A REPORT FROM
THE FINANCIAL INDUSTRY REGULATORY AUTHORITY

Report on Cybersecurity Practices

FEBRUARY 2015

Contents

Executive Summary

Like many organizations in the financial services and other sectors, broker-dealers (firms) are the target of cyberattacks. The frequency and sophistication of these attacks is increasing and individual broker-dealers, and the industry as a whole, must make responding to these threats a high priority.

This report is intended to assist firms in that effort. Based on FINRA's 2014 targeted examination of firms and other related initiatives, the report presents FINRA's latest work in this critical area. Given the rapidly evolving nature and pervasiveness of cyberattacks, it is unlikely to be our last.

A variety of factors are driving firms' exposure to cybersecurity threats. The interplay between advances in technology, changes in firms' business models, and changes in how firms and their customers use technology create vulnerabilities in firms' information technology systems. For example, firms' Web-based activities can create opportunities for attackers to disrupt or gain access to firm and customer information. Similarly, employees and customers are using mobile devices to access information at broker-dealers that create a variety of new avenues for attack.

The landscape of threat actors includes cybercriminals whose objective may be to steal money or information for commercial gain, nation states that may acquire information to advance national objectives, and hacktivists whose objectives may be to disrupt and embarrass an entity. Attackers, and the tools available to them, are increasingly sophisticated. Insiders, too, can pose significant threats.

This report presents an approach to cybersecurity grounded in risk management to address these threats. It identifies principles and effective practices for firms to consider, while recognizing that there is no one-size-fits-all approach to cybersecurity.

Key points in the report include:

- A sound governance framework with strong leadership is essential. Numerous firms made the point that board- and senior-level engagement on cybersecurity issues is critical to the success of firms' cybersecurity programs.
- Risk assessments serve as foundational tools for firms to understand the cybersecurity risks they face across the range of the firm's activities and assets—no matter the firm's size or business model.

- Technical controls, a central component in a firm's cybersecurity program, are highly contingent on firms' individual situations. Because the number of potential control measures is large and situation dependent, FINRA discusses only a few representative controls here. Nonetheless, at a more general level, a defense-in-depth strategy can provide an effective approach to conceptualize control implementation.
- Firms should develop, implement and test incident response plans. Key elements of such plans include containment and mitigation, eradication and recovery, investigation, notification and making customers whole.
- Broker-dealers typically use vendors for services that provide the vendor with access to sensitive firm or client information or access to firm systems. Firms should manage cybersecurity risk exposures that arise from these relationships by exercising strong due diligence across the lifecycle of their vendor relationships.
- A well-trained staff is an important defense against cyberattacks. Even well-intentioned staff can become inadvertent vectors for successful cyberattacks through, for example, the unintentional downloading of malware. Effective training helps reduce the likelihood that such attacks will be successful.
- Firms should take advantage of intelligence-sharing opportunities to protect themselves from cyber threats. FINRA believes there are significant opportunities for broker-dealers to engage in collaborative self defense through such sharing.

FINRA expects firms to consider the principles and effective practices presented in this report as they develop or enhance their cybersecurity programs. FINRA will assess the adequacy of firms' cybersecurity programs in light of the risks they face.

This report is not intended to express any legal position, and does not create any new legal requirements or change any existing regulatory obligations. Throughout the report, we identify cybersecurity practices that we believe firms should consider and tailor to their business model as they strengthen their cybersecurity efforts.

Questions/Further Information

Inquiries regarding the report may be directed to Daniel M. Sibears, Executive Vice President, Regulatory Operations/Shared Services, at (202) 728 6911; John Brady, Vice President, Cybersecurity, at (240) 386 5524; or Steven Polansky, Senior Director, Regulatory Programs/ Shared Services, at (202) 728 8331.

Background

In 2014, FINRA launched a targeted examination (sweep) to explore cybersecurity. FINRA had four primary objectives:

- to better understand the types of threats that firms face;
- to increase our understanding of firms' risk appetite, exposure and major areas of vulnerabilities in their information technology systems;
- to better understand firms' approaches to managing these threats; and
- to share observations and findings with firms.

FINRA sent its information request to a cross section of firms, including large investment banks, clearing firms, online brokerages, high-frequency traders and independent dealers.

Cybersecurity has also been a regular theme in our Regulatory and Examination Priorities Letter since 2007. In addition, in June 2011, FINRA conducted a survey of 224 firms (survey) to better understand industry information technology and cybersecurity practices and issues that may impact investor protection or market integrity. In 2010 and 2011, FINRA also conducted on-site reviews of firms of varying sizes and business models to increase our awareness of how firms control critical information technology and cyber risks.

Other financial sector regulators are, of course, also focusing on cybersecurity, and FINRA continues to work with its regulatory counterparts on issues of mutual concern.

In developing the observations and practices in this document, FINRA draws on a variety of sources, including the 2014 sweep, interviews with other organizations involved in cybersecurity, previous FINRA work on cybersecurity and publicly available information. This report focuses on select topics that serve as a resource for firms developing or advancing their cybersecurity programs:

- cybersecurity governance and risk management;
- cybersecurity risk assessment;
- technical controls;
- incident response planning;
- vendor management;
- staff training;
- cyber intelligence and information sharing; and
- cyber insurance.

Each section of the report highlights "Principles and Effective Practices." (Appendix I summarizes these principles and effective practices.) The report does not purport to cover all cybersecurity topics, nor does it provide exhaustive guidance on each cybersecurity issue discussed herein. Instead, FINRA's objective is to focus firms on a risk management-based approach to cybersecurity. This enables firms to tailor their program to their particular circumstances; as every firm in our sweep emphasized, there is no one-size-fits-all approach to cybersecurity. Many of the practices discussed in this report are geared to large firms with sophisticated management structures, but we believe small firms can benefit from this report as well, and we will continue to pursue opportunities to assist their cybersecurity efforts.

Defining "Cybersecurity"

Firms defined "cybersecurity" in different ways. For purposes of this report, FINRA takes a broad view and defines cybersecurity as the protection of investor and firm information from compromise through the use—in whole or in part—of electronic digital media, (*e.g.*, computers, mobile devices or Internet protocol-based telephony systems). "Compromise" refers to a loss of data confidentiality, integrity or availability.

Given this definition, not all issues we discuss in this report are viewed by firms as within the scope of their cybersecurity program. For example, some firms would address fraudulent wire transfers carried out through socially engineered phishing attacks through their anti-fraud, rather than their cybersecurity programs. Regardless of how firms categorize their cybersecurity control measures, what is important to FINRA is that firms have appropriate risk management measures in place to address the cybersecurity-related threats they face.

Threat Landscape

In both the 2014 sweep and the 2011 survey, firms identified the following top three threats:

- hackers penetrating firm systems;
- insiders compromising firm or client data; and
- operational risks.

Table 1 provides a more detailed breakdown of firms' responses regarding threats they face.[1]

Table 1: Summary of Firm Responses on Top Three Threats

	2014 Sweep Results (% of respondents ranking threat as 1st, 2nd or 3rd)			**2011 Survey Results** (% of respondents ranking threat as 1st, 2nd or 3rd)		
	1st	2nd	3rd	1st	2nd	3rd
Cyber risk of hackers penetrating systems for the purpose of account manipulation, defacement or data destruction, for example	33	28	11	38	33	19
Operational risk associated with environmental problems (*e.g.*, power failures) or natural disasters (*e.g.*, earthquakes, hurricanes)	22	17	17	31	16	29
Insider risk of employees or other authorized users abusing their access by harvesting sensitive information or otherwise manipulating the system or data undetected	22	11	33	24	35	22
Insider risk of employees or other authorized users placing time bombs or other destructive activities	0	11	0	0	4	5
Cyber risk of non-nation states or terrorist groups penetrating systems, for example, for the purpose of wreaking havoc	0	6	6	0	4	5
Cyber risk of nation states penetrating systems, for example, for the purpose of espionage	0	6	6	0	2	5
Cyber risk of competitors penetrating systems, for example, for the purpose of corporate espionage	0	0	0	0	2	4

Not surprisingly, the ranking of threats varies by firm and by business model. For example, online brokerage firms and retail brokerages are more likely to rank the risk of hackers as their top priority risk. Firms that engage in algorithmic trading were more likely to rank insider risks more highly. Large investment banks or broker-dealers typically ranked risks from nation states or hacktivist groups more highly than other firms.

Firms need to understand the types of threats they face, their assets most likely to be targeted for attack and the likely sources of these threats. That information should inform firms' approach to their cybersecurity program.

Case Study: Cyber Threats From Firm Customers

In one instance where FINRA took enforcement action, an online firm opened four accounts for higher-risk foreign customers who engaged in a pattern of fraudulent trading through the firm's Direct Market Access (DMA) platform. These customers hacked into accounts held at other online broker-dealers where they engaged in a short sale transaction scheme that facilitated the customers' large profits in their original firm accounts and losses in the outside, compromised accounts at the unsuspecting broker-dealers. This firm violated FINRA Rule 3310(a) and (b) and FINRA Rule 2010 by: a) failing to establish and implement anti-money laundering (AML) policies and procedures adequately tailored to the firm's online business in order to detect and cause the reporting of suspicious activity; and b) failing to establish and implement a reasonably designed customer identification program to adequately verify customer identity.

In a similar instance where FINRA also took enforcement action, a firm opened accounts for a foreign customer from a jurisdiction known for heightened money-laundering risk. In addition to the FINRA case, the SEC, among other entities, later filed a complaint against this customer. The SEC alleged that the customer created an international "pump-and-dump" scheme where shares in thinly traded companies were bought. Then, the customer hacked into accounts at other broker-dealers and liquidated the existing equity positions in those accounts. With the resulting proceeds, the customer bought and sold thousands, and in one case, millions, of shares of the same thinly traded stocks in the original accounts. The unauthorized trading in the hacked accounts pumped up the price of the stocks for the customer, who realized the profits in the accounts at the original firm. The FINRA investigation found this firm failed to establish and implement AML policies and procedures adequately tailored to verify the identity of the firm's higher-risk foreign customer base in order to detect and cause the reporting of suspicious activity.

Governance and Risk Management for Cybersecurity

PRINCIPLES AND EFFECTIVE PRACTICES:

Firms should establish and implement a cybersecurity governance framework that supports informed decision making and escalation within the organization to identify and manage cybersecurity risks. The framework should include defined risk management policies, processes and structures coupled with relevant controls tailored to the nature of the cybersecurity risks the firm faces and the resources the firm has available. Effective practices include:

- defining a governance framework to support decision making based on risk appetite;
- ensuring active senior management, and as appropriate to the firm, board-level engagement with cybersecurity issues;
- identifying frameworks and standards to address cybersecurity;
- using metrics and thresholds to inform governance processes;
- dedicating resources to achieve the desired risk posture; and
- performing cybersecurity risk assessments (discussed in a later section).

Governance Framework

An effective practice for firms is to establish and maintain a governance framework for the management of cybersecurity risks and related controls appropriate to the organization's size, and the nature of its cybersecurity risk exposure. The governance framework should articulate the roles and responsibilities of organizational units and individuals within those units.

As used in this report, "governance" and "governance framework" refer broadly to the establishment of "policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements" in a fashion that is understood within the organization and that informs its management of cybersecurity risk.[2] "Management" refers broadly to the implementation of those governance measures.

The governance framework should enable firms to become aware of relevant cybersecurity risks, estimate their severity and decide how to manage each risk (*i.e.*, to accept, mitigate, transfer or avoid the risk). Most firms' time will be spent on mitigation, which includes the identification, selection, implementation, performance monitoring and updating of the controls firms use in their cybersecurity programs.

Performing these tasks effectively presents a significant governance challenge. Firms need to incorporate multiple views—including from the business, information technology, risk management and internal audit—in conjunction with senior management and board oversight to implement an effective cybersecurity program. Depending on the firm, the business unit or information technology may be responsible for the front-line selection, implementation and monitoring of cybersecurity controls. The risk-management function, on the other hand, may provide standards and objective monitoring of implementation of those controls. Finally, an appropriately independent function—*e.g.*, internal or external audit—can assess the implementation and effectiveness of the firm's cybersecurity program. This can include assessing a firm's cybersecurity controls and processes to determine if they are functioning as expected and to evaluate whether controls are appropriate to the firm's risk appetite.

Board and Senior Management Involvement

Active executive management—and as appropriate to the firm, board-level involvement—is an essential effective practice to address cybersecurity threats. Without that involvement and commitment, a firm is unlikely to achieve its cybersecurity goals.

Boards should play a leadership role in overseeing firms' cybersecurity efforts. In 2014, the National Association of Corporate Directors (NACD) addressed the role of the board on cybersecurity in a publication, *Cyber-Risk Oversight*.[3] In that publication, the NACD—in collaboration with the American International Group and the Internet Security Alliance—cited five cybersecurity principles for boards. The principles state:

- Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
- Directors should understand the legal implication of cyber risks as they relate to their company's specific circumstances.
- Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.
- Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.
- Board and management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate or transfer through insurance, as well as specific plans associated with each approach.[4]

These principles can be a useful reference point for boards grappling with defining their responsibilities and roles in addressing cybersecurity risks.

Observations on Firm Practices

Some firms emphasized the important role the board played in their firm's cybersecurity efforts. At these firms, the board was actively engaged with approving the firm's overall cybersecurity strategy and in monitoring implementation of that strategy. This involvement, firms offered, had a strong positive impact in focusing attention on, and making resources available for, cybersecurity. FINRA underscores the importance of active, board-level involvement in establishing priorities for, and monitoring implementation of, firms' responses to cybersecurity threats.

Board reporting practices varied among the firms FINRA reviewed. At a number of firms, the board receives annual cybersecurity-related reporting while other firms report on a quarterly basis. A number of firms also provide *ad hoc* reporting to the board in the event of major cybersecurity events. Management at some firms reports to the full board, while at others management reports to a board subcommittee, typically audit.

Beyond the benefits of proactive senior management involvement in cybersecurity initiatives, firms should also be aware of the downsides of insufficient involvement. This includes the obvious risk that the firm may be more vulnerable to successful cybersecurity attacks.

Failure to address cybersecurity risks adequately from a governance perspective also increases regulatory risks for firms, for example under Rule 30 of SEC Regulation S-P or SEC Regulation S-ID (the "Red Flags Rule"). A review of FINRA enforcement actions related to cybersecurity reflects frequently found significant governance or management failures. In these instances, firms failed to act on warnings that, if heeded, could have substantially mitigated the loss of customer information. Common deficiencies found in these matters, some of which involved charges against individual executive officers, include:

- failure to safeguard confidential customer information;
- failure to establish an adequate system to protect the firm's data, including inadequate user access restriction, inadequate vendor oversight or supervision of outsourcing arrangements, or inadequate responses to cybersecurity breaches; and
- failure to conduct adequate periodic cybersecurity assessments.

Case Study: Cyber-related Enforcement Action

In one instance where FINRA took enforcement action, hackers used an SQL injection attack[5] on a firm's database server to obtain confidential customer information of more than 200,000 customers, including names, account numbers, Social Security numbers, addresses and dates of birth. The firm stored the data on a computer with an Internet connection and did not encrypt the information. The firm only became aware of the breach when hackers attempted to extort money from the firm. In fact, however, those breaches had been visible on the firm's Web server logs.

The case illustrates governance failures in several respects. Most broadly, the firm failed to implement adequate safeguards to protect customer information. More specifically, the firm stored unencrypted confidential customer data on a database connected to the Internet without effective password protection. Although the firm performed penetration testing, it did not include an asset with sensitive customer information as part of that test. In addition, the firm did not establish procedures to review the Web server logs that would have revealed the theft of data. And, the firm did not respond to an earlier auditor recommendation that it acquire an intrusion detection system. Finally, the firm also failed to have written procedures in place for its information security program designed to protect confidential customer information.

The Role of Frameworks and Standards

An effective practice for firms is to evaluate relevant industry frameworks and standards as reference points in developing their approach to cybersecurity.[6] There are a variety of frameworks and standards firms can draw upon, including:

- National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 (the "NIST Framework" or "Framework");
- NIST, Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53, Revision 4 (there are a number of other NIST documents that address topics related to information and cybersecurity);
- International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Information Technology 27001 and 27002 framework (collectively, ISO 27001/27002);

- ISACA's[7] Control Objectives for Information and Related Technology (COBIT) 5; and
- Payment Card Industry (PCI) Data Security Standard (DSS).

Firms can draw upon the NIST Framework, as well as NIST, ISO and PCI standards that focus on cybersecurity specifically, as well as COBIT 5, which addresses information technology management and governance broadly. The SANS Critical Security Controls for Effective Cyber Defense (referred to subsequently as the "SANS Top 20") offers a more tactical view of 20 cybersecurity risk controls that address some of the most common and significant cybersecurity threats.

The NIST Framework

The NIST Framework has received considerable attention since it was published in February 2014. The Framework has three major parts, the Framework Core, Framework Implementation Tiers and Framework Profiles. (The Framework is described in greater detail in Appendix II.) It provides a thorough, yet flexible risk-based approach for understanding where an organization stands in terms of its cybersecurity activities and where it would like to be to ensure that it is able to achieve its cybersecurity risk management priorities as defined by organizational goals, legal and regulatory requirements, and industry best practices.

This perspective helps reframe cybersecurity issues in risk management terms that may be more understandable for decision-makers, *i.e.*, whether a firm should mitigate, transfer, accept or avoid a risk.

The SANS Top 20

The SANS Top 20 focuses "first on prioritizing security functions that are effective against the latest Advanced Targeted Threats, with a strong emphasis on "What Works" - security controls where products, processes, architectures and services are in use that have demonstrated real world effectiveness."[8] For each control, the Top 20 provides an explanation of why the control is important, discusses how to implement the control, explains procedures and tools that are necessary to make the control effective, and presents implementation, effectiveness and automation metrics.

Observations on Firm Practices

Among the firms that were part of the sweep, nearly 90 percent used one or more of the NIST, ISO or ISACA frameworks or standards. More specifically, 65 percent of the respondents reported that they use the ISO 27001/27002 standard while 25 percent use COBIT. Some firms use combinations of these standards for various parts of their cybersecurity programs. The COBIT standard, for example, is focused more on information technology governance than cybersecurity *per se*. In addition, several firms underscored the utility of the PCI Standard as well as the SANS Top 20. In some cases, firms explicitly mapped their architecture to a framework or standard. In other cases, firms chose specific aspects of different frameworks as a reference point to assess or benchmark the firm's approach.

Firms that use a framework or standard identified a number of benefits in doing so. Most stated that the frameworks and standards provide a tested approach that can help a firm structure its thinking about how to address cybersecurity more clearly, including identifying gaps in a firm's cybersecurity approach and controls to fill those gaps. Some firms use a framework or part of a framework as a reference point for their own approaches while others explicitly map their approaches along one standard or another.

In addition, a number of firms noted that the frameworks and standards can improve communication, both within the firm and with third parties. Their use can help establish a common vocabulary that enhances understanding and precision in communications. Developing this common vocabulary is an iterative learning process that takes time, but which can pay dividends down the road. For example, it can reduce the likelihood of misalignment between risk appetite and controls. Several firms noted that it improved their ability to communicate with the board on cybersecurity issues. That, in turn, led to enhanced support, including funding, for cybersecurity initiatives.

While FINRA does not endorse any particular framework or standard, FINRA expects firms to use frameworks and standards to evaluate whether and how they can improve their approach to cybersecurity, for example through the identification of gaps, or ineffective controls, in the firm's cybersecurity program. FINRA will use its regulatory programs to assess whether and how firms are using frameworks or standards as a component of their cybersecurity programs.

Metrics

Performance measurement is a key aspect of cybersecurity risk management. In this regard, FINRA expects firms to bolster their cybersecurity governance and risk management by:

- developing, implementing, monitoring and updating metrics that provide visibility on the performance of key elements of a firm's cybersecurity program;[9]
- developing and implementing thresholds that define the target level of performance the firm desires to achieve; and
- implementing a governance framework that oversees, and, as necessary, updates the metrics and thresholds on an ongoing basis.

In its *Performance Measurement Guide for Information Security*, NIST states, "(i)nformation security measures are used to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data."[10] The report goes on to note that "(t)he results of an effective information security measurement program can provide useful data for directing the allocation of information security resources and should simplify the preparation of performance-related reports."[11]

NIST describes three broad types of metrics—implementation, effectiveness/efficiency and impact metrics—and presents these in the context of the maturity of an organization's information security program. More mature programs are characterized by more detailed policies, standardized and repeatable processes, and increased data that can be used for performance management. Less mature programs may focus more on implementation metrics.

Observations on Firm Practices

In the sweep, 95 percent of the firms FINRA reviewed use metrics as one of their key cybersecurity performance management tools. However, firms described a wide range of metrics. One firm's response captures the general approach of many of the larger firms FINRA reviewed: the firm uses metrics to measure nearly every aspect of its IT security programs. Detailed dashboards covering patch coverage, vulnerability management, security infrastructure performance (*e.g.*, anti-malware, anti-spam, posture checking), access control management, secure application development, training and awareness, and vendor risk are all tracked and views are provided to both central and distributed IT security teams. By contrast, some of the smaller firms FINRA reviewed described a much more limited use of metrics.

The table below presents examples of some areas in which firms track metrics to assess the performance of their cybersecurity program.

Control	Metric
Cyber Attacks	Distributed Denial of Service (DDoS) Attacks
	Network Intrusions
	Data Theft
Endpoint	Encryption Coverage (portable devices, USBs, email, data transfers)
	Adobe Patch Coverage
	Microsoft Patch Coverage
	Anti-Virus Coverage
Information Security Awareness	Employee Training (new employees and ongoing for existing employees)

For some types of metrics, firms set and manage to thresholds. For example, a firm may set a target that at least 95 percent of computers on the firm's network be up-to-date (defined as less than 90 days old) on Microsoft and Adobe patches. In situations where that threshold is not met, the firm would escalate the matter for review and resolution.

Several firms indicated that developing and implementing effective metrics can be challenging as was borne out in a recent study by the Ponemon Institute. That study found that while 75 percent of U.S. respondents said metrics were either "important" or "very important," more than half said that their firms' existing metrics were either not aligned with business objectives or the respondent was unsure whether they were aligned. Further, half of the U.S. IT professionals rated themselves as "not effective" in communicating all relevant facts about the state of security risk to senior executives.[12]

The discussion of metrics is directly tied to governance as metrics feed into firm's decision-making and, themselves, require a governance structure. Decisions about which metrics to track, thresholds against which metrics are assessed, the entities in an organization to which they are reported, the organizational units that are charged with decision making on those metrics, and the content of decisions all are essential governance functions.

The firms FINRA reviewed took a variety of approaches with larger firms typically having more formally defined policies and processes for their use of metrics. This included formal escalation procedures to senior information technology, risk or business personnel when performance metrics did not fall within the established thresholds. In addition, these same firms typically established formalized governance processes around the creation and ongoing monitoring of the usefulness and relevance of metrics and related thresholds.

FINRA underscores the importance of metrics as a critical cybersecurity management tool. FINRA is concerned that management at some firms made only limited use of metrics. This limits management's insight on the performance of the firm's cybersecurity program and its vulnerabilities and may be symptomatic of a weak approach to cybersecurity.

Cybersecurity Risk Assessment

PRINCIPLES AND EFFECTIVE PRACTICES:

Firms should conduct regular assessments to identify cybersecurity risks associated with firm assets and vendors and prioritize their remediation. Effective practices include establishing and implementing governance frameworks to:

- identify and maintain an inventory of assets authorized to access the firm's network and, as a subset thereof, critical assets[13] that should be accorded prioritized protection; and
- conduct comprehensive risk assessments that include:
  - an assessment of external and internal threats and asset vulnerabilities; and
  - prioritized and time-bound recommendations to remediate identified risks.

A cybersecurity risk assessment is a systematic process firms complete to identify and analyze potential dangers or risks to a firm's business that could arise through its information technology systems.[14] In the case of broker-dealers, such risks could include the compromise of customer or firm confidential information, the misuse of customer funds or securities resulting in potential financial losses for the firm or its clients, and the theft of proprietary trading algorithms, as well as adverse reputational impacts for the firm.

Asset Inventories and Critical Assets

Asset inventories are a key component of a risk assessment. In order to assess risks, firms need to know what assets they have, what assets are authorized to be on their network and what assets are most important to protect. Both the NIST Framework and SANS Top 20 identify inventories as foundational activities, and the NIST Framework also underscores the importance of identifying critical assets.[15]

Firms may use a variety of criteria to define critical assets. An effective asset inventory process will define measures of importance and capture this information for their assets. For broker-dealers, one consideration in identifying critical assets is firms' obligations under Regulation S-P to protect customers' personally identifiable information (PII). Therefore, databases containing personal client data and business applications containing this data would normally be considered critical assets. In addition, firms may establish a variety of other criteria to prioritize assets, for example, their importance to the firm's business operations (such as trading systems), whether clients or others have online access to initiate transactions, whether there is an impact to order routing such as order management systems, whether the asset could allow client statements to be altered, whether the asset allows for delivery of securities or cash—*e.g.*, wire transfers—and whether the asset is designed to fill a critical regulatory need.

Observations on Firm Practices

The firms FINRA reviewed described a range of approaches to developing and maintaining their asset inventories. Here we present observations on those practices. Generally, the asset inventory process involves a combination of business line and centralized risk assessment staff. Some firms begin the inventory development process with the business units completing a questionnaire in which they identify all assets in the business unit. Alternatively, a firm may set a criticality or risk threshold and ask the business unit to identify assets that meet or exceed that threshold. In other cases, a centralized team provides a list of assets that the business unit validates.

Many firms stated they maintain strong policies to ensure that all assets are subject to centralized review and control. An example of this would be those firms where business units may develop or acquire their own software. These firms typically establish policies requiring all applications go through a centralized control process before moving into production as part of the system development life cycle.

Establishing and Maintaining a Risk Assessment Program

Through risk assessments "(t)he organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals."[16] FINRA views the risk assessment process as a key driver in a firm's risk management-based cybersecurity program. It is also a potentially useful starting point for firms embarking on the establishment of a cybersecurity program. The NIST Framework, for example, identifies six sets of risk assessment activities or outcomes:

- identify and document asset vulnerabilities;
- review threat and vulnerability information from information sharing forums and sources;
- identify and document internal and external threats;
- identify potential business impacts and likelihoods;
- use threats, vulnerabilities, likelihoods and impacts to determine risk; and
- identify and prioritize risk responses.[17]

Ultimately, the risk assessment process should lead to changes in a firm's controls to remediate identified risks. The controls can take several forms:

- **Preventive**—these are controls to stop or prevent harm from taking place in the first place; these include, for example, anti-malware, anti-virus software and privilege management tools.
- **Detective**—these are controls a firm uses to identify potential threats that may have occurred, for example, through the detection of data leakage or email content analysis.
- **Corrective**—these are controls that restore a system or process back to the state prior to the detrimental occurrence, for example, a business recovery process that could restore a system to its original state after a system outage.
- **Event predictive**—these are controls that would predict a detrimental event happening, such as notification that a specific type of hack has been occurring at similar firms.

Examples of areas in which a firm may add or make changes to its controls to reduce cyber threat exposure include:

- Data storage at vendors
- Employee training
- Data encryption
- Employee access control
- Patch and software updates
- Privilege management
- WiFi protection
- Email content filtering
- Customer access control
- Hand-held device protection
- Vendor access control
- Web/URL filtering
- Staff skillset matching
- Vendor access controls
- Software development life cycle processes

Observations on Firm Practices

In the sweep, over 80 percent of firms had established cybersecurity risk assessment programs. Among these firms, a number draw on the COBIT 5 and ISO/IEC 27001 frameworks and some also map their risk domains to the Federal Financial Institutions Examination Council (FFIEC) handbook. FINRA is concerned that the remaining firms either had no program in place or were only in the nascent stages of establishing a program.

FINRA observed firms taking a variety of approaches to risk assessments. All firms viewed risk assessment as part of a broader, ongoing risk management process and the assessment itself was usually risk based, *i.e.*, firms devoted greater resources and attention to more important or critical assets. Those firms with defined risk assessment processes conduct them on either an annual or ongoing basis throughout the year, but culminating in an annual risk assessment report or summary. Firms frequently supplemented the regular risk assessment process with *ad hoc* assessments when they identified new data assets or systems through their system development lifecycle process or where they identified new risks or threats.

Assessing Threats and Vulnerabilities

Firms use a variety of inputs into their risk assessment process. With respect to threats, these inputs include past cybersecurity incidents either at the firm or noted in the industry, threat intelligence identified from other organizations or through security organizations such as the Financial Services Information Sharing and Analysis Center (FS-ISAC). These threats can include both internal threats—*e.g.*, threats from employees—or external threats, such as hacktivists or organized crime groups.

Another important component of the risk assessment process is vulnerability analysis—the process of identifying, quantifying and prioritizing potential vulnerabilities within a system. The sophistication of vulnerability analysis varied across firms. One commonly used approach is the Common Vulnerability Scoring System (CVSS) to assess vulnerabilities in applications. CVSS is an industry open standard for assessing the severity of vulnerabilities and prioritizing their remediation. The results of these reviews are used as inputs to the firm's risk assessment program and would drive risk ratings of various critical assets.

Firms' approaches to integrating threats and vulnerabilities to produce an overall risk assessment also differed. For example, some developed proprietary risk assessment methodologies while others used vendor products tailored to the firm's needs. It was common for firms to classify risks on a simple scale such as critical, high, medium or low.

These ratings feed into the governance process described earlier and play a key role in driving firms' risk remediation efforts. Typically, ratings of critical or high risk require remediation or approval through a risk acceptance process. One challenge noted in this process is maintaining visibility on assets that evolve from low to high risk. This may occur, for example, if an application is not updated, if new functionality is added or if it handles new types of data.

Risk Assessment Governance

While there were differences across the larger firms FINRA reviewed, the following discussion is representative of these firms' organizational approach to risk assessment. Firms begin by using business unit level risk teams to perform risk and control assessments across their technology assets. At the corporate level, a technology risk evaluation function performs technical risk assessments of assets with a focus on top risks, including cybersecurity. This function also partners with the business units throughout the year to support the technical reviews of the business unit's most critical functions. The output from this process is reported, tracked and remediated through the firm's enterprise risk management tracking system.

Firms affiliated with other financial organizations—typically a bank or bank holding company—conduct both the firm risk and cybersecurity risk assessments at an enterprise level, *i.e.*, involving but not limited to the broker-dealer and the process was driven and managed by in-house staff.

By contrast, some smaller firms that were at an earlier stage of maturity in their cybersecurity program stated that they did not have the in-house expertise to implement risk assessments and, for that reason, outsourced the process to a vendor.

Regardless of a firm's ability to perform a risk assessment, FINRA notes that what is important from an effective practice perspective is that firms have defined escalation processes to address risks identified as not appropriately mitigated. Typically, the more significant the risk, the higher the level of management approval required to accept that risk. Some noted that a decision to accept a risk at a higher level than the firm would like was typically time-bound, meaning, the firm puts in place a mitigation plan and deadline to reduce the risk. All firms indicated that high or critical risks dealing with customer PII or critical firm information without adequate mitigation controls were unacceptable.

In the context of the enforcement case cited earlier, a database containing unencrypted confidential customer information without effective password protection and exposed to the Internet would be considered a critical risk. A risk assessment process coupled with the escalation procedures could have identified the firm's exposure before the firm's data was stolen.

Technical Controls

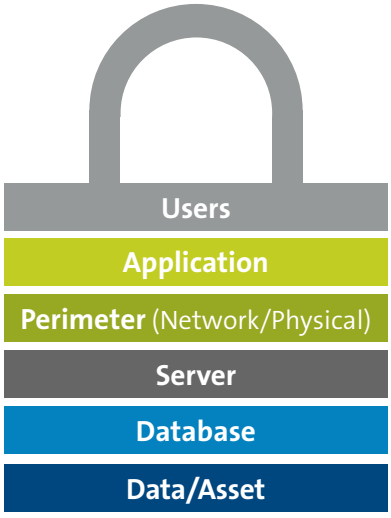
PRINCIPLES AND EFFECTIVE PRACTICES:

Firms should implement technical controls to protect firm software and hardware that stores and processes data, as well as the data itself. Effective practices include:

- implementing a defense-in-depth strategy;
- selecting controls appropriate to the firm's technology and threat environment, for example:
  - identity and access management;
  - data encryption; and
  - penetration testing.

The three areas cited here are illustrative of possible control areas.

The selection of specific controls is highly dependent on an individual firm's circumstances. An itemization of all possible cybersecurity controls, or the recommendation of a specific control selection methodology, is outside the scope of this document. Nonetheless, given recent cybersecurity events affecting firms, there is value in highlighting a general approach to cybersecurity controls that firms have found effective as well as a few, illustrative, critical cybersecurity practices.



Defense-in-depth

Many organizations apply a defense-in-depth strategy. Under such a strategy, organizations layer multiple independent security controls strategically throughout their information technology systems. A successful defense-in-depth strategy is based upon the selection and effective implementation of cybersecurity practices and controls consistent with a firm's risk profile. Defense-in-depth strategies are promoted by organizations such as the National Security Agency and Open Web Application Security Project (OWASP).

Firms can conceptualize defense-in-depth from a variety of non-mutually exclusive perspectives. For example, one perspective is to view the components of a firm's technical infrastructure as residing in layers, and then to apply security control points at each layer. A basic decomposition might view the technical environment as having the following layers: applications, perimeter, server, databases and the data itself (*see* illustration).

The Cyber Kill Chain (reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives)—or similar models—provides another perspective for conceptualizing a defense-in-depth strategy.

By viewing the defense-in-depth challenge from multiple perspectives—such as those described above—firms may gain deeper insight into the controls that can maximize the strategy's effectiveness.

The list of candidate controls can be extensive. These practices are itemized and categorized in a variety of ways, through standards such as ISO 27002 and NIST SP 800-53, as well as by industry organizations such as SANS. The recently published NIST Framework also provides useful guidance in the selection of controls commensurate with a firm's risk appetite.

The success of a defense-in-depth strategy depends both on the overall architecture of the firm's controls and the effectiveness of individual controls used. Given the increasingly sophisticated nature of cybersecurity threats, firms need to continually identify and remediate potential weaknesses in both areas. For example, some attacks may involve custom malware which would not be detectable by traditional anti-virus programs. Other attacks may hijack an application or process in a way that is not detectable through traditional security measures. Participation in information sharing organizations can help firms become aware of new potential threats to their systems, learn how other firms are addressing those threats and discuss overall approaches to cybersecurity.

In the sections that follow, FINRA discusses effective controls in three areas: identity and access management, encryption and penetration tests.

Identity and Access Management (IAM)

Establishing appropriate controls to limit users' access to a firm's systems and data—identity and access management—is one of the important challenges that systems operators face. There are many aspects to this challenge, including establishing, appropriately limiting and terminating access when no longer needed. This applies to external parties—both customers and vendors—and internal parties. The increasing use of mobile devices by both customers and employees adds to this challenge—by creating multiple new devices whose system access must be managed carefully.

Within access management, one of the areas in which FINRA has noted problems at firms is insiders gaining unauthorized access to firm systems and information. This can arise by employees:

- being granted inappropriate access upon hiring;
- being allowed to carryover or accumulate privileges as they move from job to job within a company;
- being allowed to expand their access without a compelling business need for that access; or
- having their credentials stolen and misused.

In addition, insider problems can arise if user-facing applications are granted excessive permissions for back-end systems, such as databases. Controls limiting the access that a user-facing system has to a back-end system form an additional control layer behind other controls that might be implemented in the user-facing application. These back-end system credentials should also follow a policy of least privilege (see below). This is an example of defense-in-depth. In the event that an insider finds a vulnerability in a user-facing system, applying a policy-of-least-privilege to this back-end system account will limit the impact. As a specific example, if a user-facing application does not have requirements related to sensitive fields in a database table, the back-end system account should be explicitly prohibited from accessing those fields.

Three important principles should underlie policies, processes and technical measures that, together, establish effective access management controls across a user's lifecycle: Policy of Least Privilege, Separation of Duties and Entitlement Transparency.

- Policy of Least Privilege (POLP) is the concept that the minimum entitlements necessary to accomplish a business objective should be granted to any one individual.

- Separation of Duties (SoD) is the concept that actions affecting sensitive assets should require the collaboration of multiple independent roles to succeed. Independence is essential to making implementation of SoD effective. If separation of duties is based on roles that can influence one another, the value of the practice is significantly diminished.

  Separation of Duties can take many forms. A preventive process control might require that the initiation of a sensitive action by a member of one role receive the express approval of an individual from an independent approver role before that action is executed. A detective process control might alert a member of an independent review role upon the execution of a sensitive action by an individual in an initiator role, enabling that reviewer to investigate and address any potential misuse. A simplistic example of separation of duties in the context of IAM is that an individual should not be able to request and approve access to PII.

- Entitlement Transparency is the concept that it should be easy to know who has access to what at all times.

Below, FINRA highlights selected measures that are important for firms to consider in establishing and maintaining an IAM program.

Authorization Scheme

The foundation of a strong IAM program is an authorization scheme that implements the three key principles discussed above. To that end, firms should consider incorporating the following measures in their IAM programs:

- **Centrally controlled role-based entitlements**
  If entitlements are allowed to be granted in a dispersed manner, other controls such as those enforcing separation of duties or monitoring for and terminating unneeded entitlements can become substantially more complex and expensive. Authorization responsibilities can be delegated; however, the underlying entitlement scheme should be organized and centrally controlled. If entitlements are granted independently to operating systems, applications, database or utilities, it is extremely difficult to maintain a full inventory of possible entitlement sources and therefore extremely difficult to confirm that all granted entitlements are subject to review.

- **Baseline entitlements tied to organizational roles**
  Firms should consider maximizing the use of role-based entitlements in their authorization schemes. Staff access requirements are typically associated with their role in the organization. Supplementary entitlements may also apply based on specific project assignments, but wherever possible, basing entitlements on the properties of an individual (*e.g.*, Human Resources (HR)-assigned position or department) pays dividends in terms of ensuring consistency across the organization, minimizing opportunities for entitlement accretion as individuals move between roles and departments, and dramatically simplifying the jobs of designing and enforcing appropriate separation of duties.

- **Entitlements of each role reviewed to ensure adherence to POLP**
  Firms should review the business justification for each entitlement granted and requirements for access to sensitive information should be challenged. Business necessity rather than convenience should drive access to sensitive data and systems. Prior to granting access to such data or systems, firms should consider whether a modification to an underlying business process could enable the business objective to be achieved without exposing sensitive data to that role.

- **Entitlements of roles individually and collectively reviewed to ensure appropriate Separation of Duties and Defense-in-Depth**

  Firms should compartmentalize sensitive data and processes to the degree possible. The broader a single role's access, the greater the negative impact to the firm should that role's access be misused or abused (whether by accident, malicious intent of the entitled individual, or theft of credentials by another insider.) Here again, firms should consider whether modification of an underlying business process could help facilitate improved compartmentalization.

  Firms should ensure that for each role with access to sensitive data there is at least one other control[18] that prevents (or at a minimum detects) misuse or abuse of that entitlement. Any entitlements related to that other control must not be granted to the former control. For example, entitlements to start, stop or alter logs must not be granted to a role that also uses those logs as a means to monitor the actions of members of that role.

Provisioning

For all but the simplest environments, automation may be necessary to achieve the objectives of a secure IAM solution. Automation supports the risk analysis necessary to ensure POLP and SoD. In firms that have tied baseline entitlements to organizational roles, automation enables entitlements to be provisioned automatically. It is important to ensure that those entitlements are updated if an individual changes positions or departments within the organization. Automation also helps detect SoD violations, such as assigning an individual to both requestor and approver roles.

Use Monitoring

Firms should establish controls to detect misuse of sensitive entitlements. For example, there may be nothing unusual about a member of a properly entitled role accessing the confidential records of a customer; however, a member of that role accessing 10,000 customer records within a one-hour period may indeed be unusual. Firms should seek to define business rules that differentiate between normal and abnormal use of sensitive entitlements and to create monitoring controls to rapidly detect and investigate abnormal behavior.

Entitlement Maintenance/Access Reviews

Firms should establish triggers for updating entitlements. For example, it may be possible to establish an HR process that reminds managers to review entitlements in the event that an individual's title or department changes. In a more advanced model, the entitlement would be updated automatically based on the authorization scheme.

Regardless of the degree of automation, it is imperative that firms perform regular access reviews and that these reviews are thorough. It is not sufficient simply to ask managers to perform this review. There should be a mechanism for providing the reviewer with an inventory of roles to which a user is assigned (or an inventory of specific entitlements where role-based entitlement is not in use). The reviewer should then be required to state explicitly whether a role assignment or entitlement should be retained or terminated. Those entitlements flagged for termination should be tracked to completion. It may also be prudent to audit these access reviews, perhaps by sampling, to confirm that the access review process is effective. Firms should consider the importance of training reviewers in the principles of POLP and SoD, as well as the importance of holding reviewers accountable for performing thorough reviews. The principle of separation of duties applies of course: An entitlement reviewer should not be permitted to certify his or her own entitlements.

Terminating Access

Firms should establish mechanisms that promptly terminate employee access to systems and information to which they no longer require access. If automation is not available, policies and procedures should be in place associated with entitlement maintenance and access reviews to ensure that role assignments and entitlements identified as no longer needed are terminated in a timely manner.

In the event that a user account is terminated in its entirety, some firms establish two tiers of access termination for departing employees: end-of-day termination for employees departing in good standing and immediate termination for employees terminated for cause.

Cloud and Other Third-party Services

If a firm uses cloud services, it is important that all of these IAM concepts be applied there as well. Firms may consider implementing a single-sign-on (SSO) solution that enables the firm's IAM processes and tools used for in-house resources to be applied to cloud-based resources as well. Commercial products are available that may meet firm needs in this area. This approach will help ensure that a firm's analysis of POLP and SoD, the effectiveness of a firm's access review, and other IAM processes are not adversely affected by a firm's IAM processes being segmented into "internal" and cloud domains.

Encryption

Encryption is a critically important effective practice in a firm's cybersecurity control arsenal. Encryption provides the obvious benefit of protecting the confidentiality of data by ensuring that only approved users (users who hold the decryption key) can view the data. Less obvious benefits include providing a means for ensuring information integrity (if the encrypted data cannot be read, it cannot be meaningfully altered), and non-repudiation (if a message is encrypted with a key only held by that source, the source cannot disclaim having sent that message). Depending on how it is applied, encryption can also be used to facilitate a strong Separation of Duties policy by limiting key access to staff members with a business-defined need to access the protected information.

In some sense, encryption can be seen as the last line of defense in a defense-in-depth strategy. Encryption is a control applied to the data itself. If all of the higher-layer controls fail resulting in exposure of data, encryption can protect that data from being read or altered.

While encryption is a control ultimately applied to data, the control can be implemented at multiple levels of a defense-in-depth strategy with various security benefits and operational tradeoffs occurring at each layer. The application of encryption should be considered with respect to both workstations and servers, in both at-rest and in-transit capacities, and at various technology layers from storage medium up through the application layer.

Data At-rest (Stored Data)

Data is stored in many places within an organization, including file servers, on workstations and on portable media such as thumb drives. An effective practice is to encrypt this data at-rest.

Firms should have a strategy in place for ensuring that portable media, including but not limited to USB drives, backup tapes, and the drives of portable end-user terminals such as laptops, are encrypted. There are many examples of organizations losing sensitive data through the loss of portable media and computing devices. It is a widely accepted best practice that these devices should be subject to encryption, as they are at much higher risk of loss and theft than fixed storage media devices located in offices and data centers.

In addition, firms should encrypt data stored within formal systems. To this end, firms will need to consider options and relative benefits of applying encryption at various levels of the firm's technology systems. (Appendix III discusses information rights management, encryption algorithm and key selection.)

Placing sensitive data in a cloud service carries the same risks as data stored in private systems, and firms need to address the risk of disclosure to cloud service provider insiders. A guiding principle is to encrypt all sensitive data before placing it in the cloud, using encryption that the firm controls and that is never disclosed to the cloud service provider. Any decision to deviate from this guiding principle should be done based on a thorough third-party risk analysis of the cloud service provider and with the informed risk acknowledgement of relevant stakeholders.

Data In-transit

An effective practice is to encrypt sensitive data transmitted over untrusted networks. Untrusted networks include the Internet as well as any network where the firm does not operate and control physical and logical access to the communication devices and transmission lines. It may be necessary to consider in-transit encryption between a client and a server, between two servers, between two networks, or between virtual elements within a general purpose cloud solution. In the end, each organization must determine whether a given network is considered trustworthy. While the in-transit encryption solution most commonly used in data telecommunications is Transport Layer Security—the protocol used by all modern Web browsers to make encrypted connections to Web users using a URL starting with "https"—there are other in-transit encryption solutions readily available to firms.

Third-party Penetration Testing

Penetration Testing (also known as "Pen Testing") is an effective practice that simulates a real-world attack against a firm's computer systems. The goal of a third-party penetration test is to get an attacker's perspective on security weaknesses that a firm's technology systems may exhibit.

Penetration tests are valuable for several reasons:

- determining the feasibility of a particular set of attack vectors;
- identifying higher-risk vulnerabilities that result from a combination of lower-risk vulnerabilities exploited in a particular sequence;
- identifying vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software;
- assessing the magnitude of potential business and operational impacts of successful attacks;
- testing the ability of network defenders to successfully detect and respond to the attack; and
- providing evidence to support increased investments in security personnel and technology.

Penetration Tests can take different forms depending on a firm's specific objectives for the test. Each of these contributes in its own way to an overall defense-in-depth strategy.

Broad vs. Targeted

Penetration testing may be scoped to encompass all accessible systems, or may be scoped to target a specific system or application. In the former case, it is common to provide the tester with little more than a range of IP addresses. In the latter case, URLs and an appropriate set of application credentials may be provided, along with guidance on how to exercise the functionality of the application. There are cost and risk tradeoffs to be made in balancing the depth and breadth of the work.[19]

Find vs. Exploit

Testing can be limited to finding apparent vulnerabilities, or can include the demonstrated exploitation of vulnerabilities to achieve a particular security objective (*e.g.*, obtain sensitive data). The additional work and expense of demonstrated exploitation testing may uncover compensating controls that mitigate the risk of the detected vulnerability. It may also provide hard evidence necessary to justify remediation costs of the identified vulnerability.

Production vs. Non-production

Testing against production systems is ideal from a security perspective as it leaves no question as to whether production controls are consistent with an alternate testing environment. As even testing designed to be non-destructive can potentially alter the state of a production environment, it may be necessary to perform testing with the system offline and to provide a facility for capturing the production state prior to the test and restoring after the test.

External vs. Internal

External penetration testing is designed to test a firm's systems as they are exposed to the outside world (typically via the Internet) while internal penetration testing is designed to test a firm's systems' resilience to the insider threat. An advanced persistent attack may involve an outsider gaining a progressively greater foothold in a firm's environment, effectively becoming an insider in the process. For this reason, it is important to perform penetration testing against both external and internal interfaces and systems.

"Blackbox" vs. "Glassbox"

A blackbox, or zero-knowledge test, is one where the tester is given very little information. They are simulating a hacker who knows very little about a firm's environment and who essentially has to learn as they go. In this case, strong anti-reconnaissance controls can be of great value in thwarting an attack. The tester is essentially given a black box and has to figure out how it works (and therefore how to break it) on his or her own. A glassbox test, on the other hand, is one where the tester is made knowledgeable about how the box works. The tester can see into the box, understand the mechanisms, and, therefore, can more effectively design an attack that may be successful. This test more closely simulates an insider attack. The glassbox test is also better able to evaluate more controls at deeper layers of a firm's defense-in-depth model. In the blackbox model, strong controls at the first layer may prevent the tester from ever exercising lower-layer controls. A thorough approach to penetration testing may include both test models, starting with a blackbox test followed by additional glassbox testing.

Secret vs. Open

In a secret test, a very small number of a firm's personnel are made aware of the test. This makes it possible to test the organization's detective controls (*e.g.*, monitoring/alerting) and possibly incident response and corrective controls to confirm that they are working as designed. An open test is done with full knowledge of all system stakeholders, and is focused on testing the system's preventative controls.

Incident Response Planning

PRINCIPLES AND EFFECTIVE PRACTICES:

Firms should establish policies and procedures, as well as roles and responsibilities for escalating and responding to cybersecurity incidents. Effective practices for incident response include:

- preparation of incident responses for those types of incidents to which the firm is most likely to be subject, *e.g.*, loss of customer PII, data corruption, DDoS attack, network intrusion, customer account intrusion or malware infection;
- incorporation of current threat intelligence to identify the most common incident types and attack vectors;
- containment and mitigation strategies for multiple incident types;
- eradication and recovery plans for systems and data;
- investigation and damage assessment processes;
- preparation of communication/notification plans for outreach to relevant stakeholders, *e.g.*, customers, regulators, law enforcement, intelligence agencies, industry information-sharing bodies;
- involvement in industrywide, and firm-specific simulation exercises as appropriate to the role and scale of a firm's business; and
- implementation of measures to maintain client confidence, including:
  - provision of credit monitoring for individuals whose personal information has been compromised; and
  - reimbursement to customers for financial losses incurred.

The primary objective of an incident response plan is to provide a framework to manage a cybersecurity event or incident in a way that limits damage, increases the confidence of external stakeholders, and reduces recovery time and costs.[20]

Many firms have established a dedicated Computer Security Incident Response Team (CSIRT). For smaller firms, contracting with a vendor may be the most effective method to provide incident response capability. Incident handling requires specialized knowledge and experience in several technical areas. The breadth and depth of knowledge required varies based on the severity of the organization's risks. Outsourcers may possess deeper knowledge of intrusion detection, forensics, vulnerabilities, exploits and other aspects of security than employees of the organization. Also, managed security service providers may be able to correlate events among customers so that they can identify new threats more quickly than any individual customer could.[21]

A firm's incident response plan should address different attack scenarios, since incidents can occur along many different attack vectors. While it is not feasible to develop step-by-step instructions for every imaginable incident, firms should at least have prepared response plans for the most common attacks[22] to which the firm may be subjected. Based on information firms provided to FINRA, common events at broker-dealers include DDoS attacks, malware infections, insider threats and cyber-enabled fraudulent wire transfers.

Containment and Mitigation

Containment is important to prevent an incident from continuing to inflict damage or overwhelming a firm's resources.[23] Containment and mitigation strategies will differ depending on the type of incident. The strategy to contain a malware infection will be different than the strategy to contain a network intrusion. An essential part of containment is decision making, *e.g.*, whether to shut down a system, disconnect it from a network or disable certain functions. Such decisions can be made quickly and effectively if there are predetermined strategies and procedures for containing the incident.[24] In a FINRA enforcement matter, one factor cited in the settlement was a firm's failure to rapidly remediate a device the firm knew was exposing customer information to unauthorized users. Established procedures could have led the firm to address this situation more rapidly.

Eradication and Recovery

After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected assets within the organization so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery.[25]

In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and remediate vulnerabilities to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords and tightening network perimeter security. Higher levels of system logging or network monitoring are often part of the recovery process. Once a resource is successfully attacked, it is often attacked again, or other resources within the organization are attacked in a similar manner.[26]

Investigation

When a cybersecurity incident occurs, firms are expected to conduct a timely investigation of the incident to determine the extent of data or monetary loss and identify root causes. To be prepared for an effective investigation, firms should identify all log information to be recorded and maintained and develop a log retention policy. Some firms, in an effort to reduce costs, do not save log information, and the absence of this information can impede investigations. Firms that do not have the expertise in-house to conduct a complete and thorough investigation should identify a third-party vendor or contractor with incident response expertise that can perform this function when incidents occur. The failure to conduct an adequate investigation of a breach has been a contributing factor to an enforcement action.

Notification

The incident response plan should identify the parties to be notified, as well as what information should be reported and when. Firms may have notification obligations pursuant to, for example, Regulation S-ID, state reporting requirements and FINRA rules. Identifying the varying requirements in the response plan will aid a firm's ability to provide notifications in a full, accurate and timely fashion.

FINRA reminds firms of their reporting obligations under FINRA Rule 4530(b) and also urges firms to report material cyber incidents that do not trigger a reporting obligation to their regulatory coordinator.[27] In the event firms provide information to customers about cyber incidents, the information must be accurate and not misleading.

Making Clients Whole

Incidents where clients lose money or have their PII compromised can lead to loss of investor confidence in broker-dealers. To help address this, firms should:

- provide free credit monitoring services to customers whose information has been compromised; and
- reimburse clients who have lost money through direct attacks—*e.g.*, through an account takeover—or through a cyber-enabled attack, such as a phishing attack that leads to a fraudulent wire transfer.

The following example of one firm's response to a cyberattack draws on several areas of the effective practices discussed above. First, the firm established a dedicated hotline to respond to client needs and questions related to the attack. Second, the firm provided registered representatives with individualized lists of their affected clients to enable them to personally contact each client as a supplement to the firm's general outreach. Third, the firm provided clients personal fraud monitoring service from an outside provider. Through this approach, the firm helped repair some of the reputational damage caused by the attack.

Case Study: Incident Response Plan

One firm reviewed has a dedicated Computer Security Incident Response Team. One of the team's first steps in developing the firm's incident response plans was to determine the most likely types of incidents to which the firm would need to respond. The firm then established a leader for the incident response process and an internal leader for each type of incident as well. The incident response process also includes management personnel (*e.g.*, representatives from Legal & Compliance, Human Resources, Corporate Communication (internal and external) and IT) to assist in the response effort. In addition, the CSIRT identified the role of each party and the workflow of the response steps. Involved parties include outside sources such as forensic experts, outside counsel and vendors that would handle call center and credit monitoring functions, if necessary.

In developing its incident response plan, the firm furthered its understanding of the requirements for data preservation to allow for thorough forensic analysis; established a baseline for "normal" activity so that legitimate issues can be differentiated from false positives; and identified useful external resources.

The firm's overall incident response plan includes run books that address specific types of incidents, such as denial of service attacks, data leakage, malware discovery and social engineering events.

In conjunction with an outside contractor, the firm conducts at least two table-top exercises per year to test the effectiveness of its overall plan and run books. The table-top exercises involve various hypothetical scenarios and going through all the steps documented in each run book with the responsible parties. This helps the firm identify any gaps in its plans and also serves as a training tool. The firm updates its plans on an ongoing basis to incorporate lessons learned from table-top exercises, as well as identified new threats.

Vendor Management

PRINCIPLES AND EFFECTIVE PRACTICES:

Firms should manage cybersecurity risk that can arise across the lifecycle of vendor relationships using a risk-based approach to vendor management. Effective practices to manage vendor risk include:

- performing pre-contract due diligence on prospective service providers;
- establishing contractual terms appropriate to the sensitivity of information and systems to which the vendor may have access and which govern both the ongoing relationship with the vendor and the vendor's obligations after the relationship ends;
- performing ongoing due diligence on existing vendors;
- including vendor relationships and outsourced systems as part of the firm's ongoing risk assessment process;
- establishing and implementing procedures to terminate vendor access to firm systems immediately upon contract termination; and
- establishing, maintaining and monitoring vendor entitlements so as to align with firm risk appetite and information security standards (*see* "Technical Controls" section).

Firms across many industry sectors rely on third-party vendors for a range of services. As recent incidents have shown, these same vendors can also be a significant source of cybersecurity risk. These risks can arise in different ways, for example, if a vendor or one of its employees misuses firm data or systems, if the vendor itself is subject to a cyberattack that compromises vendor systems or firm data, or if an attack on a vendor becomes a vector for an attack on a firm's systems. Firms need an effective vendor management program in place to help guard against these risks.[28]

Due Diligence on Prospective Vendors

Risk-based due diligence on a prospective vendor's cybersecurity practices is a critical first step in selecting third-party service providers. This due diligence provides a basis for the firm to evaluate whether the prospective vendor's cybersecurity measures meet the firm's cybersecurity standards. This can include discussions about the controls a vendor would need to implement to remediate a weakness relative to the firm's cybersecurity standards. As a general principle, firms should avoid using vendors whose security standards do not at least meet those of the firm in the relevant area of activity.

Specific controls many firms expect a vendor to have in place, depending on the risk level of the information to which the vendor has access, could include:

- limits on data access by vendor employees;
- virus protection;
- encryption of data while at rest or in transit;
- controls in place concerning subcontractors;
- system patch management;
- ethical hacking of online systems;
- change management processes;
- program coding methodologies; and
- business recovery practices.

Observations on Firm Practices

Firms with a more mature vendor management process have established processes for due diligence for prospective vendors that demonstrate many of the effective practices highlighted above. The teams executing the selection process include business unit partners, legal, IT and risk management, as well as the firm's information security team and compliance/privacy teams where critical customer or firm information could be at risk. Depending on the firm, the entire vendor management team or a subset thereof would be responsible for assessing the controls put in place by vendors to protect the firm's information (including customer information), whether stored within vendor systems or while being accessed by vendor employees.

During the initial or ongoing vendor management process, situations may arise where a firm's vendor review team may propose changes to a vendor's controls and these proposals are not accepted by the business or vendor, for example if they prove technically infeasible or costly. The issue would typically be raised to a firm's risk management group to determine how to proceed. Outcomes might include a decision to accept the risk, to work with the vendor to mitigate the risk over an agreed time line or to terminate the vendor relationship. In many cases, the exception approval process required that more senior members or bodies within a firm sign off on more significant risk exposure.

Many firms calibrate the level of due diligence they perform based on the level of risk the vendor relationship may create, and this is also an effective practice. For example, for a lower-risk relationship, firms may send control questionnaires to vendors for completion; for a higher-risk relationship, firms may review third-party examination reports, such as SSAE 16 reports; and for high-risk relationships, firms may conduct on-site security reviews. The results of these tests assist the firm in evaluating the adequacy of the vendor's system of controls.

Case Study: Vendor Due Diligence and Contracting

At one firm, the Purchasing department leads the vendor selection process with a steering committee, including members from six due diligence teams (Technical Architecture, IT Control Risk Assessment, Financial, Legal, Compliance and Business Continuity Management). Purchasing uses a governance, risk and compliance software platform to help the firm manage, monitor and mitigate vendor risk, including the vendor launch and utilization processes. To get a vendor approved, a business unit must submit a purchase request form to Purchasing to initiate the process (*e.g.*, contract, request for proposal, request for information). The form includes 20 to 30 questions that help Purchasing decide the level of inherent risk and which due diligence teams should be involved in vetting the potential vendors.

When the IT Control Risk Assessment team is involved, it uses questionnaires focused on the type of data or potential risk involved in the vendor process. These questionnaires are sent to each potential vendor for completion. Where customer PII would be sent off-site or a cloud vendor is involved with PII, the firm uses the most detailed list of questions. In addition, where customer PII or other highly sensitive data is involved, an independent attestation is required, such as an SSAE 16/SOC 2 audit or ISOC 27002 certification. The IT Control Risk Assessment team scores firm responses from 0 (low risk) to 100 (high risk). Should the business desire to accept a vendor with a residual high-risk score, approval from a senior vice president would be required to accept the vendor and would be reported to the Enterprise Risk Management group. Any cloud vendor where PII or human resources data is involved would also be automatically classified as a high-risk vendor.

continued

The Legal team, working with all due diligence teams, is the custodian of contract language requirements and has standardized contract wording based on the type of engagement. All contracts include standardized language for 28 identified areas, including controls, the right to audit, confidentiality and security, regulatory compliance, insurance coverage, business continuity planning, subcontracting, encrypting, incident reporting, storage of data and an exit strategy. The contract will also identify service level agreements for monitoring of required controls during the duration of the engagement. If standardized contract language is not used, an exception process is followed to have the language approved by the appropriate risk teams, business units and Enterprise Risk Management.

Contractual Provisions

As referenced in the case study, it is important for firms to establish appropriate contractual language to govern vendor relationships. The provisions of the contract will govern the vendor's obligation to the firm, as well as identify the firm's prerogatives in relation to the vendor. This includes the manner in which the firm can conduct its ongoing oversight of the vendor, the conditions for terminating the relationship, and the vendor's obligations to protect firm information in the event the relationship terminates. The stringency of these clauses should be risk-based with riskier vendor relationships requiring stronger language.

Observations on Firm Practices

FINRA found that most firms had adequate privacy and security language in contracts where customer or firm confidential data or high-risk systems were at risk. Standard contract language topics that firms included were:

- **Non-disclosure agreements/confidentiality agreements:** This language outlines confidential material, knowledge or information that the parties exchange, such as customer PII or company trade secrets. The parties agree not to share further or disclose information obtained under the contract.
- **Data storage, retention and delivery:** This language describes how firm data should be stored and transmitted while on a vendor's system. This may include encryption requirements, requirements as to the type and location of servers used, and business recovery practices.
- **Breach notification responsibilities:** This language addresses the manner and timing of the vendor's notification to the data owner of a security breach and the requirements as to who is responsible for notifying customers along with any related costs. Contract language also would include the definition of a breach as it relates to the data or systems involved.
- **Right-to-audit clauses:** This language gives the data owner the ability to perform physical audits of the vendor's data storage facility and related controls. These clauses also might outline the vendor's responsibility for having a third-party test of the vendor's controls.
- **Vendor employee access limitations:** This language defines which vendor employees have access to firm data. Typically this language also documents the approval process for granting this access, *e.g.*, who at the firm would approve employee access to restricted data.
- **Use of subcontractors:** This language outlines any subcontractors that the vendor will use and that would have access to firm data. It also addresses the controls that the vendor would require at any subcontractor, for instance regarding employee data access or data encryption. Typically, controls expected to be present at the vendor would also be required at the subcontractor.

- **Vendor obligations upon contract termination:** This language addresses requirements regarding the destruction or return of any data stored at the vendor's physical locations, including how quickly any data would be disposed of. It also includes language related to removing employee access to the data.

Ongoing Due Diligence

After a contract is signed, firms should conduct ongoing due diligence of a vendor's controls and processes. This due diligence should provide the firm with sufficient information to assess whether the vendor is upholding its contractual commitments with respect to cybersecurity. The intensity of due diligence may be risk-based, *i.e.*, vendors that have access to more sensitive data or firm systems may be subjected to a higher level of scrutiny than other firms. As part of its ongoing due diligence, the firm may review vendor controls as discussed in the "Due Diligence on Prospective Vendors" section above.

Observations on Firm Practices

The firms FINRA reviewed that had more mature vendor management processes continue to have the firm's information security team involved in monitoring the vendor's controls and processes in place to protect customer or firm information. Similar to initial due diligence, this monitoring was risk-based and included sending questionnaires to vendors concerning controls, ongoing review of third-party control assessment reports, and, in some instances, on-site reviews to verify that controls were functioning as intended. The information security groups typically sent their results to the vendor management team along with recommendations for change, if warranted. As described above, firms used defined escalation processes if they identified problems.

Vendors and Risk Assessment

Apart from ongoing due diligence, vendor systems and processes should be included in a firm's overall risk assessment process, including being scored and analyzed just as any other in-house firm system would. The firm's governance process should apply to these vendor systems and any identified risks would be required to be mitigated either by the data owner or the vendor as directed by the data owner. As discussed earlier, firms would typically apply an escalation process to risks that could not be remediated in a timely fashion or that exceeded an asset criticality threshold.

Terminating the Vendor Relationship

When business relationships with a vendor end, firms should continue to focus on protecting customer and firm data to which the vendor had access or that was stored at the vendor's facilities. Crucial management processes include how a firm retrieves this data, how it is removed from vendor systems, how this removal is documented, and how and when vendor access to firm systems is revoked. Until all data is deleted or access to that data is terminated, the vendor relationship should be included in the firm's risk assessment process and continually reviewed.

Observations on Firm Practices

Firms indicated that when vendor relationships end, they receive written confirmations from vendors indicating all information has been deleted. One firm indicated it had a vendor exit template which addressed the deletion of data.

Although a number of firms addressed the issue of vendor obligations regarding data retention and destruction after contract termination, some did not. FINRA emphasizes that it is important for firms to manage data across its full life cycle with vendors. This should be addressed through contract and process measures that can provide a firm confidence that data it provides to vendors cannot be misused after a firm's relationship with a vendor is terminated.

Case Study: Risks and Opportunities in Cloud Computing

Across industry sectors, many firms today contract with vendors to provide cloud-based services. The cloud can present a challenge to firms' cybersecurity efforts for at least two reasons. First, cloud services can enable a business unit within a firm to pursue a substantial technology initiative with minimal involvement from the technology or other departments that traditionally have been involved in vetting and approving vendor relationships and that could act as a control to ensure that sound cybersecurity practices are in place. Second, cloud services—along with other outsourced information technology service delivery models—blur the boundary between firm and non-firm systems, and this makes it challenging for firms to define the perimeter of their technology environment and establish appropriate controls.

On the other hand, while much commentary has focused on the cybersecurity risks associated with cloud computing, it could also yield security benefits. For example, cloud computing providers can leverage their technology focus and scale to invest in more sophisticated and effective controls than many firms, especially smaller ones. This may enable a cloud-based service to provide a higher level of security than an individual firm might be otherwise able to afford.

According to firms in the sweep, relationships with cloud service providers are managed the same way as other vendor relationships, with the information security team playing a key role in the due diligence of any prospective system. By ensuring the involvement of the information security team, firms avoid the problem of a business unit circumventing governance processes intended to control cybersecurity risks. Key security considerations and questions for cloud-based services include:

- Shared access of systems, as many firms may be using the same systems and computing resources.
- Authentication and access control to the data. How does a cloud vendor control access to the systems and data? What processes are followed and approvals required to gain access?
- Many of these systems operate over the Internet. What controls does the vendor have in place to prevent hacking of these systems?
- What types of secure coding practices does the vendor enforce?
- What testing is conducted on an ongoing basis to identify potential issues within the security practices?
- What system development life cycle process does the vendor follow to implement system updates? Does the vendor perform adequate testing? Are system users involved?
- Who has physical access to the vendor's data center?

There are other key risks for any cloud system—including system availability and data ownership—that vendor management teams should address before implementation.

Staff Training

PRINCIPLES AND EFFECTIVE PRACTICES:

Firms should provide cybersecurity training that is tailored to staff needs. Effective practices for cybersecurity training include:

- defining cybersecurity training needs requirements;
- identifying appropriate cybersecurity training update cycles;
- delivering interactive training with audience participation to increase retention; and
- developing training around information from the firm's loss incidents, risk assessment process and threat intelligence gathering.

Employees are one of the major sources of cybersecurity risk for firms. FINRA found that many of the cybersecurity attacks that firms identified were successful precisely because employees made mistakes, such as inadvertently downloading malware or responding to a phishing attack. For this reason, cybersecurity training is an essential component of any cybersecurity program. Even the best technical controls on a firm's systems can be rapidly undermined by employees who are inattentive to cybersecurity risks.

The importance of training is widely recognized. The NIST Framework identifies training as a critical piece of an organization's cybersecurity infrastructure.[29] NIST recommends that all users (from vendors to senior executives) are informed and trained, and users understand their specific roles and responsibilities. This includes educating those users on the risks associated with the data they may encounter. Training is also a key component in the SANS Top 20. SANS recommends that organizations perform an analysis to determine where the skill gaps and points of risk exposure exist, and develop and deliver training in those areas.

Observations on Firm Practices

Many firms emphasized the importance of staff training; 95 percent of the firms deliver mandatory cybersecurity training for staff. Typically, this includes a combination of mandatory general awareness training for all staff and targeted training for specific staff groups. Not all firms had a formal cybersecurity program in place and FINRA believes that the absence of such a program exposes a firm to increased risk of a successful cybersecurity attack.

Training Content

Where firms developed and delivered cybersecurity training, there was a wide degree of overlap in the topics. Many firms in the sweep made the distinction between general topics that were deployed firm wide and those targeted to a specific audience, based on the individual's role at the firm. Some of the key topics are identified in the table below:

General Training	IT/Management Targeted
Recognizing Risks	Application Lifecycles
Social Engineering Schemes and Phishing	Application Security
Handling Confidential Information	Privilege Management
Password Protection	Emerging Technology Issues
Escalation Policies	Software Vulnerabilities
Physical Security	
Mobile Security	

Firms' approaches to delivering content varied. One firm developed its cybersecurity training in two distinct areas: cyber-specific and cyber-enabled. Cyber-specific training addressed topics that are specific to technology issues (*e.g.*, server intrusions, coding vulnerabilities), whereas cyber-enabled training addressed areas of exposure that simply use technology as the vehicle for the breach (*e.g.*, phishing scams, identity theft). Tailoring the content to a particular audience based on its potential exposure can help to limit unnecessary information overload.

In some instances, cybersecurity threats may originate from clients, so many broker-dealers provide cybersecurity education or information to their customers, especially if a customer's account has been attacked. Some firms prominently display the resources available to their clients on the main login page of their websites. Examples of customer-specific resources include recommendations for creating secure passwords and indications of social engineering attacks. FINRA believes this type of customer education can be beneficial, particularly since it can help reduce the likelihood that the same customers will be victimized again.

Training Frequency

FINRA observed that firms initiate training based on events or milestones, such as new employee onboarding, onboarding to a new role, calendar or other interval-based training, upon provision of a mobile device and on an *ad hoc* basis in response to specific events. Most commonly, firms delivered cybersecurity training to employees on an annual basis and frequently in conjunction with the firm's other annual training.

Because the threat landscape evolves quickly, firms should plan for events that would necessitate the delivery of training on a more expedited basis in certain situations. Approximately 40 percent of the firms specifically referenced a process by which *ad hoc* training can be developed, if such a need arises. One firm indicated that the questions it receives from its employees can drive *ad hoc* training.

An example of an effective *ad hoc* training program is a firm's response to a phishing attack. In this instance, a hacker was able to gain access to a client's personal email. The hacker then portrayed himself as the client of the firm and sent written instructions to wire transfer funds to an offshore bank account. Since the amount of the transfer was not unusual and the client frequently wired transferred funds, neither the registered representative nor branch office staff called the client to confirm the transaction. Only after the funds were sent, did the firm discover that the source of the transfer instructions was fraudulent. After completing the investigation, which revealed the lapse in firm procedures, the firm implemented new required verification of client instructions and rolled out a specific training requirement for all registered representatives and support staff. The firm provided the training materials and required branch management to host a meeting for all employees within their respective offices to ensure everyone was aware of the new requirements to verbally confirm all transfer instructions received.

Development and Delivery

The most effective cybersecurity training programs are developed in conjunction with the overall cybersecurity program, which allows firms to tailor their programs to their specific points of exposure. The institutional knowledge gathered from outside of the training department can add value to the program. This also allows a firm to implement training based on the trends and emerging threats that most affect its line of business. FINRA observed firms using three approaches to developing cybersecurity training programs—in-house, through vendors or a combination of the two. One firm indicated that its staff attends vendor and industry meetings on security topics to stay informed on these issues. There are resources available to firms that provide information about cybersecurity threats that can inform firms' training curricula.

Examples cited by firms include:

Name	Type
Sans Top 20	Vulnerabilities List
Symantic Threat Report	Threat Report
Cisco Threat Report	Threat Report
TrendMicro Threat Report	Threat Report
Sophos Threat Report	Threat Report
US-Cert Bulletins	News
Google Online Security Blog	News
Krebs on Security	News
ThreatPost	News
Cyberwarzone	News
The Hacker News	News
Dark Reading	News
DShield	News and Technical Community
SecurityFocus	Technical Community
Security Now	Podcast
Security Weekly	Podcast

Firms should recognize that, like any other training, FINRA will be interested in understanding firms' processes to determine the content of training and to validate its effectiveness.

Cyber Intelligence and Information Sharing

PRINCIPLES AND EFFECTIVE PRACTICES:

Firms should use cyber threat intelligence to improve their ability to identify, detect and respond to cybersecurity threats. Effective practices include:

- assigning responsibility for cybersecurity intelligence gathering and analysis at the organizational and individual levels;
- establishing mechanisms to disseminate threat intelligence and analysis rapidly to appropriate groups within the firm, for example, the firm's risk management and front-line information technology security staff;
- evaluating threat intelligence from tactical and strategic perspectives, and determining the appropriate time frame for the course of action; and
- participating in appropriate information sharing organizations—*e.g.*, FS-ISAC—and periodically evaluating the firm's information-sharing partners.

The importance of cybersecurity threat intelligence and information sharing is increasing as cybersecurity threats proliferate and advance in complexity. Firms that can take in and analyze cyber intelligence effectively can proactively implement measures to reduce their vulnerability to cybersecurity threats and thereby improve their ability to protect both customer and firm information. In addition, firms can help other members of the industry address cybersecurity threats more effectively by sharing information about attacks.

To promote the disclosure and sharing of cybersecurity information among firms, the U.S. federal government was instrumental in establishing many industry-based information sharing and analysis centers (ISACs) pursuant to Presidential Decision Directive 63 on Critical Infrastructure Protection: Sector Coordinators. The fundamental goal of the ISACs is to expose security vulnerabilities and identify solutions to help create internal infrastructures to prevent, detect and correct security breaches as quickly as possible. The FS-ISAC provides a venue for the financial services industry to share threat intelligence, anonymously if so desired, and the ability to turn threat data into "actionable intelligence."

Observations on Firm Practices

FINRA's sweep revealed widely different approaches to the establishment of a cyber threat intelligence analysis capability. These approaches include:

- establishing an in-house group or department responsible for handling threat intelligence;
- using a managed security services provider;
- relying on software vendors to become aware of and patch vulnerabilities in their products; and
- using a combination of in-house responsibilities and reliance on vendors.

Many larger firms have established dedicated threat intelligence centers that receive and analyze threat intelligence from a variety of sources. These centers provide their firms with the ability to perform in-depth analysis of cybersecurity intelligence information, as well as the ability to respond rapidly to threats. In addition, large firms frequently supplement their in-house cyber intelligence program with outsourced services.

Some smaller firms relied on vendors to provide a range of cybersecurity services, including threat intelligence analysis. These services included analyzing information shared about software vulnerabilities and identifying common vulnerability exposures relevant to the firm's technology environment; performing network analysis to identify potentially anomalous activity; and conducting vulnerability and penetration testing. The potential advantage of this approach for smaller firms is that they can take advantage of the vendor's specialized expertise to achieve a higher level of cybersecurity than the firm could obtain at similar cost with in-house resources.

FINRA also observed that firms relied on a broad range of sources to obtain cyber threat intelligence. These sources include centralized information sharing centers (*e.g.*, FS-ISAC), industry peers, specialized cybersecurity information vendors, software vendors, and government and law enforcement agencies. The following table summarizes observations from the sweep regarding sources of information sharing.

	2014 Sweep Results (% of respondents sharing information)
Financial Services Information Sharing and Analysis Center FS-ISAC	72
United States Computer Emergency Readiness Team (US-CERT)	50
FBI or InfraGard	28
National Cyber Forensics and Training Alliance (NCFTA)	23
Department of Homeland Security (DHS)	22

Firms' willingness to share information about cybersecurity threats varied considerably. Several firms explained that they do not share threat information while others engage actively with information sharing entities. In particular, larger firms are more likely to associate with or join information sharing organizations such as the FS-ISAC, National Cyber Forensics and Training Center or Red Sky Alliance as well as to share information with government agencies.

An effective practice is for firms to maintain policies and procedures that describe the organizations with which the firm is willing to share information and the types of information subject to sharing. One firm explained that it may share certain types of information through what it defined as trust groups (*i.e.*, FS-ISAC, BITS, the technology policy division of the Financial Services Roundtable, and Red Sky Alliance). The information may include threat indicators such as domains, IP addresses, email headers and payloads, file information (*e.g.*, names) as well as files themselves for research purposes. The firm does not share internal, confidential or proprietary information, and scrubs firm-specific IP addresses, machine names, user information and other identifying information.

FINRA believes that the securities industry can be more effective in advancing cybersecurity for the community as a whole when it engages in collaborative self-defense. To that end, FINRA urges firms to revisit their hesitancy to participate in information sharing bodies in light of the extremely positive view that other firms have expressed to FINRA about the benefits.

Further, a concern expressed to FINRA was that a firm might be subject to regulatory scrutiny through information sharing. While firms must ensure that information sharing conforms with regulatory requirements, we cite the April 10, 2014, Federal Trade Commission and the Department of Justice (DOJ) policy statement on information sharing. In that statement, the FTC and DOJ explained that the sharing of "cyber threat information is not likely to raise antitrust concerns and can help secure the nation's networks of information and resources." In addition, the DOJ published a white paper on May 9, 2014, concerning the sharing of information relating to cyber threats with other organizations and with the government. The DOJ explained that the sharing of aggregate data and descriptions of an attack's characteristics (*i.e.*, unusual changes in traffic patterns) is not a violation of privacy laws.

FINRA observed firms using cybersecurity threat information and intelligence in many ways. Most of the firms described tactical uses for threat intelligence. This includes collection and analysis of threat and vulnerability information that firms could then incorporate in their technical infrastructure, *e.g.*, by adjusting firewall settings to block certain IP addresses, installing patches to fix vulnerabilities in software, or updating anti-virus and anti-malware software to capture newly identified instances of viruses or malware.

In addition to tactical uses, firms also identified other, more strategic roles for cyber intelligence. For example, trending analysis of incidents or threats may drive changes in the firm's procedures or techniques for mitigating threats. One firm noted it was significantly changing its approach to performing back-up operations in light of certain attack methodologies. Firms can also use threat intelligence to assess whether their investment in the firm's cybersecurity technology and systems are adequate to address their potential vulnerabilities and threats.

Against this backdrop, it is evident that the effective use of cybersecurity threat intelligence can be challenging. Some firms, for example, simply may not have staff with the technical capability to interpret and apply information regarding specific threats. Information sharing organizations and the industry should determine how cybersecurity threat information can be presented to different segments of the broker-dealer community in ways that make it more actionable.

Beyond this, for those firms that do have the technical knowledge to use threat information, the sheer volume of that information can make it challenging to implement timely responses. In this regard, efforts are underway to automate the transmission and ingestion of threat intelligence into security tools, such as firewalls. Several of the larger firms with which FINRA spoke were in the process of piloting or considering implementing tools to support this automation. FINRA strongly supports the objective of these programs and hopes that their benefits can be made available to firms of all sizes at affordable prices.[30]

Cyber Insurance

PRINCIPLES AND EFFECTIVE PRACTICES:

Firms should evaluate the utility of cyber insurance as a way to transfer some risk as part of their risk management processes. Effective practices include:

- for firms that have cybersecurity coverage, conducting a periodic analysis of the adequacy of the coverage provided in connection with the firm's risk assessment process to determine if the policy and its coverage align with the firm's risk assessment and ability to bear losses; and
- for firms that do not have cyber insurance, evaluating the cyber insurance market to determine if coverage is available that would enhance the firm's ability to manage the financial impact of cybersecurity events.

In assessing their cyber insurance options, firms may want to consider the following questions:[31]

- Do existing insurance policies cover any aspects of cybersecurity events?
- Which events are insurable?
- Do the firm's risk management approaches adequately cover the financial risks associated with cybersecruity events?
- What coverage will a new or enhanced cyber insurance policy provide and what will it cost?

Observations on Firm Practices

Firms with insurance articulated three broad reasons for purchasing coverage: 1) to transfer potential unmitigated risk above the firm's risk appetite; 2) to obtain coverage for gaps, such as data breaches, that may not covered in existing policies, and 3) to reduce the risk of potential impact to a firm's financial statement in the event of an attack.

These firms also identified three sources of cyber insurance coverage: 1) a standalone policy specifically underwritten by the insurance carrier to provide the firm with cyber insurance; 2) obtaining cybersecurity liability riders in connection with a firm's existing insurance policies (*i.e.*, fidelity bond, errors and omissions policies); and 3) relying on a firm's existing insurance policies (*i.e.*, errors and omissions) that included some, but limited, coverage to cyber-related incidents. The standalone policies firms purchased typically cover data breaches, remediation cost reimbursement limits to respond to the breaches, and coverage for regulatory and legal fines and penalties.

Among the firms FINRA reviewed, 61 percent purchased standalone cybersecurity insurance; 11 percent purchased a cybersecurity rider with their fidelity bond; and 28 percent did not rely on any type of cybersecurity insurance at the time of the sweep. Typically, large firms purchased standalone policies, where they had the ability to customize the types and amount of coverage based on their risk appetite. However, smaller and mid-size firms with limited cybersecurity risk typically purchased cybersecurity riders in connection with existing fidelity bond policies. None of the firms with either type of coverage made cyber insurance-related claims to recover losses.

Firms also commented that the market for cyber insurance is relatively new and evolving rapidly. There is now greater diversity of coverage available and at more affordable rates, in some cases.

One firm's experience is illustrative of factors that may lead a firm to purchase standalone cybersecurity coverage where it was not previously in place. The firm's decision to obtain coverage was driven by increased visibility of cybersecurity concerns generally, changes in the market for cyber insurance, improved firm understanding of gaps in its existing coverage (*e.g.*, with respect to intangible assets), and a change in culture in the firm's purchasing office. The firm now reviews its insurance coverage annually. Departments involved in the review process include purchasing, operational risk and IT security. This firm pointed to the ancillary benefit of having the insurance carrier review the firm's cybersecurity program.

While the decision to purchase or forego cyber insurance lies with firms, FINRA urges firms to monitor developments in the cyber insurance market and to evaluate what role, if any, it can play in a firm's efforts to mitigate cybersecurity risks and absorb the financial ramifications of a cyber-related event.

Conclusion

Cybersecurity is a key risk that the broker-dealer industry faces today and that will likely grow in importance in the coming years. Firms should make the development and implementation of measures to address cybersecurity challenges one of the cornerstones of a sound business infrastructure. The principles and effective practices described in this report can help firms in that effort.

A risk management-based approach to cybersecurity permits firms to tailor their approach to the individual circumstances and the changing threats each firm faces. The framework and standards discussed can inform firms' thinking at a programmatic as well as individual control level. As many firms noted during FINRA's sweep, there is no one-size-fits-all solution to address cyber threats.

Much attention has been focused on advanced threats that firms face, and those certainly pose significant dangers. However, most successful attacks take advantage of fairly basic control weaknesses. While firms need to stay on guard, they can also take some comfort from this. To be sure, cybersecurity is challenging to address, but it is certainly not impossible. What is required is rigorous attention to detail and execution. Risk assessments can help firms identify and prioritize those steps that are most urgent to undertake. Information sharing can help firms understand the types of threats they may face and available mitigation measures.

Looking forward, FINRA's expectation is that firms will review this report to assess what aspects of the principles and effective practices addressed herein could help them build or improve their cybersecurity readiness. Of course, this report is just one of many resources firms should draw upon to inform their cybersecurity program.

FINRA expects that firm management will make cybersecurity a priority and that it will devote sufficient resources both to understand the current and evolving cybersecurity threats to which the firm may reasonably expect to be exposed and to implement measures necessary to achieve the desired risk posture.

Appendix I – Summary of Principles and Effective Practices

Governance and Risk Management for Cybersecurity

Principle: Firms should establish and implement a cybersecurity governance framework that supports informed decision making and escalation within the organization to identify and manage cybersecurity risks. The framework should include defined risk management policies, processes and structures coupled with relevant controls tailored to the nature of the cybersecurity risks the firm faces and the resources the firm has available. Effective practices include:

- defining a governance framework to support decision making based on risk appetite;
- ensuring active senior management, and as appropriate to the firm, board-level engagement with cybersecurity issues;
- identifying frameworks and standards to address cybersecurity;
- using metrics and thresholds to inform governance processes;
- dedicating resources to achieve the desired risk posture; and
- performing cybersecurity risk assessments.

Cybersecurity Risk Assessment

Principle: Firms should conduct regular assessments to identify cybersecurity risks associated with firm assets and vendors and prioritize their remediation. Effective practices include establishing and implementing governance frameworks to:

- identify and maintain an inventory of assets authorized to access the firm's network and, as a subset thereof, critical assets that should be accorded prioritized protection; and
- conduct comprehensive risk assessments that include:
  - an assessment of external and internal threats and asset vulnerabilities; and
  - prioritized and time-bound recommendations to remediate identified risks.

Technical Controls

Principle: Firms should implement technical controls to protect firm software and hardware that stores and processes data, as well as the data itself. Effective practices include:

- implementing a defense-in-depth strategy;
- selecting controls appropriate to the firm's technology and threat environment, for example:
  - identity and access management
  - data encryption; and
  - penetration testing.

Incident Response Planning

Principle: Firms should establish policies and procedures, as well as roles and responsibilities for escalating and responding to cybersecurity incidents. Effective practices for incident response include:

- preparation of incident responses for those types of incidents to which the firm is most likely to be subject, *e.g.*, loss of customer PII, data corruption, DDoS attack, network intrusion, customer account intrusion or malware infection;
- incorporation of current threat intelligence to identify the most common incident types and attack vectors;
- containment and mitigation strategies for multiple incident types;
- eradication and recovery plans for systems and data;
- investigation and damage assessment processes;
- preparation of communication/notification plans for outreach to relevant stakeholders, *e.g.*, customers, regulators, law enforcement, intelligence agencies, industry information-sharing bodies;
- involvement in industrywide, and firm-specific, simulation exercises as appropriate to the role and scale of a firm's business and;
- implementation of measures to maintain client confidence, including:
  - provision of credit monitoring for individuals whose personal information has been compromised; and
  - reimbursement of customers for financial losses incurred.

Vendor Management

Principle: Firms should manage cybersecurity risk that can arise across the lifecycle of vendor relationships using a risk-based approach to vendor management. Effective practices to manage vendor risk include:

- performing pre-contract due diligence on prospective service providers;
- establishing contractual terms appropriate to the sensitivity of information and systems to which the vendor may have access and which govern both the ongoing relationship with the vendor and the vendor's obligations after the relationship ends;
- performing ongoing due diligence on existing vendors;
- including vendor relationships and outsourced systems as part of the firm's ongoing risk assessment process;
- establishing and implementing procedures to terminate vendor access to firm systems immediately upon contract termination; and
- establishing, maintaining and monitoring vendor entitlements so as to align with firm risk appetite and information security standards (*see* "Technical Controls" section).

Staff Training

Principle: Firms should provide cybersecurity training that is tailored to staff needs. Effective practices for cybersecurity training include:

- defining cybersecurity training needs requirements;
- identifying appropriate cybersecurity training update cycles;
- delivering interactive training with audience participation to increase retention; and
- developing training around information from the firm's loss incidents, risk assessment process and threat intelligence gathering.

Cyber Intelligence and Information Sharing

Principle: Firms should use cyber threat intelligence to improve their ability to identify, detect and respond to cybersecurity threats. Effective practices include:

- assigning responsibility for cybersecurity intelligence gathering and analysis at the organizational and individual levels;
- establishing mechanisms to disseminate threat intelligence and analysis rapidly to appropriate groups within the firm, for example, the firm's risk management and front-line information technology security staff;
- evaluating threat intelligence from tactical and strategic perspectives, and determining the appropriate time frame for the course of action; and
- participating in appropriate information sharing organizations—*e.g.*, FS-ISAC—and periodically evaluating the firm's information-sharing partners.

Cyber Insurance

Principle: Firms should evaluate the utility of cyber insurance as a way to transfer some risk as part of their risk management processes. Effective practices include:

- for firms that have cybersecurity coverage, conducting a periodic analysis of the adequacy of the coverage provided in connection with the firm's risk assessment process to determine if the policy and its coverage align with the firm's risk assessment and ability to bear losses; and
- for firms that do not have cyber insurance, evaluating the cyber insurance market to determine if coverage is available that would enhance the firm's ability to manage the financial impact of cybersecurity events.

Appendix II – The NIST Framework

The NIST Framework has three major elements: the Framework Core, Framework Tiers, and Framework Profiles. Each is described below.

Framework Core

The Framework Core breaks down cybersecurity activities into five major functions or areas of activity in which firms should engage:

- **Identify:** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities.
- **Protect:** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect:** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond:** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover:** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.[32]

Within each of these functional areas, the NIST Framework identifies related categories and subcategories of outcomes that support the function. And, for each subcategory, the Framework presents relevant "Informative References," *e.g.*, references to NIST, COBIT or ISO standards.

For example, within the functional area "protect," the Framework identifies six categories of related outcomes: access control, awareness and training, data security, information protection processes and procedures, maintenance, and protective technology. Within the first of these categories, access control, the Framework identifies the following subcategories: 1) identities and credentials are managed for authorized devices and users; 2) physical access to assets is managed and protected; 3) remote access is managed; 4) access permissions are managed, incorporating the principles of least privilege and separation of duties; and 5) network integrity is protected, incorporating network segregation where appropriate.

Framework Tiers

Framework Tiers (or Tiers) "provide context on how an organization views cybersecurity risk and the processes in place to manage that risk." The tiers reflect the level of rigor and sophistication in a firm's cybersecurity risk management practices and the degree to which those practices are integrated into an organization's risk management practices and reflect the organization's overall business needs. The Framework identifies four tiers ranging from "partial" to "adaptive" with the latter being the most advanced level.[33]

The tiers enable an organization to evaluate its perception of risk and the value of risk management activities available to mitigate those risks. The idea is to move toward a higher tier only when doing so would reduce cybersecurity risk and remain consistent with organizational goals.

The NIST Tier definitions are as follows:

Tier 1: Partial

- *Risk Management Process*—Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- *Integrated Risk Management Program*—There is limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.
- *External Participation*—An organization may not have the processes in place to participate in coordination or collaboration with other entities.

Tier 2: Risk Informed

- *Risk Management Process*—Risk management practices are approved by management but may not be established as organization-wide policy. Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- *Integrated Risk Management Program*—There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established. Risk-informed, management-approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties. Cybersecurity information is shared within the organization on an informal basis.
- *External Participation*—The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.

Tier 3: Repeatable

- *Risk Management Process*—The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
- *Integrated Risk Management Program*—There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.
- *External Participation*—The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.

Tier 4: Adaptive

- *Risk Management Process*—The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.
- *Integrated Risk Management Program*—There is an organization wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.
- *External Participation*—The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.[34]

Framework Profile

NIST describes the Framework Profile as "the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization." A firm can use a profile to express its current state of cybersecurity preparedness as well as a desired future state. By comparing the two, a firm can begin to identify gaps and develop a road map to achieve its desired profile.[35] A firm may also have more than one profile. For example, a firm with multiple business lines might create a different profile for each business line.

Appendix III – Encryption Considerations

An encryption technology that firms may consider is an Information Rights Management (IRM) solution. IRM solutions are typically applied to unstructured data elements such as PDF files and spreadsheets. They provide for both the encryption of the file contents as well as for control over how the file contents can be used by those granted access to the data. For example, someone who possesses a file can be granted the ability to view the contents, but prevented from printing the document. And in the event a holder of the file forwards the file to someone else (whether intentionally or inadvertently), the receiver will be unable to view the contents unless they have been given rights to do so.

IRM technology is increasingly available in commonly used commercial-off-the-shelf (COTS) desktop automation solutions. There are, however, key management infrastructure considerations to address should there be a need to make IRM-protected files available to third parties. Cloud-based solutions may be appealing, but this may mean exposing keys to the cloud service provider.

Whatever encryption solutions a firm deems appropriate to mitigate its risks, the firm will need to consider factors such as algorithm selection and key management. There are multiple encryption algorithms available with varying benefits in terms of security and performance. Furthermore, any encryption solution is subject to correct implementation and appropriate selection of important variables (*e.g.*, key size). Due to these complexities, it is generally recommended that firms perform encryption using a well-established COTS or open source solution. For a firm to build its own encryption solution from scratch carries with it a higher risk of a flawed implementation that can be circumvented by a determined attacker. NIST maintains a Cryptographic Algorithm Validation Program that may be a useful resource in determining whether a particular algorithm, or implementation thereof, is secure.

In any encryption implementation, firms will also need to address key management considerations such as how to securely distribute keys as well as how and when to rotate keys. The strongest encryption algorithm can fail if keys are not well controlled. NIST SP 800-57 may be a useful resource in performing key management securely.

Endnotes

1. The sweep and survey have very different sample sizes; FINRA sent the 2014 sweep to a select cross section of firms and the 2011 survey to more than 200 firms.

2. *See* National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0*, p. 21.

3. *Cyber-Risk Oversight: Executive Summary,* Director's Handbook Series, 2014 Edition, National Association of Corporate Directors in collaboration with AIG and the Internet Security Alliance.

4. *Ibid.*, p. 4.

5. Structured Query Language (SQL) is a language used to query databases. An SQL injection attack is a technique in which an SQL query is used to try and extract information from a database.

6. As used in this report, "framework" refers to a broad approach to cybersecurity while standards are more specific and prescriptive.

7. The organization that publishes COBIT 5 was formerly known as the Information Systems Audit and Control Association, but it adopted the acronym as its full name.

8. *See* SANS *Critical Security Controls page.*

9. We use metrics here to refer to two or more measurements compared with a baseline. This definition is drawn from Shirley C. Payne, *A Guide to Security Metrics*, SANS Institute, June 19, 2006. p. 1.

10. National Institute of Standards and Technology, Elizabeth Chew, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown, and Will Robinson, NIST Special Publication 800-55 Revision 1, *Performance Measurement Guide for Information Security*, July 2008, p. 1.

11. *Ibid*, p. 10.

12. *The State of Risk-Based Security: US & UK*, Ponemon Institute, 2013 Research Report, pp. 15-18.

13. "Assets" refers to people, hardware, business applications and other software, and data on the firm's network.

14. This can include firms' telephony and other Internet-protocol-based communications systems which can be a vehicle for data exfiltration.

15. *See* NIST Framework, ID.AM-1, ID.AM-2, ID.AM-5, p. 20, and SANS Top 20.

16. *See* NIST Framework at Risk Assessment (ID.RA), p. 22.

17. *Ibid.*, pp. 22-23.

18. The role-based entitlement constitutes the first control on access to sensitive data or systems.

19. A system risk categorization methodology akin to *FIPS 199* and *NIST 800-60* can help to drive these decisions.

20. McKinsey & Company, "*How good is your cyberincident response plan?*" Tucker Bailey, Josh Brandley, and James Kaplan, December 2013.

21. *Ibid.*

22. National Institute of Standards and Technology, Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone, *Computer Security Incident Handling Guide –Special Publication 800-61*, August 2012, p. 25.

23. *Ibid.*, p. 35.

24. *Ibid.*, p. 35.

25. *Ibid.*, p. 37.

26. *Ibid.*, p. 37.

27. Firms can review *Regulatory Notices 11-06* and *11-32* for additional information on Rule 4530(b) filing requirements as well as at the *Rule 4530 Reporting Requirements FAQ*.

28. *See Notice to Members 05-48* for further information about firms' obligations in outsourcing arrangements.

29. *See* NIST Framework at "Awareness and Training" (PR.AT), pp. 24-25.

30. One example of efforts in this area is Soltra Edge™, a "threat intelligence sharing solution" offered by *Soltra*, a joint venture launched by the Depository Trust Clearing Corporation and FS-ISAC in 2014.

31. Cyber Insurance Roundtable Readout Report, Department of Homeland Security, February 2014, pp. 4-7.

32. NIST Framework, pp. 8-9.

33. NIST Framework, p. 9.

34. NIST Framework, p. 10-11.

35. NIST Framework, p. 11.

Investor protection. Market integrity.

1735 K Street, NW
Washington, DC 20006-1506

www.finra.org

15_0022.1 –02/15