AUGUST 2026

Cybersecurity Effective Practices

This framework of 12 cybersecurity principles and effective practices is designed to help FINRA member firms strengthen their cybersecurity programs. The effective practices are informed by member firms' regulatory obligations, industry risk principles and practices FINRA has observed through member firm oversight. Sharing these practices supports FINRA's broader goal of protecting investors and safeguarding markets by advancing cybersecurity resilience across the broker-dealer industry.

Each practice presented below is scalable to firms of all sizes and adaptable based on a firm's risk profile, business model and technology complexity. Implementing these practices can help mitigate the risks of unauthorized access to firm systems and customer information and firm system disruptions caused by threat actors or system failures.

This framework does not create new legal or regulatory requirements, or new interpretations of existing requirements, nor does it relieve members of any existing legal or regulatory obligations. Members may consider the information in this framework in developing new, or modifying existing, practices that are reasonably designed to achieve compliance with relevant regulatory obligations based on their size and business model.

Effective Practices

Governance	2
Risk Management	2
Third-Party Risk Management	3
Asset Management	3
Access Control and Identity Management	4
Data Protection	5
Security Awareness and Training	5
Vulnerability and Patch Management	6
Security Monitoring	6
Threat Intelligence and Information Sharing	7
Incident Response and Reporting	8
Resilience and Recovery	8

Select Regulatory Obligations

As members contemplate their cybersecurity programs, they should consider their regulatory obligations. The failure to have a well-designed cybersecurity program could result in compliance shortfalls. Rules and regulations that may be implicated include SEC Regulations S-P (Privacy of Consumer Financial Information and Safeguarding Personal Information) and S-ID (Identity Theft Red Flags).

Rule 30(a) of SEC Regulation S-P requires member firms, as applicable, to have written policies and procedures that address administrative, technical and physical safeguards for the protection of customer information.[1] Those policies and procedures must include a program reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including:

- procedures to notify affected individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization;[2] and
- written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of service providers.[3]

Regulation S-ID requires member firms that offer or maintain one or more covered accounts[4] to develop and implement a written program designed to detect, prevent and mitigate identity theft in connection with opening or maintaining such accounts.[5]

Other rules and regulations that may be implicated include FINRA Rules 3110 (Supervision) and 4370 (Business Continuity Plans and Emergency Contact Information); and Exchange Act's recordkeeping obligations under Rules 17a-3 and 17a-4.

Effective Practices

1 | Governance

A strong cybersecurity governance structure can promote accountability, strategic alignment and visibility into cybersecurity risks at all levels of the organization. Well-designed governance structures can help firms maintain more cohesive programs, respond effectively to incidents, and make informed decisions about resource allocation and risk management.

Effective Practices

- **Designate a cybersecurity lead** who is accountable for program oversight.
- **Provide periodic updates on cybersecurity risks** to firm leadership or decision-makers, ensuring key decisions are documented and communicated.
- **Document cybersecurity policies** for key cybersecurity principles, including details of approval processes and any periodic review.
- **Align and integrate cybersecurity considerations** into business and operational planning, considering cybersecurity risks in strategic decisions (*e.g.*, mergers, new systems or processes, technology deployment).
- **Embed cybersecurity into firm culture** by encouraging senior management to consistently promote, resource and participate in cybersecurity initiatives.

2 | Risk Management

Cybersecurity risk management provides the foundation for understanding where a firm's most critical vulnerabilities lie and enables prioritized, risk-based decision-making. Ongoing risk assessments can help firms identify critical vulnerabilities, allocate resources to high-impact risks and adapt to emerging threats and business changes, decreasing the likelihood of a successful and costly incident. By establishing a program to identify, assess and manage cybersecurity risks to firm and customer information, systems and operations, each firm can better tailor its approach to its size, business model, technology complexity and risk exposure. This enables firms to determine an appropriate risk profile, manage residual risks and build resilience against evolving threat landscapes.

Effective Practices

- **Identify information assets, business functions and supporting systems** that are critical to operations.
- **Evaluate internal and external threats**, such as ransomware, insider threats and third-party risks. Consider both current and emerging threat landscapes.
- **Assess likelihood and potential impact** of identified risks to guide prioritization.
- **Conduct periodic vulnerability testing and penetration testing** of critical systems (*e.g.*, authentication systems) to identify gaps or weaknesses before a threat actor exploits them.
- **Use results of risk analyses** to determine business risk appetite and drive decisions about controls, staffing and investments.
- **Reassess risks on a recurring basis** as well as when significant changes occur in business operations, technology or the threat environment.
- **Periodically review residual risks with senior management** to promote informed decision-making about the risks the firm chooses to accept and whether reasonable mitigation strategies may be available.

3 | Third-Party Risk Management

Third-party service providers may have access to a firm's sensitive data and critical systems, making them an extension of a firm's security perimeter. Cybercriminals increasingly target vendors as a pathway to breach the clients they serve. Overseeing cybersecurity risks associated with third-party service providers from selection through the termination of a relationship helps firms mitigate and prevent breaches, maintain control over sensitive information, and protect customers and operations. This oversight is particularly critical for third-party service providers that have access to firm systems or maintain customer information or firm data.

Effective Practices

- **Identify and maintain a list of vendors** with access to the firm's sensitive data or systems, including understanding fourth-party relationships (vendors' vendors, or the vendors of the firm's vendors).
- **Identify and assess critical vendor functions** for the firm's business continuity, understanding which vendors are essential to daily operations or mission-critical functions.
- **Include cybersecurity-related requirements in contracts and service level agreements**, such as
  - visibility into fourth-party vendors,
  - right to audit,
  - data handling requirements upon contract termination, and
  - timely breach notifications consistent with SEC Regulation S-P obligations.[6]
- **As part of a firm's ongoing monitoring of its vendors, review access to firm systems and data**, including privileged access, connection activity and adherence to security requirements.
- **Establish, follow and document a termination process** that includes:
  - revoking vendor access promptly;
  - recovering and properly disposing of consumer and customer information, including ensuring a member firm's compliance with the disposal requirements under SEC Regulation S-P, as applicable[7]; and
  - confirming completion of all offboarding activities.

4 | Asset Management

A complete inventory of technology assets plays a crucial role in effective cybersecurity. Technology assets include anything that has value to an organization, including computing devices, IT systems, IT networks, software, virtual computing platforms, cloud services and related hardware. Unknown or unmanaged assets create blind spots that attackers can exploit to gain unauthorized access, establish persistence, and compromise data or systems. Maintaining an accurate and current inventory of technology assets—and classifying them based on sensitivity and criticality—enables appropriate security controls, patching efforts, threat monitoring and business continuity planning. It also prevents "shadow IT," where unauthorized systems and applications create security gaps and expand a firm's attack surface (potential entry points for cybersecurity threats).

Effective Practices

- **Establish and maintain an inventory of hardware, software, cloud services and data flows**, including all devices, applications and services, whether owned, leased or provided by third parties.
- **Identify asset owners and designate the owner** responsible for the asset's security and maintenance.
- **Classify assets** based on sensitivity and criticality.
- **Periodically review and validate asset inventory** as new devices are added or old ones are retired.
- **Establish processes for the secure provisioning, maintenance and decommissioning of end-of-life assets**, including:
  - secure onboarding procedures;
  - ongoing maintenance and updates;
  - proper disposal of retired equipment and data sanitization; and
  - decommissioning or isolating systems that no longer receive security updates.

5 | Access Control and Identity Management

Strong access controls ensure that users have only the access they need to perform their jobs and that their identities are properly verified. Weak passwords, shared credentials, excessive privileges or lack of multifactor authentication may create opportunities for both external attackers and malicious insiders. Firms should limit access to systems and data based on business need and implement controls to verify user identities. This includes enforcing the principles of least privilege (see below) and defense-in-depth (multi-layered controls). These practices reduce the attack surface, limit damage from compromised credentials, and ensure users and devices access only the resources necessary for their roles.

Effective Practices

- **Use unique credentials and role-based access controls** to prevent account sharing and to support a clear user audit trail.
- **Use multifactor authentication** for external account access and privileged account access, and re-authentication for high-risk transactions, account changes and other critical activities to reduce the risk of credential-based attacks.
- **Establish procedures for provisioning, modifying and deactivating access** to provide timely setup when employees onboard and deprovision when employees change roles or leave the organization.
- **Periodically review and validate user entitlements** to prevent access creep over time creating unnecessary risk.
- **Enforce the principle of least privilege** based on user role and responsibilities, granting the minimum access necessary to perform their duties.
- **Enforce segregation of duties** to prevent elevated-risk combinations, such as employees who have access to both front-office and back-office functions.
- **Apply zero trust[8] principles** by requiring verification of users and devices each time access is requested.

6 | Data Protection

Protecting firm and customer data through encryption, secure handling, and appropriate retention and data lifecycle management is essential to cybersecurity. Cybersecurity breaches, ransomware attacks and insider threats can result in unauthorized access to a firm's systems and data. Theft or compromise of sensitive information can lead to potential customer harm, operational disruption, regulatory violations and reputational damage. Strong data protection measures, including encryption, secure backup strategies, data classification and monitoring create multiple layers of defense that help prevent data loss, reduce exposure to threats, and protect firms and customers.

Effective Practices

- **Maintain data classification policies** that:
  - define categories of information;
  - assign handling requirements based on sensitivity; and
  - catalog data at rest (*e.g.*, hard drives, USBs, file folders, cloud storage) and data in transit (*e.g.*, moving between two locations: over the internet, from local to cloud storage, via email).
- **Encrypt sensitive data at rest and in transit**, where feasible, to render data unreadable to unauthorized parties even if it is intercepted or stolen.
- **Secure backup storage**, such as immutable backups (cannot be altered or deleted) and air-gapped backups (physically isolated from networks) and limit access to authorized personnel. Backups are often targeted in ransomware attacks and protecting them is critical to recovery.
- **Limit data retention** to what is necessary for business and regulatory purposes.
- **Apply security controls** (*e.g.*, remote wipe capability) to portable devices and remote work technologies.
- **Use data loss prevention or similar safeguards** to prevent unauthorized transmission of sensitive data (via email or otherwise) and monitor for unauthorized data transfers or exfiltration (unauthorized data removal or theft) attempts.

7 | Security Awareness and Training

Phishing attacks, social engineering and simple mistakes by well-intentioned individuals can circumvent even the strongest technical cybersecurity controls, resulting in credential compromise, malware installation and unauthorized access that threaten the entire security posture. Promoting cybersecurity awareness and delivering role-specific training to employees, contractors and relevant stakeholders helps ensure all associated persons (*e.g.*, staff, registered representatives, independent contractors) recognize threats and understand their role in protecting firm and customer data and helps mitigate risks both from external threat actors and internal negligence.

Effective Practices

- **Conduct ongoing cybersecurity awareness training** for all associated persons.
- **Train staff on common social engineering tactics**, such as email phishing, vishing (phishing via phone calls), and effective practices for password creation, management and security.
- **Provide enhanced training** for staff with access to sensitive systems or data related to their security responsibilities.

- **Reinforce training through simulated exercises or periodic reminders**, such as phishing simulations to help individuals recognize real attacks and create teachable moments.
- **Document completion and track participation** to enhance accountability and help identify gaps in training.
- **Maintain requirements for acknowledgement** of firm policies and procedures related to cybersecurity.
- **Foster a proactive culture of cybersecurity** with support from senior leadership, emphasizing that security is everyone's responsibility.

8 | Vulnerability and Patch Management

A structured vulnerability and patch management program can help ensure that systems are regularly assessed for weaknesses and that critical updates are applied promptly. Software vulnerabilities arise frequently, and cybercriminals actively exploit known weaknesses, often within hours of public disclosure. The longer vulnerabilities remain unaddressed, the greater the window of exposure, allowing attackers to compromise systems, steal data or establish persistence in the network. Regularly assessing systems for known vulnerabilities and applying updates in a timely manner based on risk significantly reduces the risk of exploitation and limits the impact of compromises by closing attack vectors before threat actors can weaponize them.

Effective Practices

- **Perform periodic scanning of internal and external assets** to identify weaknesses before attackers find them.
- **Prioritize remediation based on exploitability and business impact** to focus on those that are actively exploited or affect critical systems.
- **Establish patch timelines aligned with severity levels** to deploy critical patches more quickly while addressing less severe issues in standard maintenance windows.
- **Track and verify completion of remediation and patching** to ensure the work is completed as expected.
- **Address unsupported or end-of-life systems** to upgrade, isolate or decommission systems that might otherwise present ongoing risk.

9 | Security Monitoring

Continuous monitoring of systems and user activity enables rapid detection of unauthorized access, anomalous behavior and potential compromises, including both internal and external threats. Without monitoring, breaches can go undetected for months, allowing attackers to steal data, establish persistence and cause customer harm, with serious potential compliance and reputational consequences to follow. Monitoring systems and user activity for signs of unauthorized or anomalous behavior, including potential internal and external threats, significantly reduces the dwell time of attackers (the time attackers have undetected access to the system), minimizes data exposure, and helps firms respond to and recover from incidents faster.

Effective Practices

- **Use logging and alerting tools appropriate to firm size and complexity**, which may range from the Cybersecurity and Infrastructure Security Agency (CISA) tool Logging Made Easy or a more sophisticated Security Information and Event Management system.
- **Monitor for unusual access patterns, data exfiltration, or system changes** that may indicate insider or external threats.
- **Include both associated person and third-party access in monitoring scope** as vendors and contractors pose similar risks to associated persons.
- **Establish enhanced monitoring and supervision** of privileged systems and user access. Administrative accounts with greater access and controls should be appropriately supervised.
- **Retain security logs** long enough to support firm operations, incident investigations and forensic analysis—and comply with applicable regulatory requirements. Firms relying on such logs to comply with the requirements of Rule 30 of SEC Regulation S-P should note that Exchange Act Rule 17a-4(e)(14)(ii) requires a minimum three-year retention period.

10 | Threat Intelligence and Information Sharing

Cybersecurity threats evolve rapidly, and threat actors often use the same tactics across multiple targets. Maintaining awareness of relevant cybersecurity threats and participating in information-sharing efforts that improve sector-wide defenses and response capabilities enables proactive defense and faster incident detection. Information sharing amplifies the collective defense across the industry; the network effects of information sharing compound the benefits for all participants by raising the baseline security posture of the entire sector.

Effective Practices

- **Subscribe to threat intelligence feeds** appropriate to firm scale and operations, such as the Financial Intelligence Fusion Center (finra.org/FIFC) or resources from government agencies (CISA, FBI) and industry peer groups.
- **Integrate threat intelligence into the firm's risk assessments, training and monitoring efforts.**
- **Adjust defenses and detection parameters** based on emerging tactics, techniques and procedures (TTPs).
- **Participate in industry information-sharing initiatives or peer networks**, such as local InfraGard chapters or peer roundtables.
- **Share anonymized threat indicators or tactics** with regulators, trusted partners, a local FBI field office, the FBI Internet Crime Complaint Center (IC3) at IC3.gov, or CISA via CISA's 24/7 Operations Center (report@cisa.gov or (888) 282-0870).
- **Provide emerging threat information** (*e.g.*, FINRA Investor Insights) to customers to increase awareness of scams and other fraud trends.

11 | Incident Response and Reporting

As defined by the National Institute of Standards and Technology (NIST), an incident response plan (IRP) is the documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attack against an organization's information system(s).[9] Beyond compliance with the response program obligations under Regulation S-P noted above, a well-documented, regularly tested IRP enables coordinated action under pressure, reduces response time, minimizes damage, and helps to put members in a position to meet applicable notification requirements. Without a tested IRP, firms risk operational failures—including delayed detection, uncoordinated responses, and confused escalation—as well as compliance failures such as missed notification deadlines. The prolonged exposure that may result increases the potential for customer harm. A strong IRP can also help firms contain incidents faster, preserve evidence, and minimize operational and reputational impact.

12 | Resilience and Recovery

The ability to recover quickly is aided by preparation: tested backups, documented procedures, defined recovery objectives and a practiced incident response plan. Ransomware, system failures and natural disasters can render critical systems unavailable, and, without recovery capabilities, firms face potential prolonged service disruptions, customer losses and potential business failure. Ensuring the availability and recoverability of critical systems and data following a cybersecurity event enables firms to restore operations rapidly, minimize revenue loss, maintain customer trust and limit reputational damage.

Effective Practices

- **Maintain regularly tested backups** of critical data and systems.
- **Test recovery capabilities through tabletop or simulation exercises**, including offline scenarios that may require use of manual procedures for critical processes, hard-copy playbooks, and alternate contact methods for key staff during an outage or compromise. Involve key business, technology, and security staff as well as vendors and other mission-critical business partners.
- **Document scenarios in a playbook and continuously update them** based on new threats and lessons learned.
- **Incorporate resilience planning when making new technology investments**, including a review of a technology or vendor provider's recovery capabilities during the due diligence process.
- **Define system Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO)** to align with business criticality and relevant regulatory obligations. The RPO is the length of time since the last data backup. The RTO is the length of time it should take to restore to normal operations. These metrics drive backup frequency and recovery capabilities.

Endnotes

1 17 CFR 248.30(a)(1).

2 17 CFR 248.30(a)(3). *See also* 17 CFR 248.30(a)(4).

3 17 CFR 248.30(a)(5).

4 *See* 17 CFR 248.201(b)(3), which defines "covered account" as: (i) an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a brokerage account with a broker-dealer or an account maintained by a mutual fund (or its agent) that permits wire transfers or other payments to third parties; and (ii) any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

5 17 CFR 248.201(d).

6 *See* 17 CFR 248.30(a)(5).

7 *See* 17 CFR 248.30(b).

8 Zero trust means "never trust, always verify," where no user or device is automatically trusted, https://csrc.nist.gov/glossary/term/zero_trust.

9 https://csrc.nist.gov/glossary/term/incident_response_plan.

1700 K Street, NW
Washington, DC 20006-1506
www.finra.org

H-92403—08/2026