity controls. This is helpful in setting a framework for firms with limited resources. The controls include:

- Patch maintenance
- Secure system configuration
- Identity and access management
- Vulnerability scanning
- Endpoint malware protection
- E-mail and browser protection
- Perimeter security
- Security awareness training
- Risk assessments
- Data protection
- Third-Party risk management
- Branch controls
- Drafting and implementation of policies and procedures

While it is expansive and detailed, FINRA’s guidance is prescriptive in nature, which has helped many broker-dealers understand and meet the requirements. Reports from broker-dealers indicate that branch controls, Phishing, and penetration testing have received the most attention from FINRA during recent examinations. It is likely that the other issues will get more coverage in 2020 and beyond.
CONSIDERATIONS SPECIFIC TO BRANCH OFFICES OF IBDS

FINRA has issued cybersecurity guidance that is applicable to all member firms and advisers, but it has noted that there are circumstances where different considerations might apply to advisers in branch offices. This is particularly true for IBDs, where virtually all advisers are located in branch offices that are not owned or under the physical control of the broker-dealer. Perhaps more importantly, most advisers affiliated with IBDs utilize IT assets such as computers, mobile devices, and wi-fi networks that are not under the control of the broker-dealer. This creates issues that traditional financial services firms do not encounter, since advisers affiliated with IBDs are generally free to use equipment and software that is different from that of the firm. In addition, many advisers conduct Outside Business Activities (OBAs) that are separate from the business of the broker-dealer. This creates issues regarding separation of customer from non-customer data. Depending upon the type of OBA, legal or regulatory standards may require that customer data may only be shared with third parties under limited circumstances. We will address this dichotomy below.

THE FINRA TOP 10 LIST FOR BRANCH OFFICES

FINRA has identified several specific items with respect to data protection that member firms must have to demonstrate that they have adequate controls and safeguards in place to protect their data. They include:

1. **Least Privileged Access** – Least Privileged Access is based on the concept of only giving access to data or information to individuals for whom it is necessary to perform tasks associated with their job function. Any task that is not routine or standard for that individual should require granting of elevated privileges by an appropriate supervisor or administrator. This process can be managed by software products that allows the user to “check-out” a password for elevated privileges, perform the task, and then “check-in” the password. The entire session should be recorded for auditing purposes.

2. **Vulnerability Scanning and Patch Management** – All “end-points” (servers and desktop or laptop computers) should be scanned to determine if any published security vulnerability issues are present. When an item is flagged, it should be evaluated and assigned to a classification from “low” to “critical”. This classification should determine the criteria that governs when and what kind of corrective action must be taken.

3. **Data Loss Prevention (DLP)** – The aim of a DLP program is to assure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer. Most DLP solutions have three deployment strategies ranging from:
   - Logging all suspect events,
   - Logging events while also sending alerts, and
   - Providing analysis, monitoring or blocking suspicious events before data is released.

4. **Identity Management—Verification and Multi-Factor Authentication (MFA)** – This covers the process of onboarding users into firm IT systems, determining what systems individuals can access, and the use of multi-factor authentication to ensure that identification of the party is beyond dispute. MFA for both verbal and digital contact is a high priority in the view of regulatory agencies.

5. **Data Encryption** – This involves encoding or encryption of data so that it can only be accessed or decrypted by a user with the correct encryption key. ISO and NIST address the need to encrypt both data which is “at rest” and “in flight”. Any document containing PII or confidential data must be encrypted prior to sending.
6. Penetration Testing – “Pen testing” or “ethical hacking”, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit. This is generally a service performed by a vendor on a rotational basis and should be done at least quarterly. It is usually automated and should allow the firm to identify vulnerabilities and make any necessary changes to defend IT systems.

7. Incident Response – Each firm should have a Security Incident Response Team (SIRT) and a defined process for responding to all incidents. This should include the circumstances under which an incident is identified, who is responsible for correcting or reporting it and communication strategies to management, employees, customers, regulators, and any other stakeholders.

8. Awareness and Training – Information Security programs should be reinforced by strong user training and awareness programs. At a minimum, every employee should be required to complete Information Security training upon hiring and annually thereafter. In addition, training on Phishing and social engineering should be conducted on an ongoing basis for all employees. Results should be communicated to senior management of the firm and used to adjust training programs.

9. End-Point Management – All firms should track, control, and manage every aspect of devices that have access to firm data, including laptop or tablet computers and personal devices such as cellphones. This includes everything from patch management, disabling USB ports to restrict removal of data and what software resides on each device. Firms should consider removing administrative rights to all devices to ensure that the end-user cannot make any additions or changes to firm-installed software.

10. Risk Assessment – All firms should perform a Risk Assessment exercise on a regular basis. The depth and frequency of such reviews should depend on the size and complexity of the firm's business, the number and type of system users, and risks that the firm has identified. The Risk Assessment should contain a comprehensive list of risks to which a company might be subject and should be used to construct the Risk Management component of the firm’s Information Security Strategy and Business Resiliency plan. There are a wide variety of tools and companies that do this. If you elect to retain one to assist in this process, make sure they follow NIST or ISO standards.

OTHER CONSIDERATIONS FOR BRANCH OFFICES OF IBDS

In addition to employees, IBDs have large numbers of independent contractor representatives and support staff. Most of them own and maintain their own computers and other equipment and utilize systems that are not owned or controlled by the firm. This limits the ability of the IBD to control the use of that equipment and monitor or prevent breaches. In addition, many advisers also conduct other business activities independent from the firm, and some of these activities involve costumer data that is subject to rules or protocols established by other regulatory agencies. For example, many representatives of IBDs conduct separate business as insurance agents. They collect and maintain information for use in those businesses and have obligations to protect PII and other client information. In some cases, this necessitates creation of a “Chinese Wall” to prevent the IBD from having access to certain information related to clients of unaffiliated businesses.17

Many of the considerations outlined above apply equally to cybersecurity and privacy in branch offices, but the fact that the firm does not have the same degree of control over the activities of independent contractors as it does with employees creates a unique set of risks and considerations. A primary vulnerability exists with field offices, advisers, and administrative staff. Branch offices often lack the scale, expertise, and resources to effectively manage cyber risks. They are thus more likely to have outdated encryption and/or technology and are therefore more susceptible to external hacking attempts. In addition, advisers and administrative staff are the direct recipients of fraudulent asset movement requests initiated by hackers with information obtained from compromised client information.

17 See, for example, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.
This inherent vulnerability can be addressed through a number of different practices adopted by IBDs and RIAs, including Cybersecurity Training and Testing, establishment and use of Written Supervisory Procedures (“WSPs”) and Client Education.

**Cybersecurity Training and Testing**

As previously discussed, Phishing has become the most common method designed to compromise systems and client information. Broker-dealers should implement mandatory firm-element training for all affiliated persons on no less than an annual basis to ensure that advisors are receiving updated and current information on the multiple evolving methods utilized by hackers including, but not limited to, Phishing. In addition, firms should execute simulated Phishing campaigns on an ongoing basis to ensure the training is effective for both field personnel and home/back-office employees. Training should also encompass other elements of cybersecurity such as imposter websites, malware, account compromise or takeover, fraudulent wires, ransomware, distributed denial-of-service (DDoS) attacks, and vendor breaches.

**Written Supervisory Procedures**

Broker-dealers should maintain and update written policies and procedures designed to reinforce the concepts delivered in the adviser training noted above. Depending on the nature and size of the firm, such policies and procedures may include:

- A requirement for anti-virus/anti-malware and encryption software to be current for all devices utilized for securities business and communications with customers. Firms should consider testing this on a standard audit cycle.

- A requirement to document contact with customers to verify requests for trading or asset disbursements received via email. Many firms have procedures that require an adviser speak directly with a client before authorizing a disbursement request that is received by any electronic method such as e-mail. If an advisor or administrative staff person has called the client to verify a disbursement request and if the request is false, the disbursement can be stopped. The client will often appreciate the diligence and potential exposure they have avoided by not having to deal with an identity theft incident. Even in cases where a client is reimbursed by the firm after a fraudulent request, the customer may doubt the ability of the firm to protect their assets and privacy and may consider terminating their relationship as a result. The cost of a security breach is not measured only in financial terms. The firm and the adviser may suffer reputational damage with clients if the firm determines that client notification is required in connection with data that was or may have been compromised.

- Requirements for documenting authorized access to and use of client data:
  - Verification procedures for authorized access to client data based on affiliation status (registered, non-registered, field user, or home/back-office employee) and role (registered representative, administrative staff, and hierarchy/role of employees and representatives).

- Individuals who are granted access should be made aware that they are responsible for practicing safe access methods and completing firm-element training on no less than an annual basis.

- Vendor Risk Assessments (VRAs) - All vendors should be able to show they provide adequate security of client data, they are compliant with the firm’s encryption standards, and that they can comply with the firm’s compliance and supervision policies (i.e., if the vendor provides email communications to or from clients, are those being captured and retained for supervision and retention?).

---

• System Access for Individuals
  ° This includes non-registered persons such as summer interns and/or family members who may have direct (systems access) or indirect (printed/hard-copy) access to client data, even temporarily.
  ° All persons who may have direct or indirect access to client data should be subject to the broker-dealer’s background check process, including fingerprinting, prior to providing any services to be sure that they do not pose a risk to the firm.
  ° Affiliation with the firm is often required to ensure that those individuals are eligible for Error and Omission Insurance coverage, to the extent that the firm maintains such coverage. (See the discussion of Insurance Coverage, below.)

• Physical Security of Documents - Client records and other confidential information are often maintained in physical as well as electronic form. Firms should have written policies and procedures relating to security of physical documents. Areas of concern include:
  ° If the broker-dealer is using an electronic system for books & records purposes, such systems should be backed-up on a regular/periodic basis and specifically addressed in the firm’s Business Continuity Plan (BCP) processes.
  ° “Office sharing” arrangements where an advisor shares office space with an unaffiliated business or entity. Considerations include:
    ■ Are there “firewalls” in place to prevent the inadvertent exposure of client data (i.e., separate printers/faxes/scanners)?
    ■ Are there separate, secure/locked locations for client files and records?
    ■ Are there separate phone lines and signage to mitigate the potential for client confusion regarding with whom they are doing business?

• Requirements to Encrypt Mobile Devices- Encryption of mobile devices is a critical component to data loss prevention. Communications with customers via email and/or text messages from mobile devices should only be made via firm-approved/registered email addresses and text applications that are both protected and captured via the firm’s archiving platform for review and retention as required by industry regulations.

  The written policies and procedures of the firm must be practical and enforceable. As with all policies and procedures, if a control mechanism cannot be appropriately tested to document compliance, the firm should reconsider the scope and applicability of the policy. For example, if the firm requires all access to the firm’s systems and customer information must be transmitted via a virtual private network (VPN) the firm should have a method by which to test and confirm compliance with that requirement.

**Client Education**

Client education regarding common practices utilized by hackers, best practices for prevention, and awareness of red flags can assist by limiting successful attempts and fraudulent use or access to client information. Education should include information regarding scams frequently aimed at vulnerable or unsophisticated clients such as seniors that result in the customer making a legitimate request for funds to be directed to illegitimate recipients. These include schemes such as new “online friends”/romantic interests, scams that require the customer to pay funds upfront in order to receive a larger amount or require the customer to pay taxes upfront for an inheritance or cash prize/sweepstakes. Client education can have other beneficial effects, reminding clients that they play an important part in maintaining the security of their information and assets. Clients are often the first line of defense in identifying and stopping improper actions.
MITIGATION TECHNIQUES

In an attempt to mitigate the complex threats associated with a cybersecurity breach, broker-dealers should consider the use of software tools that can be deployed to help with some of the issues noted above. Such tools include consistent use of quality anti-virus/anti-malware protection for all electronic devices utilized for access to client information and products such as AVG, Carbon Black or equivalent. Password managers such as LastPass, Carbonite, Backblaze, or similar products for backup and storage of passwords are also recommended.

With regard to asset inventory and technical controls, firms should consider exploring endpoint device compliance solutions. There are software options that are tailored for broker-dealers and advisors such as Workplace Frontline, made by OS33.

Additional consideration should be given to the use and backup of cloud-based services such as VEEM and LoJack for laptops/mobile devices so they can be wiped remotely if stolen. Depending on the size of your firm, use of a written cybersecurity checklist and inventory of all devices issued and to whom they are assigned is recommended, if applicable.

It is also recommended for firms to look to satisfy DLP and Identity & Access Management guidance from both FINRA and the SEC. There are a host of targeted software solutions available on the market. Some firms may wish to consider solutions tailored for the industry such as Workplace Stronghold, made by OS33.

The use of customer relationship management (CRM) programs should be evaluated to determine if policies and procedures are appropriate to the broker-dealer’s business model. Firms may want to limit what information can be maintained in CRM systems (i.e., only last 4 digits of client identifiers such as Social Security Numbers including only the day and month (but not year) of date of birth, or requirements that field offices only use a firm-sponsored CRM system that is behind the firm’s firewall. Processes to protect customer privacy and opt-out options regarding the sharing and transfer of customer information must be considered with the use of CRM programs.

Firms should also consider obtaining insurance coverage sufficient to address any financial damage that they may incur in connection with cybersecurity incidents or other breaches. This may take the form of a cybersecurity addendum to their Error and Omission or other coverage or may be obtained as a standalone policy. Coverage should include:

- Reimbursement for damages suffered by clients or third parties as a result of unauthorized use of client data. This includes reimbursement to clients in the event of unauthorized disbursements or transactions, and the cost of remediation in the event of such actions. This could include the cost of providing credit monitoring services for clients whose PII is compromised.
- Reimbursement to the firm for costs incurred in recovering data lost to hackers or other unauthorized users, or replacement of equipment damaged as a result of intrusions. Firms may also consider obtaining business interruption insurance to cover other costs that they may incur if they cannot operate normally due to a data breach or other cybersecurity incident.
- There are often limits on the ability to obtain insurance to cover costs such as fines or penalties assessed by regulatory agencies for violations of applicable law or rules, but firms should consider obtaining coverage for these items to the extent that they are available. As discussed below, such penalties can range into the millions of dollars.
- In designing policies and procedures, firms should be aware that insurance coverage may be compromised or nullified if the firm or individuals associated with it do not follow applicable firms’ procedures. (i.e., if the field office did not verbally confirm a distribution request received via email from a customer).
Human Resources Security

All home office staff should certify their compliance with your firm’s IT Policy, which should govern appropriate usage and affirm the importance of the confidentiality, integrity, and available IT Systems. Firms should ensure all employees’ or third-party contractors’ access to information assets are suitable for their roles and that they understand their responsibilities at onboarding, during employment, while under contract, and after termination. Controls include background checks, non-disclosure agreements, periodic access control reviews, audits, formal and informal training, and an orderly termination process that includes the return and wipe of assets and removal of access to information systems.

Information & Data Security

File and Data Storage

Consider the use of full disk, BIOS-level encryption for all laptops and desktops. All data at rest is encrypted using industry standard technologies. This ensures protection against data loss in the event of theft or misplacement.

Securing Documents and File Server

All file and document repositories should be strictly secured by logical access control policies.

FTP transfers between your firm and external firms should be handled via SFTP or FTPS depending on the requirements of the counter party. Key management for these protocols is typically handled by internal technology staff.

Software Development Security

Software development practices should adhere to industry best practices and Sarbanes-Oxley controls. Your firm’s internal software development controls should be audited by internal and third-party auditors. Changes to websites and applications should have penetration testing performed by internal developers prior to release to a production environment. In addition, all applications should be tested by a third party to ensure code is secure from common hacking strategies.

Email Encryption

Your firm should consider the use of automatic encryption and data leak prevention engines that screen and enforce security policy and the protection of personally identifiable information. All email sent to recipients not supporting TLS should be sent to a secure portal to retrieve messages.
Web Identity and Access Management & Dual Factor Authentication

Along with multi-factor authentication, your firm should employ a secure and robust self-service password reset mechanism. Password strength and expiration rules should be managed centrally and adhere to your firm’s IT password policy. User activity and access should be logged and monitored per your firm’s IT Policy.

Redundancy and Disaster Recovery

Your firm should consider using a multi-step approach to achieving redundancy as well as disaster recovery. Data should be stored securely and backed up between primary and secondary geographically dispersed locations. Backups should be taken regularly and stored at an offsite secure location.

All locations should have remote work facilities established so that, in the event of a disaster, employees have a secondary work location to continue to work and process business.

Database Security

Applications requiring database access should be given a SQL user account with limited access rights to the necessary databases. SQL accounts should be bound by the same password policy as the Active Directory domain. Access to individual client data in a database should be restricted by application role-based security. Sensitive client data in the database should be encrypted.

Encryption should be utilized when needed to secure data, and access to these account credentials and keys should be restricted.

Mobile Device Management

All mobile devices connected to your firm’s enterprise email platform should be centrally managed via security policy. Policy should be enforced by the email host.

Suggested Security Settings

Device Password Required
Device Encryption Required
Storage Card Encryption Required
Minimum Passcode Length of 4
Biometrics Allowed
Max Passcode Failures Attempts is 10
Idle Timeout Lock is 10 min
**Suggested Hardware Settings**
Bluetooth Allowed  
Camera Allowed  
Wifi Allowed  
Storage Cards Allowed

**Suggested Message Settings**
Texting Allowed  
Attachments Allowed

**Suggested Software Settings**
Personal Email Allowed  
Data Tethering Allowed  
Remote Desktop Allowed  
Browser Allowed  
Desktop Sync Allowed  
HTML Email Allowed

---

**Bring Your Own Device Policy**

This policy is intended to protect the integrity and security of Your firm’s networks and data. Firms that permit users to bring their own devices (laptops, smartphones, tablets) into the office should consider the following guidelines.

**Acceptable Use**

Devices should be connected to guest wi-fi. Internal corporate wi-fi should be restricted to domain joined PCs. Access to the internal wi-fi should only possible with a domain certificate.  
Devices should abide by a mobile device management (MDM) policy.  
Devices connected to corporate email should be forced into the MDM policy.  
Smartphones and tablets connecting to corporate email should be quarantined until verified by Technology Solutions.

**Network Security**

**Intrusion Detection**

Your firm should consider leveraging real-time threat and intrusion prevention services to monitor communication points on your web servers, externally facing applications, and networks. Event management and monitoring should be handled by a 24/7 offsite monitoring hosted service. The system used should monitor data transmission along primary subnets. The sensors should act as a vulnerability scanner that evaluates the current level of exposure associated with each device on the network.
The system’s alarm monitoring should use threat modeling, which quantifies the type of attack by the potential vulnerability to determine the overall risk. If an alarm is generated, it should be investigated by the operations center immediately to determine if the alarm is credible based on human intelligence. The responses to a positive alarm can include automatically shutting down the attack source switch port.

**Internet Usage Monitoring & Control**

All Your firm web-based traffic should be monitored, logged, and filtered by a category-based filtering device. Malicious and harmful sites should be explicitly blocked.

**Denial of Service Response (DoS)**

DoS attacks should be detected and prevented by use of your firm’s Intrusion Detection hosted service in conjunction with support from the ISP and data center hosting facility.

**Wired Network Access Security**

Physical and logical access controls are employed to restrict wired network access. All physical network device provisioning should be governed by Your firm’s IT Policy.

**Password Management**

Your firm should comply with industry best practices for password complexity, expiration, and rotation rules. Password management is typically handled centrally by approved administrative personnel for all accounts and should adhere to Your firm’s IT Policy.

**Network Port Blocking Gateway**

Your firm firewalls should restrict data transmission to specific ports. Port and firewall rules should be audited and follow a strict change control process for any approved updates. Your firm port and firewall security position should be reviewed periodically by internal and third-party auditors.

On an annual basis, your firm should undertake penetration testing by an outside security firm that leverages cutting edge security and practical organizational defense mechanisms. The firm should leverage both automated security tools as well as expert human assessments.

**Spam and Malware Filtering**

Your firm’s spam filtering solution should be consistent with the industry leaders within the financial services industry. This filtering should monitor all incoming/outgoing emails to and from the organization.

**Wireless Network Access Security**

Your firm’s wireless access should be encrypted and restricted to authorized users.
Physical & Environmental Security

Asset Management
Your firm should have indexes of all hardware, software, replications, and backups.

Secure Equipment Disposal
All storage devices disposed of by Your firm should be subject to a low-level wipe to ensure the non-recoverability of the data. This includes drives and tapes.

Building Access
Your firm’s buildings should only be accessible with access badges or employee escort. In addition, data centers and network areas should only be accessible with additional access badge checks or keys. All entrances are tracked into log files and reviewed as necessary.

Office Access
Offices that contain sensitive information should be locked with individual keys. Individuals that access sensitive information should have lockable file cabinets for document storage.

Office Surveillance
Your firm should consider monitoring offices with motion detector cameras. All ingress and egress locations should be recorded.

Secure Office Areas
Certain areas that require additional security should be within locked areas and accessible only by those specific employees assigned to that department.

Data Loss Prevention

Encrypted Devices
All Windows machines should be encrypted using hardware and software-based encryption. Smartphones and tablets use native encryption technologies. This protects Your firm in the event of loss or theft of a device

VPN Security
Full IP VPN should only be allowed on domain joined PCs through certificate verification. For non-domain clients, only remote desktop should be allowed. This restricts access to file shares and other internal corporate resources. All VPN connections should be forced through multifactor authentication.
Pattern Searches for Email
All outbound emails should be checked for patterns deemed critical. Messages matching these patterns should be forced to send via secure portal.

Outbound TLS
All messages outbound should be sent via TLS regardless of content. If the recipient does not support TLS, they should be forced to retrieve their message in the secure portal.

Risk Assessment

System Patching
All Windows systems should be patched at least on a monthly basis.
Third party systems should be patched on an as needed basis.

Vulnerability Scanning
Windows systems should be scanned at least weekly for missing patches to be applied.

Perimeter Detection
Intrusion detection should occur at the perimeter adjacent to the perimeter firewalls. Alerts should be centrally managed and escalation notifications should occur in the event of a high-risk event.

Penetration Testing
Penetration testing should be performed at least annually for all externally available IP addresses. Any critical and high-risk vulnerabilities should be addressed immediately. Any lower and medium risk vulnerabilities should be evaluated for proper remediation.

Phishing Exercises
Your firm should operate an annual phishing exercise against a random sample of employees via email. These employees can be sent a suspicious email asking them to click a link taking them to a fraudulent website. They can be asked to login and download an Excel file with a macro, and then asked to allow this macro to run. Reports can be generated on what percentage of users remain vulnerable at each deeper step into the phishing attempt.
A Data Classification Policy provides a framework for managing assets based on their business value, regulatory requirements and the potential impact to customers and the business should these assets be lost or compromised. This policy also creates guidelines for applying the appropriate levels of protection to address fiduciary, proprietary, ethical, or operational considerations, as well as any governing law related to these data sets. All firm information assets, whether electronic or printed, should be classified at the appropriate level (as detailed below) to ensure they are handled in the appropriate manner.

**Objectives:**

The purpose of the Data Classification Policy is to provide a foundation for the development and implementation of necessary security controls to protect information according to its value and/or risk. The Classification Policy is also designed to assign control element settings for each category of data.

Security standards, which define these security controls and requirements, may include*: document marking/labeling, release procedures, privacy, transmission requirements, printing protection, storage requirements, destruction methods, physical security requirements, access controls, backup requirements, transport procedures, encryption requirements, and incident reporting procedures.

* When provided in this policy, examples are illustrative only, and serve to assist in classifying data sets, and are not to be considered an exhaustive list of requirements. Nothing in this policy is intended to identify a restriction on the right of offices to require policies and/or procedures in addition to the ones identified in this document.

**SECTION 1: CLASSIFICATION LEVELS**

All assets owned, used, created, stored or maintained by Your firm can be classified into the following categories:

- Confidential
- Internal Use
- Public

Your firm should carefully evaluate the assets for classification into one of the categories above.

Owners should be responsible for ensuring appropriate managerial, operational, physical, and technical controls for access to, use of, transmission of, and disposal of data in compliance with this policy.
Confidential

Assets should be classified as Confidential when the unauthorized disclosure of those data sets would cause a material impact to your firm, its affiliates, clients or stakeholders.

Any data breach/disclosure should be reviewed by an Incident Response Team to determine if the breach/disclosure can be classified as a Material Event. A Material Event may include but is not limited to the following:

- A financial loss/cost of $50,000 or greater
- A potential violation of laws, regulations or rules of self-regulatory organization
- Create a widespread negative public opinion of the organization
- Prevent the continuation of normal business operations

Access to Confidential data must be controlled from creation to destruction and should be granted only to those persons that require such access in order to perform their business function (“need-to-know”). Access to Confidential data should be authorized by the appropriate accountable party, normally the Data Owner.

Examples of Confidential Data:

- Any data set that would uniquely identify a specific individual (Personally Indefinable Information or PII). Typically, PII is defined as an individual’s first name or first initial and last name in combination with any one or more of the following data elements:
  - Social Security Number
  - Driver’s license number or government issued Identification Card number
  - Account number, credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account.
  - System usernames and passwords or access Codes
- Protected Health Information or individually identifiable health information, including
  - An individual’s past, present or future physical or mental health or condition,
  - The provision of health care to an individual
  - the past, present, or future payment for the provision of health care to an individual
- Any information deemed confidential by statute or regulation

Handling of Confidential Data:

Access to confidential data sets stored on information systems internal to the organization (“at rest” behind corporate firewalls) should be restricted to a “need-to-know” basis:

- Access to Confidential Data Sets should be approved (typically by the Data Owner)
- Access to Confidential Data Sets should be reviewed on a yearly basis

Any transmission of confidential data sets to parties external to the organization should be encrypted “in transit”:

- Email transmission should leverage inline (TLS) or portal-based encryption
- Removable media, laptops or mobile devices should be encrypted
- Other electronic transfer methods should leverage encryption technologies commonly regarded as secure (SSL, SSH)
Confidential data sets stored internally (in office), but not on active information systems (examples: paper files, removable media, etc.) should be stored in restricted access locations:

• Confidential data should be kept in locked storage cabinets or storage rooms
• Desktops should be encrypted
• All workstations and servers should run anti-virus
• Staff accessing or processing confidential data should secure or shred it when not at their workstations (“Clean Desk” policy)
• Copier/printer/fax machines should be checked for confidential documents at the end of the workday

External parties, business partners or vendors holding Your firm’s confidential data sets should:

• Certify that data stored “at rest” is encrypted
• Operate under a non-disclosure agreement
• Ensure controls are in place so that your firm authorizes access and appropriate use of these data sets
• Provide industry-recognized certifications of proper operational controls which are updated at least on an annual basis

When equipment or media that may have contained confidential data sets is being discarded, returned, recycled or donated, all employees and affiliated persons of your firm should:

• Ensure any equipment (i.e. hard drives) have a “low level wipe” standard.
  ◦ This includes photo copier, fax machines, printers, desktop/laptop computers and mobile devices/tablets
• If hard drives cannot be wiped, they should be removed and destroyed.

All paper records that contain confidential data should be shredded before being discarded or recycled.

**Internal Use**

Data should be classified as Internal Use when the unauthorized disclosure of that data, while not materially damaging, would still have some negative impact to Your firm or its affiliates.

Negative impact is defined as an outcome that would cause or be considered any of the following:

• Result in a financial loss of up to $50,000
• A potential violation of laws, regulations or rules of self-regulatory organization
• Cause negative public perception of the company

Access to sensitive data must be controlled from creation to destruction and should be granted only to those persons or groups internal to the organization, or with whom Your firm has a structured business relationship. Access to sensitive data should only be granted to parties that have reasonable business need to access the data sets.

Examples of Sensitive Data:

• Client information that would not identify an individual specifically
• Internal work documents and memos to staff, not approved for external distribution
• List of system usernames without passwords
**Handling of Sensitive Data:**

Access to sensitive data sets stored on information systems internal to the organization (“at rest” behind corporate firewalls) should only be granted to those with expected business needs.

Any transmission of sensitive data sets to parties external to the organization should be encrypted, and only sent to parties with an authorized business interest/use for the data.

Sensitive data sets stored internally (in office), but not on active information systems (examples: paper files, removable media, etc.) must be stored in restricted access locations.

External parties, business partners or vendors holding Your firm sensitive data sets should:

- Ensure controls are in place so that Your firm authorizes access to these data sets
- Provide industry-recognized certifications of proper operational controls which are updated at least on an annual basis

When equipment or media that may have contained sensitive data sets is being discarded, returned, recycled or donated, offices should ensure their hard drives have a “low level wipe” performed.

All paper records that contain sensitive data should be shredded before being discarded or recycled.

**Public**

Data should be classified as public when the unauthorized disclosure of that data would result in little or no business impact. While little or no controls are required to protect the confidentiality of public data, some level of control should be required to prevent unauthorized modification or destruction of public data.

Public data is not considered sensitive; therefore, it may be granted to any requester or published with no restrictions. The integrity and validity of public data should be protected.

The appropriate Owner must authorize replication or copying of the data in order to ensure it remains accurate over time.

Examples of Public Data:

- Your firm offices’ addresses and directories
- Approved for release marketing campaigns, public relations information or press releases

**SECTION 2: MANAGEMENT ROLES**

For effective governance of the classification and handling procedures for various data sets, several data management roles should be defined.

All individuals or groups who interact with any given data must be assigned one of the following roles:

- Owner
- Custodian
- Consumer
Owners

Owners are your firm’s staff with direct operational-level responsibility for the management of one or more types of data.

Owner responsibilities may include:
• Assigning classification labels using your firm classification methodology
• Implementing safeguards for confidential data
• Ensuring proper education on the required minimum safeguards for protected data to authorized data users and data custodians

In cases where multiple data owners collect and maintain the same restricted data elements, the data owners must work together to implement a common set of safeguards.

Custodians

Custodians are Information Technology or computer system administrators responsible for the operation and management of systems and servers which collect, manage, and provide access to the organization’s data. Custodians should be authorized by the CTO of Information Technology.

Data Custodian responsibilities may include:
• Maintaining physical and system security and safeguards appropriate to the classification level of the data in their custody
• Complying with applicable computer security standards
• Managing Consumer access as authorized by appropriate Owners
• Following data handling and protection policies and procedures established by Owners and Information Technology Management

Consumers

Consumers are individuals who have been granted access to corporate data sets in order to perform assigned duties or in fulfillment of assigned roles or functions. This access is granted solely for the conduct of your firm’s business.

Data Consumer responsibilities may include:
• Following the policies and procedures established by the appropriate Owner and Information Technology Management
• Complying with federal and state laws, regulations, and policies associated with the data used
• Implementing safeguards prescribed by Information Technology Management team and the appropriate Owners for confidential data
• Reporting any unauthorized access or data misuse to your firm’s Coordinated Incident Response team
Addendum 3
Selected Privacy and Cybersecurity Enforcement Actions against Broker-Dealers and Registered Investment Advisers


Without admitting or denying the allegations of the SEC, Voya Financial Advisers (VFA) agreed to settle SEC allegations that criminals impersonating independent advisers of VFA called the firm’s support line and requested new passwords which gave the intruders access to the personal information of 5,600 customers. The perpetrators then used this information to create new online customer profiles, and also obtained access to three customers’ account documents.

Within hours of the first fraudulent reset request, a VFA adviser received an email notification and informed the firm. According to the SEC order, VFA took steps to respond to the intrusion but did not prevent the attackers from accessing the VFA portal through other compromised adviser logins.

The SEC alleges that the intruders gained access through weaknesses in VFA’s cybersecurity procedures, some of which had previously been exposed in similar frauds. In two instances when the intruders called VFA’s support line, they used phone numbers previously identified as being associated with fraudulent activity. The order also states that VFA also failed to apply its procedures to systems used by independent contractors, who make up the largest part of VFA’s workforce.

VFA agreed to a penalty in the amount of $1 million and other remedial steps.


Without admitting or denying FINRA allegations, Buttonwood Partners, Inc. consented to the entry of findings that it failed to establish, maintain and enforce a supervisory system and Written Supervisory Procedures (WSP) reasonably designed to review and monitor transmittals of funds from customer accounts to third-party accounts. As a result, funds belonging to a firm customer were fraudulently transferred after her email account was hacked.

The findings also stated that the firm had no WSP addressing transmittal of customers’ funds to third-party accounts based on a request via email or other electronic communication. The firm’s system was unreasonable because it allowed firm personnel to copy pre-signed, blank forms as the only means of recording the customer’s authorization of each funds transfer, with no requirement for a customer confirmation, notification or follow-up for each transfer.

In a settled enforcement action, FINRA alleged that Lincoln Financial Securities Corporation (LFS) migrated many of its records—including those containing customer non-public personal information such as social security numbers—to a cloud-based server. LFS failed, however, to ensure that the third-party cloud host had sufficient antivirus software or data encryption in place. Information relating to approximately 5,400 customers was exposed.

FINRA alleged that LFS’s WSP were insufficient to provide adequate guidance to the firm’s employees in implementing and enforcing policies and procedures. For example, the data security policy required that firewalls must be used to prevent unauthorized access, but the policies offered no help in how to install such a firewall.

LFS agreed to pay a monetary fine in the amount of $650,000.


In a settled enforcement matter, the SEC alleged that a broker-dealer failed to adopt written policies and procedures reasonably designed to insure the security and confidentiality of customer records and information in violation of Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)) (the “Safeguards Rule”), and to make and keep certain communications relating to its business.

From January 20, 2012 until approximately June 2014, the firm used email addresses other than those in its official domain name to electronically receive more than 4,000 faxes from customers and other third parties. These faxes routinely included sensitive customer records and information, such as customer names, addresses, social security numbers, bank and brokerage account numbers, and copies of driver’s licenses and passports.

The SEC alleged that, although the firm had WSP covering data protection, they were not reasonably designed to protect customer records and information as required by the Safeguards Rule. The WSP failed to designate the responsible supervisor, to address how customer records and information transmitted through the electronic fax system was to be handled, contained blanks as to how the firm was to comply with the Safeguards Rule, and did not reflect actual business practices.
Addendum 4
Cybersecurity and Resiliency Observations
from the U.S. Securities and Exchange Commission

Cybersecurity and Resiliency Observations
OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS

U.S. SECURITIES AND EXCHANGE COMMISSION
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance and Risk Management</td>
<td>2</td>
</tr>
<tr>
<td>Access Rights and Controls</td>
<td>3</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>4</td>
</tr>
<tr>
<td>Mobile Security</td>
<td>6</td>
</tr>
<tr>
<td>Incident Response and Resiliency</td>
<td>6</td>
</tr>
<tr>
<td>Vendor Management</td>
<td>8</td>
</tr>
<tr>
<td>Training and Awareness</td>
<td>9</td>
</tr>
<tr>
<td>Additional Resources</td>
<td>9</td>
</tr>
<tr>
<td>Conclusion</td>
<td>10</td>
</tr>
</tbody>
</table>

**DISCLAIMER:** This statement represents the views of the staff of the Office of Compliance Inspections and Examinations (OCIE). It is not a rule, regulation, or statement of the U.S. Securities and Exchange Commission. The Commission has neither approved nor disapproved its content. This statement, like all staff guidance, has no legal force or effect: it does not alter or amend applicable law, and it creates no new or additional obligations for any person.
Cybersecurity threats come from many sources, are global in nature, and do not discriminate across the spectrum of securities and financial markets and market participants. The seriousness of the threats and the potential consequences to investors, issuers, and other securities market participants, and the financial markets and economy more generally, are significant and increasing. As markets, market participants, and their vendors have increasingly relied on technology, including digital connections and systems, cybersecurity risk management has become essential. Indeed, in an environment in which cyber threat actors are becoming more aggressive and sophisticated—and in some cases are backed by substantial resources including from nation state actors—firms participating in the securities markets, market infrastructure providers and vendors should all appropriately monitor, assess and manage their cybersecurity risk profiles, including their operational resiliency.

The SEC has focused on cybersecurity issues for many years, with particular attention to market systems, customer data protection, disclosure of material cybersecurity risks and incidents, and compliance with legal and regulatory obligations under the federal securities laws. Among other things, the SEC maintains a Cybersecurity Spotlight webpage that provides cybersecurity-related information and guidance. Cybersecurity is also a key priority for OCIE. OCIE has highlighted information security as a key risk for security market participants, and has included it as a key element in its examination program over the past eight years. OCIE has also published eight risk alerts related to cybersecurity.

1 For example, the SEC’s Division of Enforcement established the Cyber Unit in September 2017, the SEC hosted a roundtable in 2014 to discuss cybersecurity issues, and the SEC’s Office of Investor Education and Advocacy published Investor Alerts and Bulletins, such as Investor Alert: Identity Theft, Data Breaches and Your Investment Accounts, (Sept. 22, 2015) and Updated Investor Bulletin: Protecting Your Online Investment Accounts from Fraud, (Apr. 26, 2017).

2 “Spotlight on Cybersecurity, the SEC and You” available at www.sec.gov/spotlight/cybersecurity. This page contains information for investors, issuers, and registered firms and organizations, including the Commission Statement and Guidance on Public Company Cybersecurity Disclosures, guidance from the Division of Investment Management, the Division of Trading and Markets, and Investor Alerts and Bulletins.

Through thousands of examinations of broker-dealers, investment advisers, clearing agencies, national securities exchanges and other SEC registrants, OCIE has observed various industry practices and approaches to managing and combating cybersecurity risk and the maintenance and enhancement of operational resiliency. These include practices in the areas of governance and risk management, access rights and controls, data loss prevention, mobile security, incident response and resiliency, vendor management, and training and awareness. Recognizing that there is no such thing as a “one-size fits all” approach, and that all of these practices may not be appropriate for all organizations, we are providing these observations to assist market participants in their consideration of how to enhance cybersecurity preparedness and operational resiliency.

GOVERNANCE AND RISK MANAGEMENT

Effective cybersecurity programs start with the right tone at the top, with senior leaders who are committed to improving their organization’s cyber posture through working with others to understand, prioritize, communicate, and mitigate cybersecurity risks. While the effectiveness of any given cybersecurity program is fact-specific, we have observed that a key element of effective programs is the incorporation of a governance and risk management program that generally includes, among other things: (i) a risk assessment to identify, analyze, and prioritize cybersecurity risks to the organization; (ii) written cybersecurity policies and procedures to address those risks; and (iii) the effective implementation and enforcement of those policies and procedures.

OCIE has observed organizations utilizing the following risk management and governance measures:

- **Senior Level Engagement.** Devoting appropriate board and senior leadership attention to setting the strategy of and overseeing the organization’s cybersecurity and resiliency programs.

- **Risk Assessment.** Developing and conducting a risk assessment process to identify, manage, and mitigate cyber risks relevant to the organization’s business. This includes considering the organization’s business model, as part of defining a risk assessment methodology, and working to identify and prioritize potential vulnerabilities, including remote or traveling employees, insider threats, international operations and geopolitical risks, among others.
• **Policies and Procedures.** Adopting and implementing comprehensive written policies and procedures addressing the areas discussed below and identified risks.

• **Testing and Monitoring.** Establishing comprehensive testing and monitoring to validate the effectiveness of cybersecurity policies and procedures on a regular and frequent basis. Testing and monitoring can be informed based on cyber threat intelligence.

• **Continuously Evaluating and Adapting to Changes.** Responding promptly to testing and monitoring results by updating policies and procedures to address any gaps or weaknesses and involving board and senior leadership appropriately.

• **Communication.** Establishing internal and external communication policies and procedures to provide timely information to decision makers, customers, employees, other market participants, and regulators as appropriate.

**ACCESS RIGHTS AND CONTROLS**

Access rights and controls are used to determine appropriate users for organization systems based on job responsibilities, and to deploy controls to limit access to authorized users. Access controls generally include: (i) understanding the location of data, including client information, throughout an organization; (ii) restricting access to systems and data to authorized users; and (iii) establishing appropriate controls to prevent and monitor for unauthorized access.

OCIE has observed strategies related to access rights and controls at organizations that perform the following:

• **User Access.** Developing a clear understanding of access needs to systems and data. This includes limiting access to sensitive systems and data, based upon the user’s needs to perform legitimate and authorized activities on the organization’s information systems, and requiring periodic account reviews.

• **Access Management.** Managing user access through systems and procedures that: (i) limit access as appropriate, including during onboarding, transfers, and terminations; (ii) implement separation of duties for user access approvals; (iii) re-certify users’ access rights on a periodic basis (paying particular attention to accounts with elevated privileges including users, administrators, and service accounts); (iv) require the use of strong, and periodically changed, passwords; (v) utilize multi-factor authentication (MFA) leveraging an application or key fob to generate an additional verification code; and (vi) revoke system access immediately for individuals no longer employed by the organization, including former contractors.
• **Access Monitoring.** Monitoring user access and developing procedures that:
  (i) monitor for failed login attempts and account lockouts; (ii) ensure proper handling of customers’ requests for user name and password changes as well as procedures for authenticating anomalous or unusual customer requests; (iii) consistently review for system hardware and software changes, to identify when a change is made; and (iv) ensure that any changes are approved, properly implemented, and that any anomalies are investigated.

**DATA LOSS PREVENTION**

Data loss prevention typically includes a set of tools and processes an organization uses to ensure that sensitive data, including client information, is not lost, misused, or accessed by unauthorized users.

OCIE has observed the following data loss prevention measures utilized by organizations:

- **Vulnerability Scanning.** Establishing a vulnerability management program that includes routine scans of software code, web applications, servers and databases, workstations, and endpoints both within the organization and applicable third party providers.

- **Perimeter Security.** Implementing capabilities that are able to control, monitor, and inspect all incoming and outgoing network traffic to prevent unauthorized or harmful traffic. These capabilities include firewalls, intrusion detection systems, email security capabilities, and web proxy systems with content filtering. Implementing an enterprise data loss prevention solution capable of monitoring and blocking access to personal email, cloud-based file sharing services, social media sites, and removable media such as USB and CDs.

- **Detective Security.** Implementing capabilities that are able to detect threats on endpoints. Considering products that can utilize both signature and behavioral-based capabilities and can identify incoming fraudulent communications to prevent unauthorized software or malware from running. Establishing policies and procedures to capture and retain system logs from systems and applications for aggregation and analysis. For software that provides automated actions, such as macros and scripts, enabling optional security features or following the security guidance that may be offered by third party software providers.
- **Patch Management.** Establishing a patch management program covering all software (i.e., in-house developed, custom off-the-shelf, and other third party software) and hardware, including anti-virus and anti-malware installation.

- **Inventory Hardware and Software.** Maintaining an inventory of hardware and software assets, including identification of critical assets and information (i.e., know where they are located, and how they are protected).

- **Encryption and Network Segmentation.** Using tools and processes to secure data and systems, including: (i) encrypting data “in motion” both internally and externally; (ii) encrypting data “at rest” on all systems including laptops, desktops, mobile phones, tablets, and servers; and (iii) implementing network segmentation and access control lists to limit data availability to only authorized systems and networks.

- **Insider Threat Monitoring.** Creating an insider threat program to identify suspicious behaviors, including escalating issues to senior leadership as appropriate. Increasing the depth and frequency of testing of business systems and conducting penetration tests. Creating rules to identify and block the transmission of sensitive data (e.g., account numbers, social security numbers, trade information, and source code) from leaving the organization. Tracking corrective actions in response to findings from testing and monitoring, material changes to business operations or technology, and any other significant events.

- **Securing Legacy Systems and Equipment.** Verifying that the decommissioning and disposal of hardware and software does not create system vulnerabilities by using processes to: (i) remove sensitive information from and prompt disposal of decommissioned hardware and software; and (ii) reassess vulnerability and risk assessments as legacy systems are replaced with more modern systems.
MOBILE SECURITY

Mobile devices and applications may create additional and unique vulnerabilities. OCIE has observed the following mobile security measures at organizations utilizing mobile applications:

- **Policies and Procedures.** Establishing policies and procedures for the use of mobile devices.

- **Managing the Use of Mobile Devices.** Using a mobile device management (MDM) application or similar technology for an organization’s business, including email communication, calendar, data storage, and other activities. If using a “bring your own device” policy, ensuring that the MDM solution works with all mobile phone/device operating systems.

- **Implementing Security Measures.** Requiring the use of MFA for all internal and external users. Taking steps to prevent printing, copying, pasting, or saving information to personally owned computers, smartphones or tablets. Ensuring the ability to remotely clear data and content from a device that belongs to a former employee or from a lost device.

- **Training Employees.** Training employees on mobile device policies and effective practices to protect mobile devices.

INCIDENT RESPONSE AND RESILIENCY

Incident response includes: (i) the timely detection and appropriate disclosure of material information regarding incidents; and (ii) assessing the appropriateness of corrective actions taken in response to incidents. An important component of an incident response plan includes business continuity and resiliency (*i.e.*, if an incident were to occur, how quickly can the organization recover and again safely serve clients?).

OCIE has observed that many organizations with incident response plans tend to include the following elements:

- **Development of a Plan.** Developing a risk-assessed incident response plan for various scenarios including denial of service attacks, malicious disinformation, ransomware, key employee succession, as well as extreme but plausible scenarios. Considering past cybersecurity incidents and current cyber-threat intelligence in developing business continuity plans and policies and procedures. Establishing and maintaining procedures that include: (i) timely notification and response if an event occurs; (ii) a process to escalate incidents to appropriate levels of management, including legal and compliance functions; and (iii) communication with key stakeholders.
• **Addressing Applicable Reporting Requirements.** Determining and complying with applicable federal and state reporting requirements for cyber incidents or events, such as requirements for financial institutions to file a suspicious activity report or for public companies to disclose material risks and incidents. For example, the organization should consider:

  » Contacting local authorities or the FBI if an attack or compromise is discovered or suspected.

  » Informing regulators and sharing information, including indicators of compromise (artifacts observed on a network or operating system indicating a potential intrusion), with the appropriate organizations.

  » Notifying customers, clients, and employees promptly if their data is compromised.

• **Assigning Staff to Execute Specific Areas of the Plan.** Designating employees with specific roles and responsibilities in the event of a cyber incident. In doing so, identifying additional cybersecurity and recovery expertise in advance.

• **Testing and Assessing the Plan.** Testing the incident response plan and potential recovery times, using a variety of methods including tabletop exercises. If an incident does occur, implementing the plan and assessing the response after the incident to determine whether any changes to the procedures are necessary.

OCIE has observed the following strategies to address resiliency:

• **Maintaining an Inventory of Core Business Operations and Systems.** Identifying and prioritizing core business services. Understanding the impact on business services of an individual system or process failure. Mapping the systems and processes that support business services, including those over which the organization may not have direct control.

• **Assessing Risks and Prioritizing Business Operations.** Developing a strategy for operational resiliency with defined risk tolerances tailored to the organization. In developing a strategy, organizations consider: (i) determining which systems and processes are capable of being substituted during disruption so that business services can continue to be delivered; (ii) ensuring geographic separation of back-up data and avoid concentration risk; and (iii) the effects of business disruptions on both the institution’s stakeholders and other organizations.
- **Considering Additional Safeguards.** Maintaining back-up data in a different network and offline. Evaluating whether cybersecurity insurance is appropriate for the organization’s business.

**VENDOR MANAGEMENT**

Practices and controls related to vendor management generally include policies and procedures related to: (i) conducting due diligence for vendor selection; (ii) monitoring and overseeing vendors, and contract terms; (iii) assessing how vendor relationships are considered as part of the organization’s ongoing risk assessment process as well as how the organization determines the appropriate level of due diligence to conduct on a vendor; and (iv) assessing how vendors protect any accessible client information.

OCIE has observed the following practices in the area of vendor management by organizations:

- **Vendor Management Program.** Establishing a vendor management program to ensure vendors meet security requirements and that appropriate safeguards are implemented. Leveraging questionnaires based on reviews of industry standards (e.g., SOC 2, SSAE 18) as well as independent audits. Establishing procedures for terminating or replacing vendors, including cloud-based service providers.

- **Understanding Vendor Relationships.** Understanding all contract terms including rights, responsibilities, expectations, and other specific terms to ensure that all parties have the same understanding of how risk and security is addressed. Understanding and managing the risks related to vendor outsourcing, including vendor use of cloud-based services.

- **Vendor Monitoring and Testing.** Monitoring the vendor relationship to ensure that the vendor continues to meet security requirements and to be aware of changes to the vendor’s services or personnel.
TRAINING AND AWARENESS

Training and awareness are key components of cybersecurity programs. Training provides employees with information concerning cyber risks and responsibilities and heightens awareness of cyber threats. OCIE has observed the following practices used by organizations in the area of cybersecurity training and awareness:

- **Policies and Procedures as a Training Guide.** Training staff to implement the organization’s cybersecurity policies and procedures and engaging the workforce to build a culture of cybersecurity readiness and operational resiliency.

- **Including Examples and Exercises in Trainings.** Providing specific cybersecurity and resiliency training, including phishing exercises to help employees identify phishing emails. Including preventive measures in training, such as identifying and responding to indicators of breaches, and obtaining customer confirmation if behavior appears suspicious.

- **Training Effectiveness.** Monitoring to ensure employees attend training and assessing the effectiveness of training. Continuously re-evaluating and updating training programs based on cyber-threat intelligence.

ADDITIONAL RESOURCES

We are committed to working with federal and local partners, market participants, and others to monitor developments and effectively respond to cyber threats. In addition to checking the SEC’s Cybersecurity Spotlight page (www.sec.gov/spotlight/cybersecurity), OCIE encourages SEC registrants, issuers, other regulated entities, and investment professionals, as well as other members of the cybersecurity community, to sign up for alerts published by the Cyber Infrastructure Security Agency (CISA), which is part of the U.S. Department of Homeland Security. CISA is responsible for protecting the nation’s critical infrastructure from physical and cyber threats, and collaborates and coordinates among a broad spectrum of government and private sector organizations.

The following link can be used to sign up for CISA alerts: https://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new.
In addition to receiving CISA Cyber Alerts, many organizations participate in information-sharing groups through industry associations such as the Financial Services Information Sharing and Analysis Center (FS-ISAC, www.fsisac.com). Participation in these information sharing groups provides a mechanism for collaborating across industry and government—providing access to sector specific information about cyber best practices and early warning indicators related to cyber threats. Through such information sharing arrangements, OCIE believes that organizations are able to achieve greater cybersecurity resiliency.

Another key resource developed through the collaboration between government and industry is the National Institute of Standards and Technology Cybersecurity Framework (https://www.nist.gov/cyberframework). This voluntary framework provides a mapping of cybersecurity control objectives to industry standards, guidelines, and practices designed to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

**CONCLUSION**

In sharing these staff observations, we encourage market participants to review their practices, policies and procedures with respect to cybersecurity and operational resiliency. We believe that assessing your level of preparedness and implementing some or all of the above measures will make your organization more secure. OCIE will continue to focus on working with organizations to identify and address cybersecurity risks and encourages market participants to actively engage regulators and law enforcement in this effort.