# Cybersecurity Best Practices for Broker-Dealers Checklist

By Frank Weigand, Brock Bosson, and Kayla Gebhardt, Cahill Gordon & Reindel LLP

This checklist discusses best practices for broker-dealers to mitigate the risk of cybersecurity incidents. Considerations include implementing cybersecurity programs that address supervision, risk reduction, and oversight of activities and vendor relationships to mitigate the risk of cybersecurity threats.

**Background**

Earlier this year, the U.S. Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) released their respective annual reports setting out their priorities for the year ahead.

In the SEC's 2025 Examination Priorities Report, it reiterated its focus on cybersecurity, noting that the SEC will continue to review broker-dealers' practices, policies, and procedures to safeguard customer information, with a heightened focus on the firms' use of third-party vendors. See *SEC 2025 Examination Priorities: Division of Examinations (Oct. 21, 2024).*

Similarly, the FINRA Annual Regulatory Oversight Report provides guidance on broker-dealer obligations with respect to cybersecurity and technology management, specifically highlighting cybersecurity as one of the top operational risks facing broker-dealers. See *2025 FINRA Annual Regulatory Oversight Report (Jan. 28, 2025)* (2025 FINRA Oversight Report). In connection therewith, firms are expected to create and maintain cybersecurity programs and controls that align with their scale of operations, risk profile, and overall business model. See 2025 FINRA Oversight Report.

Phishing campaigns, ransomware, network intrusions, customer account takeovers, fraudulent wires or ACH transactions, and vendor breaches are just some of the cybersecurity threats that broker-dealers face. The resulting unauthorized exposure of customer information or fraudulent financial activity can lead to financial loss and reputational risk that may compromise a firm's ability to comply with a number of rules and regulations. Broker-dealers could run afoul of several FINRA rules if they do not implement proper cybersecurity measures, including *FINRA Rule 3110* (Supervision), *FINRA Rule 3120* (Supervisory Control System), *FINRA Rule 4370* (Business Continuity Plans and Emergency Contact Information), *FINRA Rule 4530(b)* (Reporting Requirements), and *FINRA Rule 4530.01* (Reporting of Firms' Conclusions of Violations); as well as certain SEC rules, including Rule 17a-3 (*17 C.F.R. § 240.17a-3*) under the Exchange Act of 1934, as amended (Exchange Act), Exchange Act Rule 17a-4 (*17 C.F.R. § 240.17a-4*), Rule 30 (*17 C.F.R. § 248.30*) of SEC Regulation S-P, and SEC Regulation S-ID (*17 C.F.R. § 248.201, et seq.*).

By way of example, in a recent FINRA enforcement action in June 2025, Rialto Markets LLC was censured and fined $50,000 for failing to establish and maintain a supervisory system, including written supervisory procedures (WSPs) reasonably designed to safeguard customer records and information. *Rialto Markets LLC, Acceptance, Waiver, and Consent, FINRA No. 2022075714101 (June 11, 2025)*. FINRA had previously advised the firm to establish WSPs and systems to address and mitigate cybersecurity risks. However, FINRA found that the firm did not implement “data loss prevention controls such as multi-factor authentication for all email accounts, email access and other audit logs, alerts for suspicious activities such as anonymous IP address use, or email forwarding rules,” leading to the unauthorized access to nonpublic personal information of over 4,400 firm customers and the unauthorized transfer of over $1 million from the firm’s escrow agent to a bank account controlled by an unauthorized user.

In addition, in a FINRA enforcement action in March 2024, Osaic Wealth and Securities America were each censured and fined $150,000 for, among other things, failing to use multi-factor authentication which led to numerous cyber intrusions and email takeovers. *Osaic Wealth and Securities America, Acceptance, Waiver, and Consent, FINRA No. 2021071722201 (Mar. 14, 2024)*. According to FINRA, these failures led to the unauthorized access of the firms' networks and exposed the records and nonpublic personal information of over 32,640 customers. Incidents like this are expected to become more prevalent as cybersecurity threats increase in quantity and sophistication.

**Recommendations**

Broker-dealers should strongly consider implementing cybersecurity programs that address supervision, risk reduction, and oversight of activities and vendor relationships to mitigate the risk of cybersecurity threats. Specific recommendations include:

- Adopting written policies, procedures, and protocols for addressing cybersecurity risks;
- Designating a board committee with reporting lines to oversee cybersecurity efforts and periodic reporting by management to the board;
- Considering appointing a chief information security officer, the CISO, to develop, implement, and enforce cybersecurity policies across the firm;
- Providing training for employees on cybersecurity issues including formal online training, simulated phishing exercises, and informal discussions of cybersecurity events;
- Ensuring that the firm's IT professionals (if applicable) are trained and kept informed about the current cybersecurity threat landscape and ensure that they continually assess the effectiveness of the firm's controls;
- Implementing a vendor diligence, contracting, and oversight program that specifically addresses cybersecurity issues;
- Considering regular audits of its cybersecurity controls and obtaining audit reports from vendors;
- Maintaining physical and technological data security safeguards, including multi-factor authentication, encryption, and firewalls;
- Developing and testing a protocol for responding to cybersecurity incidents such as hacks, penetrations, or other cyber threats;
- Enhancing awareness that cybersecurity incidents can trigger disclosure under broker-dealer-specific reporting rules, such as *FINRA Rule 4530(b)*; –and–
- Staying abreast of regulatory developments in this area

**Related Content**

***Resource Kit***

- *FINRA Resource Kit*
- *Cybersecurity Resource Kit*

***Practice Notes***

- *FINRA Regulations*
- *Broker-Dealer Federal Regulation Compliance*
- *Broker-Dealer Disclosure and Complaint Filings: FINRA Rule 4530*

- *Broker-Dealer Recordkeeping Requirements*
- *Market Trends 2024/25: Cybersecurity-Related Disclosures*

***Checklist***

- *Broker-Dealer Recordkeeping Checklist*
- *Cybersecurity Incident Checklist*
- *FINRA Cycle Examination Checklist*
- *Recent SEC Cybersecurity Disclosure Requirements Checklist*

***Articles***

- *SEC Examination 2025 Priorities Report Summary*
- *SEC Cybersecurity Disclosure Trends*
- *Cybersecurity — Cracking the Code on Upcoming Disclosures*

---

**End of Document**