# Report on Selected Cybersecurity Practices – 2018

**DECEMBER 2018**

## Contents



A REPORT FROM **THE FINANCIAL INDUSTRY REGULATORY AUTHORITY**

## Introduction

This report continues FINRA's efforts to share information that can help broker-dealer firms further develop their cybersecurity programs. Firms routinely identify cybersecurity as one of their primary operational risks. Similarly, FINRA continues to see problematic cybersecurity practices in its examination and risk monitoring program. This report presents FINRA's observations regarding effective practices that firms have implemented to address selected cybersecurity risks while recognizing that there is no one-size-fits-all approach to cybersecurity.

When selecting the topics for this report, FINRA considered the evolving cybersecurity threat landscape, firms' primary challenges and the most frequent cybersecurity findings from our firm examination program. First, we address how firms have strengthened their cybersecurity controls in branch offices, which is especially important for firms with decentralized business models. Second, we discuss limiting phishing attacks, which remain a top cybersecurity challenge for many firms. Third, we explain the importance of identifying and mitigating insider threats, which are of concern for many firms. Fourth, we describe the elements of a strong penetration testing program. Finally, we share observations regarding establishing and maintaining controls on mobile devices, which have emerged as a significant risk for many firms because of their increasingly widespread use by employees and customers.

FINRA notes that the specific practices highlighted in this report should be evaluated in the context of a holistic firm-level cybersecurity program. FINRA's 2015 *Report on Cybersecurity Practices* addresses the elements of such cybersecurity programs and provides guidance to firms seeking to improve their current protocols. Further, small firms seeking to develop or improve their cybersecurity practices should review the appendix to this report "Core Cybersecurity Controls for Small Firms." This appendix, combined with the FINRA *Small Firm Cybersecurity Checklist* will assist small firms in identifying possible cybersecurity controls.

This report is not intended to express any legal position, and does not create any new legal requirements or change any existing regulatory obligations.

Inquiries regarding this report may be directed to Carlo di Florio, Executive Vice President, Member Supervision/Shared Services, at (212) 858-3908 or *carlo.diflorio@finra.org*; or Steven Polansky, Senior Director, Member Supervision/Shared Services, at (202) 728-8331 or *steven.polansky@finra.org*.

## Branch Controls

FINRA has observed that some firms face challenges maintaining effective cybersecurity controls at their branch locations. Branches' autonomy from the home office may adversely affect firms' ability to implement a consistent firm-wide cybersecurity program. Some firms may experience increased challenges if their branches may, for example, purchase their own assets, use non-approved vendors or not follow their firms' software patching and upgrade protocols. Similarly, representatives working from home may require even further oversight and technological support to comply with firm standards. As a result, firms should evaluate whether they need to enhance their branch-focused cybersecurity measures to maintain robust cybersecurity controls and protect customer information across their organizations.

FINRA has observed firms implementing the following effective practices:

- Establishing Written Supervisory Procedures (WSPs) to define minimum cybersecurity controls for branches and formalize oversight of branch offices;
- Developing an inventory of branch-level data, software and hardware assets;
- Maintaining branch technical controls; and
- Implementing a robust branch cybersecurity examination program.

### Branch-Level WSPs

Although most firms have developed WSPs addressing cybersecurity controls, FINRA has observed that branch offices may have less developed cybersecurity controls in comparison to the home office. In some cases, for example, firms may have distributed guidance on cybersecurity to branches in a range of memos, newsletters, questionnaires and training, but may not have consolidated those into a comprehensive, easily referenced set of minimum standards or best practices for their branches.[1] Other firms may not have formalized their oversight of branch offices' administration of cybersecurity controls.

FINRA has observed firms implementing the following effective practices:

- Developing branch-level WSPs and other comprehensive guidance on cybersecurity controls and distributing such guidance to all branches;
- Distributing alerts and notifications on emerging cybersecurity issues to both home office employees and branch representatives;
- Designating the branch office supervisor or another branch office staff member with responsibility for that branch's cybersecurity controls;
- Providing branches a list of required and recommended hardware and software options and settings, as well as approved vendors;
- Mandating that branch personnel notify branch management of and properly respond to violations of firm cybersecurity standards or material cybersecurity incidents involving loss of confidentiality, availability or integrity of customer personally identifiable information (PII) or sensitive firm data (*see* Sections 11 and 12 of FINRA's *Small Firm Cybersecurity Checklist*); and
- Mandating that registered representatives complete an annual attestation to comply with the firm's WSP requirements, including its cybersecurity policies.

Further, FINRA notes that training plays an integral role in improving the quality of branch-level cybersecurity programs and controls. In particular, firms could consider requiring branch staff and registered representatives with access to customer information, as well as those working remotely, to complete initial onboarding, as well as ongoing, regular training on firm cybersecurity standards, practices and risks (in addition to their required firm continuing education (CE) program training).[2] Ongoing training may include web-based or in-person courses, simulations of actual cases experienced by the firm or peer firms, security awareness bulletins and phishing or other campaigns. In order to determine the scope and depth of branch personnel training, firms may also consider incorporating into their training program a formal or informal evaluation of the staff's understanding of and compliance with firm cybersecurity requirements. *See* Section 8 of FINRA's *Small Firm Cybersecurity Checklist* for additional guidance on firm training.

## Asset Inventory

Asset inventories are a key element of any firm's cybersecurity program, especially where branches' autonomy may make it difficult for firms to know the scope of assets they need to protect. Branches and registered representatives may not be aware of the locations where they store sensitive customer or firm data; use unapproved software, hardware or vendor-provided services; or not comply with other firm cybersecurity standards. An asset inventory can help reduce these risks and provide important information for managing branch office security controls.

When used in conjunction with a cybersecurity risk assessment, an asset inventory can serve as a starting point to identify critical assets and their vulnerability to attack, as well as appropriate policy, technical and physical controls to mitigate those risks.

For further information on asset inventories, see Sections 1 and 8 of FINRA's *Small Firm Cybersecurity Checklist* and the "Asset Inventories and Critical Assets" discussion in FINRA's *Report on Cybersecurity Practices*.

FINRA has observed firms implementing the following effective practices:

- Requiring branches to perform initial and recurring inventories of branch assets and update the firm regarding any changes;
- Identifying sensitive customer and firm information and the location(s) where such information is stored;
- Ensuring the physical security of branch assets;
- Establishing processes by which branches manage and report lost or stolen assets;
- Providing secured asset disposal, such as destroying hard drives of computers no longer in use; and
- Ensuring branch operating systems are properly supported and maintained either by the firm or by vendors.

## Technical Controls

Firms face a variety of potential threats to their data and systems at the branch level. Firms can use a cybersecurity risk assessment to determine which threats are most significant for each branch and, then, identify and implement appropriate technical (and other) controls to mitigate those threats.[3]

FINRA has observed firms implementing the following effective practices:

- Developing identity and access management protocols for registered representatives and other staff, including managing the granting, maintenance and termination of access to firm and customer data;
- Limiting registered representatives' access to only their own customers' data and related exception reports;
- Setting minimum password requirements and multi-factor authentication for access to firm systems and applications by firm employees, registered representatives, vendors, contractors and other insiders (*see* Insider Threats section of this report, below);
- Prohibiting the sharing of passwords among firm staff;
- Prohibiting the storage of sensitive customer or firm data in unapproved or prohibited locations (*e.g.*, a file server, cloud provider or thumb drive and without encryption or transmitted without encryption);
- Establishing minimum encryption standards for all branch hardware used to access firm systems, including laptops, desktops, servers, mobile devices and removable media devices;
- Requiring branches to adhere to minimum encryption standards (and providing technical tools to enforce that standard) for data-in-transit, such as emails and file transfers that include customer PII or sensitive information;
- Ensuring branches use only secure, encrypted wireless settings for office and home networks;
- Maintaining regular patching, anti-virus protection, anti-malware and operating system updates for all branch computers and servers that access firm data in a manner that is consistent with firm, vendor and industry standards;
- Developing physical security protocols for all portable devices used to access firm data and systems, including laptops and mobile devices;
- Mandating all branch vendors (including cloud providers) meet firm security requirements, especially if firm data or other sensitive information will be accessed or maintained by the vendor; and
- Creating processes and selecting firm-approved vendors for the secure disposal of hard copy records and firm computer hardware (*e.g.*, hardware listed in the firm's inventory) that may contain sensitive information.

For further information on technical controls, see Sections 3 through 10 of FINRA's *Small Firm Cybersecurity Checklist* and FINRA's *Report on Cybersecurity Practices*.

### Branch Review Program

Firms' branch office reviews are an important tool to evaluate branches' cybersecurity vulnerabilities and ensure that branches are consistently applying cybersecurity controls across a firm's branch network. The review program may include on-site branch inspections, remote surveillance, inspections, reports and questionnaires to evaluate and record each branch's and registered representative's compliance with the firm's cybersecurity standards.

FINRA has observed firms implementing the following effective practices:

- Developing a framework to capture cybersecurity risks, risk levels and related controls at each branch;
- Implementing periodic exam visits or risk-based audits, the frequency and focus of which may depend on the risk profile of each branch;
- Implementing automated ways to verify and monitor branch controls, such as verifying patching, virus and malware protection, encryption and password protection;
- Ensuring that firm branch examiners have sufficient cybersecurity expertise to perform effective examinations of branch cybersecurity programs;
- Confirming branches meet firm cybersecurity standards and use firm-recommended vendors or other vendors meeting firm standards;
- Imposing consequences (including but not limited to fines, sanctions, or termination) for branches and registered representatives engaging in repeat violations of firm standards;
- Providing compliance and technology support to branches and registered representatives implementing firm cybersecurity protocols; and
- Re-evaluating branches where branch reviews identified material deficiencies or reported material cybersecurity incidents to ensure that the branch has implemented corrective action.

## Phishing

Social engineering or "phishing" attacks are one of the most common cybersecurity threats firms have discussed with FINRA. Phishing attacks may take a variety of forms, but all of them try to convince the recipient to provide information or take an action. Although some phishing emails are distributed to millions of recipients, other attempts are thoroughly researched and carefully customized to reach one or more selected individuals (*e.g.*, an individual who attackers have determined is likely to have administrator privileges), while a related attack targets one or more senior firm personnel (*e.g.*, the CEO or CFO). (These types of attacks are referred to as "spear phishing" and "whaling" respectively, but we refer to them collectively as "phishing" in the remainder of this document.)

In a phishing event, the attackers try to disguise themselves as a trustworthy entity or individual via email, instant message, phone call or other communication, where they request PII (such as Social Security numbers, usernames or passwords), direct the recipient to click on a malicious link, open an infected attachment or application or attempt to initiate a fraudulent wire transfer. Such "phishes" can appear to come from a variety of sources, including the following types of senders:

| Entities | Individuals |
|---|---|
| Firm or affiliate | Friends |
| Government agencies, such as the U.S. Securities and Exchange Commission, FINRA and IRS | Customers |
| Banks or other financial institutions | Information Technology (IT) administrators or Help Desk representatives |
| Social media sites | Office managers |
| Auction sites | Senior executives |
| Online payment processors | CEO or CFO |

The growing sophistication and quality of phishing (especially spear phishing and whaling) attacks makes it challenging for recipients to distinguish them from legitimate communications. The following list may help firms understand the hallmarks of phishing communication:

| Category | Characteristics |
|---|---|
| **Sender** | Discrepancies between the name and email address or "reply to" address of the sender |
| | Unknown individual or corporation |
| | New individual with whom you do not regularly correspond, such as IT manager, senior manager or CEO of the organization |
| **Recipients** | Additional unknown recipients |
| **Content** | Generic salutations |
| | Unexpected timing, type or style of communication from a known sender, such as a friend, co-worker or boss |
| | Problems with grammar or spelling, including subtle character substitutions, such as 0 (zero) in place of O (the letter O), or 1 (the digit one) in place of l (lower-case letter L) |
| | Request for highly sensitive information, such as customer account lists, Social Security numbers, credit card numbers, user names or passwords |
| | Sense of urgency with a request to access links or attachments, provide personal information or initiate a transaction (FINRA observes this frequently in the context of fraudulent wire transfer requests) |
| | Pressure to bypass or ignore firm policies or procedures |
| | Notifications that are "too good to be true" (such as winning the lottery or receiving an inheritance) |
| | Content that is designed to induce an emotional reaction in the recipient, such as political messages, personal attacks or untrue accusations |
| **Attachments and Links** | Unexpected attachments, apps or links |
| | Discrepancy between the written address of the link and its true destination (determined by hovering over the link) |
| | Suspicious URL patterns where the name of the intended web site appears anywhere other than at the very beginning of the URL |
| | Upon visiting the site, a message that indicates a problem with the "certificate" |

Phishing is a serious threat to firms and their customers. Victims of phishing attacks may release customer, firm, or personal information to cyber criminals; engage in unauthorized wire transfers or payments; or introduce viruses, malware, ransomware, or crimeware that destroys, shuts down, takes over or infects firm systems. Although most firms are aware of the risks posed by phishing attacks, many firms could do much more to strengthen their controls to mitigate this threat.

FINRA has observed firms implementing the following effective practices:

- Creating policies and procedures to specifically address phishing, including but not limited to identifying phishing emails; clarifying that users should not click on any links or open any attachments in phishing emails; requiring deletion of the phishing email; developing a process to securely notify IT administrators and compliance staff; confirming all requests for wire transfers with the customer via telephone or in person;[4] and ensuring proper resolution and remediation after a phishing attack.
- Including phishing scenarios in the firm-level risk assessment process;
- Establishing confirmation policies and procedures for transaction requests over a reasonable threshold (*e.g.*, for a customer money transfer to a new bank or CEO- or CFO-initiated vendor payment) to reduce the likelihood of successful spear phishing or whaling attacks;
- Implementing email scanning and filtering to monitor and block phishing and spam communication;
- Regularly training employees on phishing and related firm policies and procedures (especially for those employees in IT, Human Resources, or customer-facing functions who are more likely to be targeted because of their access to valuable personal and financial information);
- Conducting regular simulated phishing email campaigns to evaluate employee understanding and compliance with the firm's policies and procedures;
- Developing remedial training and imposing appropriate consequences for employees who repeatedly violate the firm's phishing standards or do not demonstrate sufficient sensitivity to phishing risks during the firm's simulated phishing email campaigns;
- Reviewing the firm's processes and procedures to detect and remediate a successful phishing campaign;
- Reducing the impact of a successful phishing attack by segmenting customer and other critical assets, implementing multi-factor authentication and other data loss prevention controls (*see* Data Loss Prevention (DLP) subsection of the Insider Threats section of this report below);
- Maintaining a log of phishing incidents and the firm's responses;
- Establishing a relationship with the local Federal Bureau of Investigation (FBI) office to know when and how to report cyber incidents – including but not limited to phishing attacks – to that office; and
- Reporting such attacks to cybersecurity information-sharing organizations in which they participate.[5]

Since some phishing attacks may begin with successful attacks on customers, firms may wish to direct customers to resources that may help them protect themselves from attack, for example, FINRA's *Phishing and Other Identity Theft Scams: Don't Take the Bait* (Feb. 29, 2012).

## Insider Threats

Insider threats remains a critical cybersecurity risk because an insider typically circumvents many firm controls and may cause material data breaches of sensitive customer and firm data. Whether due to malicious behavior—such as a bad actor who plans to sell customer account data on the dark web—or inadvertent error—such as a registered representative who loses his or her laptop or other storage media with unencrypted customer PII—insiders are in a unique position to cause significant harm to an organization. In response to the 2017 and 2018 FINRA Risk Control Assessment (RCA), the vast majority (95-99 percent) of higher revenue firms and 66 percent of mid-level revenue firms indicated that they address insider threats in their cybersecurity programs.

"Insiders" include individuals who currently have or previously had authorized access to firm systems and data because of their function or role and include individuals such as full and part-time employees, contract or temporary employees, consultants and interns, but they may also include employees or contractors of third-party vendors and sub-contractors.

FINRA has observed that effective insider threat programs typically integrate the following components into an overarching, risk-based insider threat program:

- Executive leadership and management support;
- Identity and access management policy and technical controls, including heightened controls, for individuals with privileged access;
- Technical controls including security information and event management (SIEM) and data loss prevention (DLP) tools, as appropriate for the scale and technological sophistication of the firm;
- Training for all insiders; and
- Measures to identify potentially abnormal user behavior in the firm's network.

A comprehensive asset inventory is also a key element of an effective insider threat program (as well as a firm's broader cybersecurity program) and we discuss this in more detail in the branch section of this report as well as FINRA's *Report on Cybersecurity Practices*.

### Executive Leadership and Management Support

FINRA has observed the following effective practices by senior executives and management:

- Demonstrating commitment to the firm's cybersecurity policy by personal compliance with its requirements;
- Designating a senior executive or manager with responsibility for the firm's insider threat controls;
- Imposing consequences for all employees violating the policy, regardless of their position or status in the organization;
- Providing timely notifications when access or privileges are changed or an employee resigns, moves to another department or is terminated; and
- Identifying behaviors of potentially malicious insiders and creating a process by which mid-level managers can address such concerns, including escalating the issue to senior leadership, adjusting or eliminating employee privileges or terminating the employee (*see* Identifying Potentially Malicious Insiders section of this report below).

## Identity Access Management and User Entitlements

Effective Identity Access Management (IAM) and user entitlements processes can serve as a first line of defense to ensure that all insider users (including contractors, consultants, interns and vendors) are assigned proper access to systems, applications, files and databases. "Proper access" requires that systems entitlements are aligned with specific job functions and assigned only on a need-to-know basis. IAM needs to cover the full lifecycle of entitlements: user on-boarding (*e.g.*, assignment to specific functions and customer accounts), transfers and promotions to new departments/functions and timely off-boarding for users leaving an organization. IAM should also support proper segregation of functions between front office and back office users (*e.g.*, individuals assigned to a trading desk should not have access to wire funds or transfer assets, while individuals assigned to perform reconciliations should not have access to update trading systems).

FINRA has observed firms implementing the following effective practices:

- Establishing and maintaining WSPs to manage the system user access lifecycle (including employee onboarding, departmental and function transfers, promotions and timely terminations of employees, contractors and vendors) where firms typically approve access according to defined procedures and use an auditable ticketing system to document those decisions;
- Conducting periodic review and certification of user entitlements (*e.g.*, annually for all employees, and semi-annually or quarterly for individuals with access to particularly sensitive information or systems or with elevated privileges) and implementing appropriate segregation of duties;
- Implementing comprehensive password policies and controls that require complex passwords, periodic password changes after a specified period of time (and old passwords cannot be re-used) and password locks after a certain number of unsuccessful login attempts;
- Disabling or changing the use of generic IDs (such as vendor-provided "default user" and "administrator" IDs and passwords used for the first time system install) to require individual IDs for each user and strong passwords; and
- Implementing policies and processes to automatically and rapidly revoke network and system access (for example, some firms establish an automated data feed from their human resource system to their identity access management system to drive the creation and removal of basic accounts (such as active directory and email accounts) based on roles).

## Privileged User Controls

Privileged users represent a potentially heightened insider threat. Typically, these users are server, network and database administrators who have access to powerful system commands and utilities that enable them to copy, delete or change any data files or system options and parameters (*e.g.*, creating new users with broad system access or elevating other users' or systems' access to firm information). These users may also be able to shut down business applications, networks and processes. In addition, individuals involved in the development, testing, deployment and maintenance of software may possess elevated system privileges. For example, developers may need to be able install software and drivers on their workstations as part of their job function. While these individuals support a firm's information technology infrastructure, their status requires firms to establish appropriate controls to ensure that they have only those privileges necessary for their job function and do not abuse their privileges.

FINRA has observed firms implementing the following effective practices:

- Establishing WSPs to require the monitoring of privileged user system access activities;
- Establishing consistent structures and processes for identifying privileged users;
- Assigning privileged users to special administrative groups and reviewing their activities to identify situations where they may engage in unapproved activities;
- Segmenting privileged users' access according to their roles, including but not limited to development, deployment and maintenance, as well as the change management process;
- Employing a password "vault" to check out one-time passwords in order to enter into an administrative session to protect against password "leakage";
- Using SIEM and other tools to collect and monitor privileged users' activity logs (discussed further below); and
- Requiring multifactor authentication for privileged user logins at all times.

## Security Information and Event Management (SIEM) and User and Entity Behavioral Analytic (UEBA) Tools

SIEM tools collect and aggregate and correlate log information from numerous sources, including but not limited to: firewalls, Intrusion Detection and Prevention systems, servers, and network devices. Firms use the aggregated log to monitor various user activities and events. A SIEM system may identify and generate alerts regarding risky activities and potential attacks so that the firm can respond to and prevent sensitive information from going outside the firm's network. In some advanced cybersecurity programs, firms use machine learning in conjunction with SIEM tools to learn and model baseline and irregular behavior, which improves the system's ability to identify potentially malicious behavior, including risky insider activities.

UEBA tools can also enhance a firm's capability to detect anomalous behaviors. Such tools focus on analyzing individual user and entity behaviors, and typically include a learning element that enables the tool, over time, to identify normal and abnormal behaviors and to flag the latter for further review.

FINRA has observed firms implementing the following effective practices:

- Establishing WSPs to require capturing of system logs[6] from sources for aggregation into a SIEM tool;
- Establishing risk-based approaches to identify high risk events, provide timely alerts and escalate events according to agreed procedures;
- Establishing procedures for timely notification when log sources stop sending data to a SIEM tool;
- Implementing behavioral analytics and other artificial intelligence systems to identify emerging trends and suspicious activities in a timely manner;
- Establishing formal change management procedures for SIEM-related rules changes; and
- Maintaining SIEM logs in order to perform historical analysis and forensics.

## Data Loss Prevention (DLP)

A strong DLP program creates preventative controls that can help to detect and mitigate insider (and other) threats. DLP controls can prevent the inadvertent or malicious transmission of sensitive customer or firm information to unauthorized recipients. DLP controls typically identify sensitive customer and firm data based on rules and then block or quarantine the transmission of the data whether by email, data upload or download, file transfer or other method. Whereas some firms maintain DLP software internally, others use vendors to support these efforts.

FINRA has observed firms implementing the following effective practices:

- Establishing a formal DLP program and applicable WSPs to monitor and prevent data breaches;
- Requiring user verification prior to permitting the sending of outbound emails;
- Establishing consistent structures and processes for capturing DLP events—such as outbound emails and attachments or file transfers containing sensitive information—and placing them into quarantine status for compliance review prior to release;
- Establishing robust DLP rules to identify and block or encrypt the transfer of data, such as customer account numbers, Social Security numbers, trade blotter information and source code (and alerting compliance via notification alerts if such rules are violated);
- Establishing rules to control printing of sensitive data and documents;
- Restricting data downloads to USB, CD drives, and SD ports and other mobile devices, as well as blocking access to personal web email programs, cloud-based file sharing service providers and social media sites;
- Implementing robust controls for employees and contractors working from home using personal computers, for example by requiring individuals to use multi-factor authentication and a secure Virtual Private Network (VPN)[7] channel for login, as well as blocking the printing, copying, pasting or saving of firm data to personally owned computers, smartphones or tablets; and
- Installing call verification systems that can potentially screen and identify incoming customer calls to ensure the numbers do not belong to known fraudsters.

## Training

As noted, many of the data breaches FINRA has observed occurred because well-intentioned employees or other users made preventable mistakes. Developing a firm culture that focuses on cybersecurity awareness and providing regular cybersecurity training can help address this problem. Effective practices FINRA has observed include firms providing ongoing—rather than one-time—training for staff on:

- Appropriate handling of customers' requests for user name and password changes, money transfers and identity verification, particularly those involving large amounts of money transferred to an overseas location or third parties;
- Sound practices regarding the opening of email attachments and links, including using simulated phishing campaigns where the firm notes and re-tests the individuals who failed the exercise; and
- Identifying social engineering activities from hackers.

A number of firms observed that using actual cases experienced by the firm or peer firms can make the training more interesting and effective for participants.

## Identifying Potentially Malicious Insiders

Malicious insider threats are particularly challenging for firms to address. Firms may be over-confident that their hiring practices will ensure "only good people are hired" and that management can identify disgruntled employees through day-to-day interaction. Moreover, malicious insiders know their organization and its weaknesses and can try to work around a firm's controls. Effective programs to identify malicious insiders typically combine people-, process- and technology-based controls. In particular, firms may monitor for non-technical behavior indicators, including but not limited to the following:

| Employment Status | Work Patterns | Personality and Personal Circumstances | Unlawful Activities |
|---|---|---|---|
| Received warning, otherwise not in "good standing" or under review for termination of employment | Change of working pattern | Drastic change in personality or behavior | Notification or evidence of criminal activity |
| Concerns about missed promotions | Unexcused or unauthorized absences | Threats of retaliation | Acts or threats of violence |
| Notification or discussion regarding leaving the company | Decline in performance | Harassment | Destruction of property |
| Searching for new jobs | Conflicts at work | Significant debt and recurring financial irresponsibility | Attempts to bypass/ defeat any security system |
| | | | Time and attendance fraud |
| | | | Falsifying reports or records |
| | | | Theft |

In addition to implementing the policy and technical measures described in the sections above, FINRA has observed firms that implement the following effective practices:

- Cultivating a strong culture of compliance that encourages confidential reporting of potentially suspicious activity (*e.g.*, "if you see something, say something"); and
- Performing regular reviews of individuals with higher risk combinations of privileges, especially in environments where it is difficult to maintain segregation of duties.

## Penetration Testing

Penetration testing (or a pen test) is an important element in many firms' cybersecurity programs. A pen test simulates an attack on a firm's internally- or externally-facing computer network to determine the degree to which malicious actors may be able to exploit vulnerabilities in the network and evaluate the effectiveness of the firm's protective measures.[8] For example, one particular type of pen test focuses on a firm's web application to evaluate its security design and associated databases (*e.g.*, a firm's public website where employees, representatives or customers log in to access account and position data, including PII or other confidential information).[9] The pen test process requires an active analysis of a firms' network, applications or other targets for any weaknesses, technical flaws, gaps or vulnerabilities. Such testing often involves both automated scanning tools and manual techniques and may include social engineering. Any identified security issues would be presented to the business owner and information technology management, together with an assessment of the impact, risk classification of findings, and a proposal for mitigation or a technical solution.

Pen tests may take the perspective of an outside attacker attempting to infiltrate a firm's system or an insider attacker trying to gain access to assets to which they should not have access. Both types of tests can be performed in different modes: (1) "White Box" mode where the test team knows something about the system such as a range of IP addresses, software packages in use or a user ID; (2) "Black Box" mode in which the test team knows nothing about the system; or (3) "Gray Box" mode where the test team has some limited information about the system.

According to FINRA's 2018 RCA, 100 percent of higher revenue firms include penetration testing as a component in their overall cybersecurity program. The utility of pen tests is less a function of firm size, however, and much more a function of a firm's business model and technology infrastructure. For example, pen tests are highly relevant to firms that provide online access to customer accounts. FINRA has observed higher, mid-level and lower revenue firms that conduct pen tests. Other factors these firms consider in evaluating the relevance of penetration testing include the degree to which they manage or store confidential or critical data such as trading strategies, customer PII, information about mergers and acquisitions or confidential information from other entities (for example, in the case of clearing firms).

FINRA has observed firms implementing the following effective practices:

- Adopting a risk-based approach to penetration testing;
- Thoroughly vetting their testing providers;
- Establishing contractual provisions that carefully prescribe vendor responsibilities;
- Rigorously managing and responding pen test results; and
- Periodically rotating testing providers to benefit from a range of skills and expertise.

### Risk-Based Approach

Many firms determined the systems to be tested and the frequency with which they should be tested based on a risk assessment where higher risk systems were tested more frequently. Factors firms considered in identifying high risk systems included the sensitivity of the data contained or accessed by that system, the operational importance of the system and the presence of any known vulnerabilities.

Also, firms with strong cybersecurity programs conducted pen tests at least annually and more frequently for mission critical, high risk systems such as for an online trading system. In addition to a calendar-based approach to testing, some also perform risk-based penetration tests after key events, such as any time a significant change is made to important elements of the firm's applications and systems infrastructure.

### Vendor Selection and Due Diligence

Firms generally used third parties to perform pen tests (even for those tests that take an "insider" view). Firms conducted thorough due diligence to select vendors with a sound knowledge of cyber risks, current attack techniques and appropriate tools to emulate the actions of an attacker. Moreover, some firms required vendors to provide an ethical hacking certification such as Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP) or GIAC Penetration Tester (GPEN) certifications prior to an engagement. Firms may alternate between providers, or use multiple providers, to maximize the likelihood of identifying issues. In some cases, firms with sufficient resources to develop this specialized skill set conducted pen tests using their own staff.

### Contractual Arrangements

Firms typically established a written contract with the vendor performing the pen test. That contract specified what the vendor should and should not do during the test, for example, which applications, systems, networks or IP addresses the vendor should test; the degree to which the vendor should attempt to exploit a system if a control is breached (*e.g.*, a firewall or user entitlements); or the time of day the pen test should take place (*e.g.*, to avoid an simulated attack during peak usage period). Contracts also typically specified vendor responsibility for non-disclosure of confidential information or findings, as well as the details the vendor would report to the firm. Pen tests took place on both an announced and unannounced basis, although in the latter case, at least some firm staff were aware of the planned timing for the test.

### Pen Test Results

Firms established governance structures and procedures to assess the risk level and determine how quickly the firm would mitigate issues identified during the pen tests. Typically firms, or the pen test vendor, assigned a risk level (*e.g.*, critical, high, medium, low); systematically tracked issues identified along with their risk level; and addressed the higher risk levels more quickly. This process was completed in accordance with prescribed policies that included escalation requirements for particularly serious risks and documentation requirements regarding the measures implemented to mitigate the vulnerability. In some cases, firms conducted a follow-up pen test to assess the effectiveness of mitigation measures adopted to address a previously identified control weakness.

## Mobile Devices

The widespread and expanding use of mobile devices creates new opportunities for attacks on sensitive customer and firm data. Employees, customers, consultants and contractors may regularly use smartphones, tablets, laptops and other devices for a variety of activities, including communication, trading, receiving investment alerts, money transfers and account monitoring.[10] As the industry becomes more reliant on mobile devices, risks associated with this technology continue to increase. Firm and personal mobile devices are exposed to risks including, but not limited to, malicious advertisements and spam communication; infected, cloned or pirated mobile applications; vulnerabilities in mobile operating systems; and phishing, spoofing or rerouting of calls, emails and text messages (*see* Phishing section of this report above). Although all firms offering access to their systems through mobile devices face such risks, firms with large numbers of retail customers may be subject to greater exposure and should consider especially rigorous implementation of cybersecurity controls to protect firm and customer information.

FINRA has observed firms implementing the following effective practices for their employees, consultants and contractors:

- Developing policies and procedures addressing employee obligations to protect customer and firm information and "bring your own device" standards for the use of personal devices for firm business;[11]
- Prohibiting the use of personal devices for firm business (including email, texting, messaging or any other communication) unless the devices have been approved by the firm, and the employee has signed an attestation agreeing to comply with the firm's policies and procedures;
- Including reviews of mobile device security controls in branch office audits and inspections, including for remote employees and branch office staff (*see* Data Loss Prevention and Branch Controls sections of this report above);
- Ensuring that firm compliance and technology support staff have sufficient expertise in mobile cybersecurity issues;
- Providing regular training to all firm employees, consultants and contractors on firm mobile device requirements and effective practices to protect mobile devices;
- Maintaining an inventory of all personal and firm devices used to access firm systems and data;
- Requiring all personal devices to maintain a separate, secure, encrypted mobile device management (MDM) application for all firm activities, including email communication, calendar and other activities;
- Enforcing the use of passwords and setting password standards for length and complexity;
- Setting time-outs after certain periods of non-usage;
- Installing security software and antivirus software to protect all mobile devices used to engage in firm business and monitor for compliance with firm security standards;
- Implementing authorization and authentication controls in "offline" mode;
- Removing all software, services and applications that violate the firm's security policy;
- Implementing transmission controls for secure transfer of data between the mobile device and the firm's servers;
- Emphasizing the importance of physically securing all personal and firm devices at all times to prevent the risk of theft or loss;
- Implementing reporting procedures for lost personal or firm devices;
- Maintaining an inventory of all lost personal and firm devices, including the type of remediation taken to reduce or eliminate the risk of exposure of firm or customer information;
- Ensuring that the firm is able to remotely wipe firm data from a device that belongs to a former employee or from a device that an employee has lost; and
- Enforcing mobile device policies and procedures by pursuing consequences for violations, including but not limited to additional training, written notices, fines, suspension, or termination of employment.

FINRA has also observed firms implementing the following effective practices for their customers:

- Monitoring mobile application markets on the dark web for malicious applications that impersonate the firm's mobile application;
- Informing customers about the risks of accessing and storing personal and financial data on their mobile devices;
- Advising customers about the risks of "jailbreaking" or "rooting" mobile devices to make them "open" for unauthorized applications, games and networking tools, which increase the risks of viruses, malicious code and unauthorized modifications to operating systems;
- Requiring multi-factor authentication for access to customer accounts and trading applications and other data loss prevention controls (*see* Data Loss Prevention (DLP) subsection of the Insider Threats section of this report above);
- Restricting certain changes to account settings, financial information or contact information via mobile device and requiring customers to contact their advisor for such requests;
- Maintaining account and trading session security by automatically terminating access after a certain period of inactivity; and
- Ensuring secure development and testing procedures when releasing or changing mobile account or trading applications (*e.g.*, scanning for security vulnerabilities and performing pen tests for mobile platforms prior to release).

## Appendix: Core Cybersecurity Controls for Small Firms

The following list identifies core controls that are likely to be relevant to many small firms' cybersecurity programs. To establish an effective program, however, firms will need to consider these measures in the context of their business model and technology infrastructure, along with other factors that should inform firms' cybersecurity programs. In addition to this report, FINRA has provided a number of cybersecurity *resources* for small firms, such as the 2015 FINRA *Report on Cybersecurity Practices* ("the 2015 Report") and FINRA's *Small Firm Cybersecurity Checklist* ("the Checklist"). Use of this list does not create a "safe harbor" with respect to FINRA rules, federal or state securities laws, or other applicable federal or state regulatory requirements.

- **Patch Maintenance.** Enable the automatic patching and updating features of operating systems and other software to help firms maintain the latest security controls (*see* Sections 4 and 5 of the Checklist).
- **Secure System Configuration.** When configuring systems and software, use vendor guidance or industry standards, such as those published by the Center for Internet Security ("CIS") (*see* Overview and Resources section of the Checklist).
- **Identity and Access Management.** Limit access to confidential customer and firm information based on business need. Tightly restrict use of "admin" or highly privileged entitlements and regularly review user accounts and privileges to modify or delete those which are no longer necessary to achieve business objectives (*see* the Insider Threats section of this report, Technical Controls section of the 2015 Report and Section 8 of the Checklist).
- **Vulnerability Scanning.** Use Commercial Off-The-Shelf ("COTS") software or third-party vendors to continuously scan for vulnerabilities and quickly address detected discrepancies (*see* the Phishing section of this report, the Cybersecurity Risk Assessment as well as Technical Controls sections of the 2015 Report and Section 10 of the Checklist).
- **Endpoint Malware Protection.** Install COTS software on firm computers, servers and firewalls to detect and block viruses and other malware (*see* the Technical Controls section of the 2015 Report and Sections 4 and 5 of the Checklist).
- **E-mail and Browser Protection.** Install software or use services to block web-based e-mail programs and unsafe content received through e-mail (*e.g.*, phishing attacks) or accessed via web browsers (*see* the Phishing section of this report and Sections 4 and 5 of the Checklist).
- **Perimeter Security.** Use network access controls, such as firewalls, to block unnecessary connectivity between firm systems and outside systems. If feasible, incorporate an Intrusion Detection and Prevention capability (*see* the Insider Threats section of this report, Technical Controls section of the 2015 Report and Sections 4, 5 and 10 of the Checklist).
- **Security Awareness Training.** Provide cybersecurity training to all employees upon their employment and at least annually thereafter (but preferably more often) to ensure all users are aware of their responsibilities for protecting the firm's systems and information. Training should address common attacks, how to avoid becoming a victim and what to do if you notice something suspicious. Consider implementing an ongoing phishing awareness campaign (*see* the Insider Threats section of this report, Staff Training section of the 2015 Report and Section 8 of the Checklist).
- **Risk Assessments.** Conduct annual risk assessments and testing of firm controls to verify effectiveness and adequacy. This assessment may be accomplished using third-party or firm security experts (*see* Cybersecurity Risk Assessment section of the 2015 Report and Sections 1 and 2 of the Checklist).

- **Data Protection.** Encrypt critical data, back it up frequently and store copies of back-ups offline. Regularly test the firm's ability to restore data. Consider blocking USB ports and use of all removable data storage devices, including CDs and flash drives (*see* Sections 4, 5, 6 and 12 of the Checklist).
- **Third-Party Risk Management.** Review System and Organization Controls (SOC) or SSAE 18 reports for third party vendors and other partners with access to confidential firm and customer data to ensure they have security controls commensurate with, or better, than the firm's. All contracts should have provisions to enforce controls to protect data, including prompt notification of any changes to those controls and vulnerabilities or breaches that may affect the firm (*see* the Vendor Management section of the 2015 Report and Section 3 of the Checklist).
- **Branch Controls.** Ensure that branches apply and enforce relevant firm cybersecurity controls, which may include many of the controls identified in this list, as well as other relevant controls such as those elsewhere in this report or in the Small Firm Cybersecurity Checklist (*see* the Branch Controls section of this report).
- **Policies and Procedures.** Create policies and procedures that address each category of controls applicable to the firm, such as those identified in this list (*see* the Governance and Risk Management for Cybersecurity section of the 2015 Report).

## Endnotes

1. On an annual basis for the past seven years, FINRA has conducted a voluntary Risk Control Assessment (RCA) Survey with all active member firms. The RCA segments firms based on their business activities and other characteristics, including, but not limited to, their revenue. In order to share some of the insights from the RCA, we provide the relevant data for firms with higher revenue, firms with mid-level revenue and firms with lower levels of revenue. The 2018 RCA shows that 95 percent of higher revenue firms maintain a branch password policy; 90 percent maintain a process for the installation of system patches across branches; 85 percent require encryption of hard drives; 79 percent implement an electronic communication usage policy; 78 percent require up-to-date virus protection; and 75 percent have network security standards.

2. According to the 2018 RCA, 60 percent of higher revenue firms maintain branch-level registered representative training requirements.

3. According to the 2018 RCA, 94 percent of higher revenue firms and 70 percent of mid-level revenue firms use a risk assessment as part of their cybersecurity program.

4. *See FINRA Regulatory Notice 09-64* for additional information on verifying instructions to transmit or withdraw assets from customer accounts.

5. One example of such an organization is the Financial Services – Information Sharing and Analysis Center (FS-ISAC).

6. "System logs" refers to data stored that creates an audit trail of events that occur on, and tasks performed by, a computer's hardware and software.

7. A VPN provides a secure, encrypted communications channel between a remote user over a public network, typically the internet, and a company's secure network.

8. Pen tests are distinct from "vulnerability assessments." The latter are typically performed on a routine basis, in some cases daily, using automated tools – such as web and network scanners – and look across multiple firm systems. An example of vulnerability scanning may include checking servers for security patches to ensure they are current.

9. In response to FINRA's 2016 and 2018 RCAs, 89 percent of higher revenue firms, 71 percent of mid-level revenue firms and 47 percent of lower revenue firms reported that they manage or store confidential customer information. Accordingly, all firms should recognize their need to monitor and safeguard confidential customer data.

10. According to the 2018 RCA, 55 percent of higher revenue firms and 28 percent of mid-level revenue firms provide retail customers access to their accounts via a website browser on a mobile device and 35 percent of higher revenue firms and 14 percent of mid-level revenue firms provide such access via mobile apps.

11. According to the 2018 RCA, 93 percent of higher revenue firms maintain a firm-wide mobile device policy and 29 percent maintain a branch-specific mobile device policy.

**Investor protection. Market integrity.**

1735 K Street, NW
Washington, DC 20006-1506

www.finra.org


18_0299.1 –12/18