Regulatory Notice 22-29

Ransomware

FINRA Alerts Firms to Increased Ransomware Risks

Summary

FINRA has received reports about increasing numbers and sophistication of ransomware incidents. Ransomware typically involves bad actors gaining unauthorized access to firm systems and encrypting or otherwise accessing sensitive firm data or customer information, then holding that hijacked data for ransom. Some ransomware attacks have become significant threats that include theft of data and bad actors' ongoing network access.

Ransomware attacks have proliferated due to, in part, increased use of technology and continued adoption of cryptocurrencies, which bad actors use to hide their identities when collecting ransom payments. Further, Ransomware-as-a-Service (RaaS) models, where bad actors purchase attack services on the dark web[1], have helped execute attacks on a much larger scale and make attacks available to less technologically savvy bad actors.

Rule 30 of the U.S. Securities and Exchange Commission's (SEC) Regulation S-P requires firms to have written policies and procedures that are reasonably designed to safeguard customer records and information. FINRA Rule 4370 (Business Continuity Plans and Emergency Contact Information) also applies to ransomware attacks that include denials of service and other interruptions to members' operations.

This *Notice* provides questions firms can use to evaluate their cybersecurity programs in light of the increased ransomware threat, lists possible additional firm controls and provides relevant resources.

This *Notice*, including the questions for consideration, 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 the information in this *Notice* 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. Moreover, some questions may not be relevant due to certain firms' business models, size or practices.

Questions regarding this *Notice* should be directed to cybertech@finra.org.

FINRA

December 14, 2022

Notice Type
- Guidance

Suggested Routing
- Compliance
- Cybersecurity
- Information Technology
- Legal
- Operations
- Risk Management
- Senior Management

Key Topics
- Business Continuity Planning
- Customer Nonpublic Information
- Cybersecurity
- Internal Controls
- Supervision

Referenced Rules
- FINRA Rule 4370
- FINRA Rule 4530
- Regulation S-P Rule 30

Background and Discussion

Ransomware, a type of highly sophisticated malware, can quickly impair firms' business operations and expose firms to risks of data theft or publication (on the dark web or publicly available internet) to coerce a ransom payment. The malware encrypts firms' files, databases and applications to prevent firm employees from accessing them until the firms pay a ransom to the bad actors. In addition to encrypting sensitive data, bad actors may copy firms' data to a storage location on the internet, leading to breaches that could result in reputational harm, federal and state legal and regulatory consequences, and significant financial costs. Bad actors exploit firm systems through phishing, as well as several common attack types that capitalize on known system vulnerabilities (including aging systems), inadequate remote-access controls and compromised login credentials. Ransomware threats may impact firms' internal networks, as well as data stored by their cloud service providers and third parties, and in mobile devices and related mobile applications.

Ransomware attacks have grown in frequency, sophistication and scope in recent years because they are profitable, relatively easy to execute compared to other attacks and often use cryptocurrency payment methods that allow bad actors to hide their identities. As firms become increasingly reliant on digital infrastructures, some have become more willing to pay ransoms to minimize downtime in operations, thereby increasing bad actors' incentives to pursue ransomware compared to other strategies. Bad actors continue to increase their use of ransomware for cybersecurity attacks and RaaS has made ransomware attacks more accessible for less technologically savvy bad actors because they can rely on others for assistance. Further, bad actors using ransomware—including sophisticated cyber criminals, organized crime syndicates and state actors—have increasingly targeted small and mid-size firms.

Common Attack Types and Considerations for Firms' Ransomware Threat Defenses

The broad scope and complexity of ransomware attacks require firms to implement strategies that include maintaining security with multiple layers of defense. Firms may use the following questions to evaluate their cybersecurity controls addressing ransomware risks. This *Notice's Appendix 1—Ransomware Controls* provides additional information regarding controls.

- **Governance and Risk Assessment.** Do your firm's policies and procedures clearly define responsibilities for cybersecurity controls and related breaches, including ransomware attacks? Does your firm require staff to report ransomware risks, as well as related steps to address those risks, to senior management? Does your firm use tools, such as penetration testing and vulnerability scanning, to support your firm's risk assessment?

- **Asset Management Inventory.** Does your firm maintain a comprehensive inventory of its hardware, software, data and applications? As part of your firm's inventory and related reviews, has your firm identified and addressed any at-risk hardware or software that are vulnerable to a ransomware attack?
- **Technical Preventive and Detective Controls.** Does your firm prioritize implementing controls on commonly targeted systems and devices?
  - Does your firm require multi-factor authentication to access firm systems or devices? Has the firm evaluated its capabilities to detect and block sophisticated attacks using tools, such as endpoint detection and response, a host-based intrusion detection system and a host-based intrusion prevention system?
  - Is sensitive data encrypted to prevent it from being readable if a bad actor copies this information outside of your firm's network as part of a ransomware attack?
  - Has your firm enabled the latest tools to restrict or limit access to firm systems, such as PowerShell and logging, restricting access to Remote Desktop Protocol services and access for admin tools, as well as using a file server resource manager (with restrictions on writing ransomware extensions)?

Ransom Payment Risks

Paying ransom demands does not guarantee a return to normal operations for firms. FINRA has observed instances where firms pay ransoms, but fraudsters:

- failed to provide, or only provided a portion of, the promised recovery keys to decrypt and recover the firms' files and data; and
- completed subsequent successful ransomware attacks shortly after the initial attack and demanded additional ransom payments.

In the event of a ransomware attack, FINRA reminds firms that FinCEN has issued guidance describing when broker-dealers and other financial institutions must file Suspicious Activity Reports (SARs) and immediately notify law enforcement of ransomware incidents. Firms should also consult Office of Foreign Assets Control's (OFAC) guidance when making or facilitating a ransomware payment may violate sanctions regulations.

- **Social Engineering and Phishing.**[2] Does your firm address social engineering and phishing risks for firm staff, including:
  - Addressing such risks in your firm's policies and procedures or by, for example:
    - identifying phishing emails;
    - clarifying that staff should not click on any links or open any attachments in phishing emails;
    - requiring deletion of phishing emails;
    - developing a process to securely notify Information Technology (IT) administrators or compliance staff of phishing attempts; and
    - ensuring proper resolution and remediation after phishing attacks?
  - Training firm staff on such threats, tactics and procedures used by bad actors and regularly conducting phishing email campaign simulations to evaluate employee understanding of and compliance with your firm's phishing policies and procedures?
  - Implementing email scanning and filtering to monitor and block phishing and spam communication, including blocking known malicious sites and ransomware files, unmasking URLs, and noting risk and reputation ratings and previews of the target pages; and
  - Maintaining controls to review and approve access requests, particularly those made through customer service channels?
- **Third-Party Vendors.** Does your firm have procedures to evaluate and, as appropriate, test vendors' cybersecurity controls, including the vendor's ability to protect sensitive firm and customer nonpublic personal information?
  - Does your firm establish written contractual terms with vendors appropriate to the sensitivity of the information to which the vendor has access and which govern the ongoing relationship with the vendor and the vendor's responsibilities after the relationship ends?
  - Are vendors required to notify the firm of cybersecurity events and their 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 for firm and customer impact?

- **Branch Controls.** Does your firm require a minimum set of cybersecurity controls for all locations, including branch and non-branch locations? How does your firm verify and monitor compliance with these controls?
  - Does your firm require that branch and non-branch locations use firm-approved vendors or vendors meeting specified standards?
  - How does your firm address risks for any branch and non-branch locations that purchase their own hardware or software?
  - Does your firm require branch and non-branch locations to conduct virus scans and software security patching and encrypt laptops and other devices?
  - For locations connecting remotely to your firm systems, does your firm require a Virtual Private Network (VPN) connection or use a Mobile Device Management tool that enforces hygiene requirements on "Bring Your Own Device" devices connecting remotely to your firm?
  - Does your firm require branch and non-branch locations to regularly back up data, including requiring that these backups are not connected the existing branch technology environment?
  - Does your firm provide training to branch and non-branch staff to address identifying and reporting potential ransomware incidents?
- **Backups and Recovery.** Does your firm keep offline encrypted backups of systems and data, which are not connected to the primary data source, to prevent bad actors from locking up the back-up data with the primary data? Does your firm test its data recovery capabilities and backup processes on a regular basis, such as those referenced in the firm's business continuity (BCP), disaster recovery or incident response plans (IRP)?
- **Incident Response.** Does your firm's IRP address potential ransomware attacks? If so, does your plan include:
  - prioritizing higher impact incidents, such as ransomware attacks—which may be followed by a Distributed Denial of Service (DDoS) attack, or simultaneous attacks, which can distract your firm's IT or cybersecurity resources—rather than remediating all attacks, regardless of risk level, in sequential or chronological order;
  - engaging cybersecurity experts to conduct forensics investigations and to assist in recovery efforts;
  - assessing and mitigating the impact of these attacks;
  - notifying affected parties (*e.g.,* customers, employees, regulators, law enforcement) as required by data breach notification laws applicable to your firm;
  - filing SARs on ransomware activity; and
  - if applicable, making cybersecurity insurance claims?

Reporting Ransomware Attacks

In addition to making any required immediate notifications to law enforcement and SAR filings, FINRA urges firms to protect customers and other firms by immediately reporting ransomware attacks to:

- FINRA's Regulatory Tip Form found on FINRA.org;
- U.S. Securities and Exchange Commission's tips, complaints and referral system or by phone at (202) 551-4790;
- the Federal Bureau of Investigation's (FBI) tip line at (800) CALL-FBI (225-5324) or a local FBI office;
- the Internet Crime Complaint Center for cyber-crimes (particularly if a firm is trying to recall a wire transfer to a destination outside the United States);
- Office of Foreign Assets Control, if there is any reason to suspect the cyber actor demanding ransomware payment may be sanctioned or otherwise have a sanctions nexus;
- local state securities regulators; and
- local law enforcement.

Firms should also consider whether ransomware attacks may require firms to report the event pursuant to FINRA Rule 4530 (Reporting Requirements).

Appendix 1—Ransomware Controls

Firms have implemented the following technical controls to address ransomware risks relevant for their operations, customer base and technology infrastructure. FINRA expects firms to develop and maintain reasonably designed cybersecurity programs and controls that are consistent with their risk profile, business model and scale of operations; however, there should be no inference that FINRA requires firms to implement any specific practices described in this *Notice*.

Control	Description
Adaptive Monitoring and Tagging	Ongoing monitoring and adaptive technology include active tagging of workloads, threat hunting, virus assessments and consistent evaluation of traffic for mission-critical applications, data or services.
Advertisement Blocks	Blocking advertisement pop-ups on all devices and browsers via extensions to address risks relating to malicious advertisements.
Anti-Ransomware Software Updates	Consistent updating of network software to address emerging ransomware risks, including updating existing intrusion detection and prevention system (IDPS), antivirus and anti-malware.
Anti-Spam Filter	Effective spam filters block malicious emails sent to firm employees. Content based dynamic spam filters offer protection against new and emerging spam techniques.
Bring-Your-Own-Device (BYOD) Policy	A BYOD policy allows firm employees to use their personal devices (*e.g.,* computers, smartphones, tablets) to access the firm's network, such as enterprise mobility management.
Cloud Access Security Broker (CASB)	CASBs help manage policy enforcement for firms' cloud infrastructure and provide added visibility, compliance, data security and threat protection in securing firms' data.
Data Loss Prevention (DLP)	A set of technologies, products, and techniques that prevent end users from moving key information outside the firm's network.
Desktop Extensions	Blocking extensions protects firms' authentication of usernames and passwords, prevents web browsing activity trackers and limits malicious messages that may be added into frequently visited web pages. Extensions may include third-party applications hosted in the cloud that are "watching" trade activities and may conduct identity theft and, as a result, induce trade transactions that may appear as insider trading. Displaying extensions and training staff not to open executable files with a ".exe" extension may also mitigate this threat.

Email Gateway	Updating secure web gateway helps firms monitor email attachments, websites and files for malware and provides visibility into potential attacks.
Endpoint Detection and Response Tools	Integrated endpoint security solutions that combine real-time continuous monitoring and collection of endpoint data with rules-based automated responses and analysis capabilities.
Executable File Blocks	Preventing all ".exe" files from launching until they have been quarantined and deemed safe helps address risks relating to executable files on the internet, which may include malicious executable code, trojans and viruses that can lock down firms' networks.
Forensic Analysis	After any detection of ransomware, investigations include its entry point and time in the environment, as well as confirming that it has been fully removed from all network devices.
Host-Based Intrusion Detection System and Host-Based Intrusion Prevention System	Software that protects computer systems from malware and other unwanted, negative activity utilizing advanced behavioral analysis and the detection capabilities of network filtering to monitor running processes, files, and registry keys within an operation system.
Inventory Tools	Inventory tools help firms identify their most valuable assets or network segments, understand how bad actors could infiltrate firm networks, provide visibility into traffic flows and identify what segments need added protection or restrictions.
JavaScript File Blocks	Disabling Windows Script Host and reviewing all readme.txt., .exe and .zip files on a regular basis prevents ransomware from infecting all internal brokerage and third-party order entry and clearing systems.
Managed Service Providers	Third-party companies that remotely manage a customer's IT infrastructure and end-user systems.
Multi-factor Authentication (MFA)	An authentication method that requires a user to provide two or more verification factors to gain access, such as something you know (*e.g.,* password), something you have (*e.g.,* token), something you are (*e.g.,* biometrics) or somewhere you are (*e.g.,* geolocation).

Microsegmentation	Strict policies at the application level, segmentation gateways and next generation firewalls (NGFWs) can prevent ransomware from reaching firms' most sensitive systems or data.
Patching	Regular software updates with the latest security patches help prevent ransomware and other cybersecurity attacks because they address the latest threats.
Ransomware as a Service (RaaS)	A service provided by experienced ransomware bad actors to other ransomware users, where the experienced actors receive compensation for developing or launching ransomware attacks developed by the operators.
Rapid Response Testing	Preparing to restore systems and data recovery quickly by pre-assigning roles and ensuring a plan is in place.
Restricted Privilege	Periodic user access reviews limit the scope of any successful ransomware attacks to the compromised user's scope of access.
Sandbox Testing	Testing new or unrecognized files using sandboxes, which provide a safe environment that is disconnected from firms' networks.
Service Level Agreement	A contract between a service provider and a customer that identifies the types of provided services, and the standards the customer expects the service provider to meet.
Zero Trust Approach	Zero trust architecture provides visibility and control over your network, including stopping ransomware, by helping firms prioritize assets and evaluate traffic, microsegment their users and conduct adaptive monitoring.

Appendix 2—Additional Resources

Regulatory Notices and Guidance

- *Regulatory Notice* 21-44 (Business Continuity Planning and Lessons from the COVID-19 Pandemic)
- *Regulatory Notice* 21-42 (FINRA Alerts Firms to "Log4Shell" Vulnerability in Apache Log4j Software)
- *Regulatory Notice* 21-30 (FINRA Alerts Firms to a Phishing Email Campaign Using Multiple Imposter FINRA Domain Names)
- *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)
- *Regulatory Notice* 20-32 (FINRA Reminds Firms to Be Aware of Fraudulent Options Trading in Connection With Potential Account Takeovers and New Account Fraud)
- *Regulatory Notice* 20-30 (Fraudsters Using Registered Representatives Names to Establish Imposter Websites)
- *Information Notice* 03/26/20 (Measures to Consider as Firms Respond to the Coronavirus Pandemic (COVID-19))
- *Regulatory Notice* 20-13 (FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic)

Reports and Guidance

- Cybersecurity Topic Page
- Report on Selected Cybersecurity Practices – 2018
- Report on Cybersecurity Practices – 2015
- Customer Information Protection Topic Page

Compliance Tools

- Small Firm Cybersecurity Checklist
- Core Cybersecurity Threats and Effective Controls for Small Firms
- Firm Checklist for Compromised Accounts
- Cross-Market Options Supervision: Potential Intrusions Report Card

Non-FINRA Resources

- Federal Bureau of Investigation (FBI)
- FBI Internet Crime Complaint Center (IC3)
- Cybersecurity and Infrastructure Security Agency (CISA)
- Stop Ransomware
- Joint FBI and CISA Cybersecurity Advisory Zeppelin Ransomware
- FinCEN Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime
- FinCEN Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments
- FinCEN Analysis Reveals Ransomware Reporting in BSA Filings Increased Significantly During the Second Half of 2021 (Nov. 1, 2022)
- Department of Homeland Security Ransomware Fact Sheet
- U.S. Department of Treasury, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (Sept. 21, 2021).
- National Conference of State Legislatures (NSCL) State Security Breach Notification Laws
- No More Ransom

Endnotes

1. The dark web includes websites that are not indexed by search engines and only accessible via specialized web browsers.

2. In a phishing event, bad actors may try to disguise themselves as trustworthy entities or individuals via email, electronic message, phone call or other communication, where they request sensitive firm data or customer information (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. 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, CFO). (These types of attacks are referred to as "spear phishing" and "whaling" respectively, but we refer to them collectively as "phishing" in this document.)