Insider Threats – Effective Controls and Practices

Cybersecurity, and data privacy and protection, are key operational risks facing firms that will likely only grow in significance in the coming years. As the frequency, sophistication and variety of cybersecurity incidents continue to increase, the emerging risks posed by insider[1] threats may harm investors, member firms and the markets.

This publication updates and expands on our guidance on insider threats in FINRA's Report on Selected Cybersecurity Practices – 2018 (the 2018 Report) by outlining the factors behind insider threat risks and helping member firms identify, prevent, detect and respond to insider threats, including:

- identifying how insider threats can occur at firms, and what factors may indicate that these incidents are on the rise;
- providing a summary of effective controls and practices firms may consider when evaluating their insider threat programs, including questions to assist firms with addressing such threats; and
- providing appendices with a glossary of relevant terms and FINRA publications that provide additional information on effective cybersecurity practices.

Increasing Insider Threat Risks

Insider threats have been an ongoing focus for FINRA and member firms, and we have observed these incidents may become more prevalent, in part due to:

- Industry-wide trends that may decrease employees' satisfaction and engagement with their positions at their firms (*e.g.*, reductions in workforce and bonuses, increases in employee turnover); and
- High demand for employees with a background in critical cybersecurity fields (*e.g.*, information technology), which may impact firms' ability to hire adequately skilled and experienced applicants to effectively safeguard against insider threat incidents.

This publication does not create new legal or regulatory requirements or new interpretations of existing requirements, nor does it relieve firms of any existing obligations under federal securities laws and regulations. Member firms may consider this information in developing new, or modifying existing, practices that are reasonably designed to achieve compliance with relevant regulatory obligations based on the member firm's size and business model.

Contact Us

Questions related to this or other Cybersecurity topics can be sent to Member Supervision's Cyber and Analytics Unit (CAU) team at cybertech@finra.org.

[1] "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. Insiders may also include employees or contractors of vendors and sub-contractors.

Background and Discussion

Insider threats remain a critical cybersecurity risk because firms typically provide insiders with access that can circumvent many firm controls and may potentially cause material data breaches of sensitive customer and other firm data. Whether due to malicious behavior—such as bad actors who may sell customer account data on the dark web—or inadvertent error—such as registered representatives who lose their laptops or other storage media with unencrypted customer personally identifiable information (PII)—insiders are in a unique position to cause significant harm to a member firm and its customers.

Regulatory Obligations

Rule 30 of the U.S. Securities and Exchange Commission's (SEC) Regulation S-P requires firms to adopt written policies and procedures that are reasonably designed to insure the security and confidentiality of customer records and information, protect against any anticipated threats or hazards to that security or integrity, and protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. In addition, FINRA Rule 4370 (Business Continuity Plans and Emergency Contact Information) requires members to create and maintain a written business continuity plan identifying procedures relating to an emergency or significant business disruption, which may include denial of service attacks or other cyberattacks.

In addition to potential harm to individuals if PII or other information is compromised, cybersecurity incidents, such as insider threat incidents, and any related exposure of customer information or fraudulent financial activity can expose member firms to financial losses, reputational risks and operational failures that may compromise firms' ability to comply with a range of rules and regulations – including SEC Regulation S-P Rule 30, FINRA Rules 3110 (Supervision), 3120 (Supervisory Control System), and 4370 (Business Continuity Plans and Emergency Contact Information), as well as Exchange Act Rules 17a-3 and 17a-4.[2]

EFFECTIVE CONTROLS AND PRACTICES

The following are effective controls and practices observed by FINRA as part of some firms' holistic systems of administrative, detective and preventative controls to manage insider threat risks, as well as relevant questions for consideration firms could use to evaluate their current insider threat programs. (Additional information on these and other controls and practices related to cybersecurity—such as FINRA *Notices*, Reports on Cybersecurity Practices and Compliance Tools—can be found in the Appendix.)

1 EXECUTIVE LEADERSHIP

☐ Reviewed ✔

Active executive management—and, as appropriate to the firm, board-level involvement—is an important effective practice to address insider threats because leaders should regularly engage with relevant cybersecurity experts and discuss how to manage the risk posed by insider threats. Firms may consider asking the following questions, where applicable, with respect to how their executive leadership implements and holds themselves accountable to their firm's internal threat program:

[2] On March 15, 2023, the SEC proposed changes to Regulation S-P and Regulation Systems Compliance and Integrity (SCI). *See* Exchange Act Rel. No. 97141 (March 15, 2023), 88 FR 20616 (April 6, 2023), and Exchange Act Rel. No. 97143 (March 15, 2023), respectively. The SEC also proposed a new cybersecurity risk management rule for broker-dealers, clearing agencies, major security-based swap participants, the Municipal Securities Rulemaking Board, national securities associations, national securities exchanges, security-based swap data repositories, security-based swap dealers, and transfer agents. *See* Exchange Act Rel. No. 97142 (March 15, 2023), 88 FR 20212 (April 5, 2023). As of the publication date of this resource, the SEC has not adopted these proposals.

- How does your firm's executive leadership demonstrate commitment to the firm's cybersecurity policy?
- What are the consequences for violating your firm's cybersecurity policies and procedures? Are all employees subject to these consequences, regardless of their position or status?
- What senior executive or manager is responsible for your firm's insider threat controls? Do their responsibilities include:
    - ensuring timely notifications when access or privileges are changed, or an employee resigns, moves to another department or is terminated;
    - establishing a clear and comprehensive process for sharing information related to mitigating and reporting insider threats; and
    - identifying behaviors of potentially malicious insiders and creating a process by which midlevel managers can address such concerns, including:
        - escalating the issue to senior leadership;
        - adjusting or eliminating employee privileges; or
        - terminating the employee?

2 IDENTITY ACCESS MANAGEMENT AND USER ENTITLEMENTS

☐ Reviewed ✔

Effective Identity Access Management (IAM) and user entitlements processes serve as a first line of defense to ensure that all insiders, such as employees, contractors, consultants, interns and vendors, are assigned proper access to systems, applications, files and databases.[3] These processes cover the full lifecycle of user entitlements and support proper segregation of functions between front-office and back-office users (*e.g.*, individuals assigned to a trading desk not having access to wire funds or transfer assets; individuals assigned to perform reconciliations not having access to update trading systems). Firms may consider asking the following questions, where applicable, when implementing or evaluating their IAM and user entitlements processes:

- Does your firm follow the Principle of Least Privilege[4] when granting user access?
- Does your firm maintain written supervisory procedures (WSPs) to support the Principle of Least Privilege and manage the system user access lifecycle? If so, do they address, for example:
    - employee onboarding;
    - departmental and function transfers; and
    - promotions and timely terminations of employees, contractors and vendors?
- Does your firm use an auditable ticketing system to document all decisions related to access approval?
- Does your firm review and certify user entitlements on a consistent schedule (*e.g.*, annually for all employees; semi-annually or quarterly for individuals with access to particularly sensitive information or systems or with elevated privileges) as well as implement an appropriate segregation of duties?

[3] In this context, "proper access" means aligning systems entitlements with specific job functions and assigning these entitlements only on a need-to-know basis.

[4] As defined in the Appendix 1 Glossary, the Principle of Least Privilege is the information security practice that any user, program or process is given the minimum privileges necessary to perform a function.

- How strict are your firm's policies and controls regarding employee logins? Do they disable or change the use of generic IDs (*e.g.*, vendor-provided "default user" and "administrator" IDs used for the initial system install) and require individual IDs for each user?
- How comprehensive are your firm's policies and controls regarding employee passwords? For example, do they:
    - require complex passwords;
    - require periodic password changes after a specified period of time;
    - prohibit the re-use of previous passwords; and
    - allow a limited number of unsuccessful login attempts before locking users out of their account?
- Has your firm implemented policies and processes to automatically and rapidly revoke network and system access (*e.g.*, an automated data feed from a firm's human resources system to their IAM system?
- Has your firm adopted practices and tools to review employee and contractor access to identify or prevent unusual access or activities (*e.g.,* accessing critical systems late at night; copying or printing customer or firm data during an unusual access session)?

3 PRIVILEGED USER CONTROLS

☐ Reviewed ✔

"Privileged users" represent a potentially heightened insider threat because 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). Similarly, individuals involved in the development, testing, deployment and maintenance of software may possess elevated system privileges. While these individuals constitute a core element of firms' information technology infrastructure, their status requires firms to limit their access and controls to only those privileges necessary for their job function and prevent any risks that they may abuse their privileges by, for example, shutting down business applications, networks and processes. Firms may consider asking the following questions, where applicable, when implementing or evaluating their privileged user controls:

- What WSPs has your firm established to monitor the use of privileged users' system access activities?
- Has your firm established consistent processes regarding privileged users' system access to:
    - identify privileged users;
    - assign privileged users to special administrative groups and monitor their systems use for situations where they may engage in unapproved activities; and
    - segment privileged users' access according to their roles (*e.g.*, development; deployment and maintenance; change management)?
- What controls related to privileged users' system access has your firm implemented, for example:
    - a password "vault" to check out one-time passwords in order to enter into an administrative session (while protecting against password "leakage");
    - allowing access to privileged accounts only when a valid corresponding approved change request is confirmed;
    - multi-factor authentication (MFA) for all privileged user logins[5]; and

[5] *See Regulatory Notice 21-18* (FINRA Shares Practices Firms Use to Protect Customers From Online Account Takeover Attempts) for more information related to MFA.

- tools to collect and monitor privileged users' activity logs (examples discussed below)?

4 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) AND USER AND ENTITY BEHAVIORAL ANALYTICS (UEBA) TOOLS

☐ Reviewed ✔

SIEM tools collect, aggregate and correlate log information from numerous sources—such as firewalls, intrusion detection and prevention systems, servers, and network devices—to monitor various user activities and events. A SIEM system—in some cases, in conjunction with machine learning capabilities—may identify and generate alerts regarding risky or unusual activities and potential incidents so that the firm can respond to and prevent sensitive information from leaving the firm's network. UEBA tools can also enhance a firm's capability to detect anomalous behaviors. These tools focus on analyzing individual user and entity behaviors, and typically include a machine learning element that enables the tool, over time, to differentiate normal and abnormal behaviors and to flag the latter for further review. Firms may consider asking the following questions, where applicable, when establishing or implementing SIEM or UEBA tools or procedures:

- Has your firm established WSPs to require capturing of system logs from sources for aggregation into a SIEM tool (as well as procedures for timely notification when log sources stop sending data to a SIEM tool)?
- Does your firm maintain SIEM logs in order to perform historical analyses and forensics?
- What are your firm's formal change management procedures for SIEM-related rules changes?
- Does your firm have processes to track and correlate suspicious activities over time to help manage insider threat risk, such as SIEM and UEBA systems?

While some smaller firms may not be able to adopt full-fledged SIEMs and UEBA systems, they may consider procedures and controls to otherwise identify and respond to unusual activities in the environment, such as:

- monitoring unusual system access or activities by employees or third-party IT providers;
- leveraging email system data loss prevention (DLP) controls to scan outbound emails for sensitive customer and firm information; and
- preventing unauthorized copying of critical information stored in the firm's systems.

5 DATA PROTECTION

☐ Reviewed ✔

Customer and firm data protection is another integral part of a firm's insider threat program because protecting information assets helps prevent harm to both a firm's customers and the firm's reputation. Strong DLP controls can 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; they can also prevent the inadvertent or malicious transmission of sensitive customer or firm information to unauthorized recipients. Firms may consider asking the following questions, where applicable, with respect to how they establish WSPs and controls to protect sensitive customer and firm data:

- Has your firm established formal DLP controls and applicable WSPs to monitor and prevent data breaches, addressing areas including:

    - consistent structures and processes for capturing DLP events – *e.g.*, outbound emails, attachments or file transfers containing sensitive information – and then placing them into quarantine status for compliance review;
    - robust rules for identifying, and blocking or encrypting, the transfer of data, such as:
        - customer account numbers;
        - Social Security numbers;
        - trade blotter information;
        - source code; and
    - notification alerts sent to a firm's compliance department if DLP rules are violated?
- How regularly does your firm update its anti-virus and malware policies?
- Has your firm identified where sensitive information is stored and transmitted?
- Does your firm have a policy regarding the ability to print sensitive data and documents?
- What is your firm's policy regarding storing sensitive data on removable media or personal devices, as well its retention and secure disposal?
- Does your firm restrict 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?
- What controls has your firm implemented for employees and contractors working remotely using personal computers, for example:
    - requiring individuals to use MFA and a secure Virtual Private Network (VPN) channel for logins; and
    - blocking the printing, copying, pasting or saving of firm data to personally owned computers, smartphones or tablets?
- How does your firm implement encryption for confidential data at rest or in transit?
- Does your firm validate the recipient(s) of all outbound emails before allowing them to be sent?
- Has your firm installed call verification systems that can potentially screen and identify incoming customer calls (to ensure the numbers do not belong to known fraudsters)?
- Are the systems where you store, use or transmit PII or firm sensitive data password protected? If so, have you reset from the default password?
- Does your firm have a process to notify regulators and customers about data breaches, when required?

6 IDENTIFYING MALICIOUS INSIDERS

☐ Reviewed ✔

Malicious insider threats are particularly challenging for firms to address. Firms may be overconfident 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. Firms may want to consider asking the following questions, where applicable, with respect to how they identify malicious insiders:

- Does your firm cultivate a strong culture of compliance that encourages confidential reporting of potentially suspicious activity (*e.g.*, "if you see something, say something")?
- How often does your firm monitor and review the activity of individuals with privileges that give them access to particularly sensitive systems or information (especially in environments where it is difficult to maintain segregation of duties)?

- Does your firm monitor for non-technical behavioral indicators that could indicate an employee potentially represents an insider threat, including:
    - uncertain or unstable employment status (*e.g.*, signs that employees are not in "good standing" with their firm, such as official warnings or placing them under review for termination; employee concerns about missed promotions; notifications or discussions regarding leaving the firm; indications that employees are searching for new positions outside of the firm);
    - concerning work patterns (*e.g.*, unexcused or unauthorized absences; decline in job performance; conflicts at work; working odd or unusual hours, either remotely or on-site);
    - personal circumstances (*e.g.*, drastic change in personality or behavior; threats of retaliation; harassment; significant debt and recurring financial irresponsibility); and
    - unlawful activities (*e.g.*, destruction of property; attempts to bypass firm security system; submitting false reports, records, or time and attendance information)?
- Does your firm monitor technical employee behavior for red flags that could represent known threat indicators, including:
    - using a new, unapproved personal device, such as a phone or laptop, without coordinating with IT;
    - submitting requests to access drives, documents or applications that the employee did not need previously;
    - showing new or unusual interest in the firm's security tools, policies or procedures; and
    - contributing to surges in network traffic that may indicate a data download or transfer?

7 ASSET INVENTORIES

☐ Reviewed ✔

Asset inventories are a key element of a firm's insider threat program because they outline what assets firms have, what assets are authorized to be on their network and what assets are most important to protect. Firm employees may not be aware of the locations where they store sensitive customer or firm data; use unapproved software, hardware or third-party vendor-provided services; or not comply with other firm cybersecurity standards. 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. Firms may want to consider asking the following questions, where applicable, with respect to how they manage their asset inventories:

- Has your firm identified its sensitive customer and firm information, and the location(s) where such information is stored?
- Does your firm perform initial and recurring inventories of its assets, and update its records with any changes?
- What are your firm's processes for managing and reporting lost or stolen assets?
- Are your firm's operating systems properly supported and maintained, either by the firm or by vendors?
- Does your firm provide secured asset disposal to its employees (*e.g.*, destroying hard drives of computers no longer in use)?

8 VENDOR MANAGEMENT

☐ Reviewed ✔

Firms across many industry sectors rely on vendors for a range of services; however, these same vendors can also be a significant source of insider threat risk. These risks can arise in different ways, for example, if:

- a vendor or one of its employees misuses firm data or systems;
- the vendor itself is subject to a cyberattack that compromises vendor systems or firm data; or
- an attack on a vendor becomes a vector for an attack on a firm's systems.

Consequently, firms should consider implementing effective vendor management programs to help guard against these risks.[6] Firms may consider asking the following questions, where applicable, with respect to how they select, conduct due diligence on and document relationships with cybersecurity vendors:

- Does your firm have a process for its decision-making on outsourcing, including the selection of cybersecurity vendors?
- Does your firm implement risk-based due diligence on vendors' cybersecurity practices critical to managing risks present in a firm's environment, including the ability to protect sensitive firm and customer non-public information?[7]
- How does your firm ensure that vendors involved in maintaining or storing sensitive information have reasonable data protection safeguards and cybersecurity controls? Are their data protection responsibilities mutually agreed upon?
- Do your firm's contracts with vendors define "breach"—in the context of data and systems the vendor is involved with—as well as address 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?
- Does your firm document relationships with vendors in written contracts that clearly define all parties' roles and responsibilities related to cybersecurity, such as evidencing compliance with federal and state securities laws and regulations, and FINRA rules; protection of sensitive firm and customer information; and notifications to your firm of cybersecurity events, and the vendor's efforts to remediate those events?
- Does your firm conduct independent, risk-based reviews to determine if vendors have experienced any cybersecurity events, data breaches or other security incidents? If so, does your firm evaluate the vendors' response to such events?
- Does your firm follow the Principle of Least Privilege by ensuring that vendors only have access to the data or parts of your firm's systems that they need to perform their functions?
- Does your firm immediately terminate vendors' access to firm systems when their contract has expired (or they are otherwise no longer doing business with the firm)?

[6] Firms can find relevant guidance in *Regulatory Notice* 21-29 (FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors) and Cybersecurity and Infrastructure Security Agency's (CISA) Risk Considerations for Managed Service Provider Customers.

[7] *See Regulatory Notice* 21-29 (FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors) at Section II for steps small firms can take when performing due diligence (*e.g.*, talking to industry peers; collecting and reviewing American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 2 reports, if available).

9 TRAINING

☐ Reviewed ✔

Many of the data breaches FINRA has observed at member firms 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. Firms may want to consider asking the following questions, where applicable, with respect to how they train employees on insider threat awareness:

- Does your firm provide ongoing—rather than one-time—training for staff on effective practices to prevent insider threat incidents, such as:
    - the appropriate handling of customers' requests for username 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?
- Does your firm provide ongoing training for managers on effective practices to identify and respond to potential insider incidents, such as:
    - being aware of employee behavior insider threat indicators and appropriate responses;
    - monitoring the environment to identify red flags that indicate an insider is engaging in malicious or harmful activities; and
    - responding to a suspected insider threat, including who to contact within the firm?
- Does your firm's training include case studies based on real-life scenarios experienced by the firm (or peer firms)?
- Does your firm's training cover password hygiene (*e.g.*, selecting complex passwords for accounts with the firm)?

Appendix 1 – Glossary

Data Loss Prevention (DLP) – a set of technologies, products and techniques that prevent end users from moving key information outside the firm's network.

Identity Access Management (IAM) – the security discipline that makes it possible for the right entities to use the appropriate resources (*e.g.*, applications, data) when they need to, without interference, using their preferred devices.

Multi-Factor Authentication (MFA) – an authentication method that requires a user to provide two or more verification factors to gain access. Verification factors include something you know (password), something you have (token), something you are (biometrics) or somewhere you are (geolocation).

Personally Identifiable Information (PII) – data or information that allows the identity of an individual to be directly or indirectly inferred.

Principle of Least Privilege – the information security practice that any user, program or process is given only the minimum privileges necessary to perform a function.

Security Information and Event Management (SIEM) – a technology that aggregates log data, security alerts and events into a centralized platform to provide real-time analysis for security monitoring.

User and Entity Behavioral Analytics (UEBA) – a cybersecurity process that uses algorithms and machine learning to model the typical behavior of participants on a network, in order to detect anomalies that could represent signs of a cyberattack.

Appendix 2 – Additional Resources

FINRA Resources

Guidance

- *Regulatory Notice* 22-29 (FINRA Alerts Firms to Increased Ransomware Risks)
- *Regulatory Notice* 21-29 (FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors)
- *Regulatory Notice* 21-18 (FINRA Shares Practices Firms Use to Protect Customers From Online Account Takeover Attempts)

Reports

- 2023 Report on FINRA's Examination and Risk Monitoring Program – Cybersecurity and Technology Governance
- Report of Selected Cybersecurity Practices – 2018
- Report on Cybersecurity Practices – 2015

Compliance Tools and Other Resources

- Core Cybersecurity Threats and Effective Controls for Small Firms
- Small Firm Cybersecurity Checklist
- Firm Checklist for Compromised Accounts
- Cybersecurity Topic Page
- Compliance Vendor Directory

Non-FINRA Resources

- CISA Insider Threat Mitigation
- Other Non-FINRA Cybersecurity Resources