Cahill

March 5, 2024

Cybersecurity Best Practices for Broker-Dealers

The U.S. Securities and Exchange Commission ("SEC") and the Financial Industry Regulatory Authority ("FINRA") recently released their respective annual reports setting out their priorities for the year ahead. Not surprisingly, the reports reiterate cybersecurity as a top priority and remind broker-dealers once again of the importance of instituting best practices to mitigate the risk of cybersecurity incidents. We summarize below key areas for consideration and provide recommendations for firms to consider in light of the growing nature of cybersecurity threats.

Background

In its 2024 Examination Priorities Report, the SEC 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.[1] The SEC is also considering rules that would require broker-dealers to establish and implement written policies and procedures that are reasonably designed to address cybersecurity risks and to provide immediate notice to the SEC of significant cybersecurity incidents.[2]

Similarly, FINRA's 2024 Annual Regulatory Oversight Report[3] provides guidance on broker-dealer obligations with respect to cybersecurity and technology management,[4] specifically highlighting cybersecurity as one of the top operational risks facing broker-dealers. 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.[5]

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.[6]

By way of example, in a recent FINRA enforcement action in November 2023, Bolton Global Capital was censured and fined $75,000 for, among other things, failing to use multi-factor authentication for third-party service

---

[1] SEC 2024 Examination Priorities: Division of Examinations, https://www.sec.gov/files/2024-exam-priorities.pdf.

[2] 2024 FINRA Annual Regulatory Oversight Report: Cybersecurity and Technology Management (January 9, 2024), https://www.finra.org/rules-guidance/guidance/reports/2024-finra-annual-regulatory-oversight-report/cybersecurity.

[3] 2024 FINRA Annual Regulatory Oversight Report (January 9, 2024), https://www.finra.org/rules-guidance/guidance/reports/2024-finra-annual-regulatory-oversight-report.

[4] *See supra* note 3.

[5] *Id.*

[6] Broker-dealers could run afoul of several FINRA rules if they do not implement proper cybersecurity measures including FINRA Rules 3110 (Supervision); 3120 (Supervisory Control System); 4370 (Business Continuity Plans and Emergency Contact Information); 4530(b) (Reporting Requirements); and 4530.01 (Reporting of Firms' Conclusions of Violations), in addition to SEC rules including Exchange Act Rules 17a-3 and 17a-4; Rule 30 of Regulation S-P; and Regulation S-ID.

providers that had access to the firm's administrative systems and data.[7] According to FINRA, this failure led to the unauthorized access of the firm's network and exposed the records and non-public personal information of over 6,000 firm customers.[8] 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 ("CISO") to develop, implement, and enforce cybersecurity policies across the firm;
- providing training for employees on cybersecurity issues including, but not limited to, 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
- continuously staying abreast of regulatory developments in this area.

* * *

If you have any questions about the issues addressed in this memorandum, or if you would like a copy of any of the materials mentioned in it, please do not hesitate to call or email authors Frank Weigand (Partner) at 212.701.3890 or fweigand@cahill.com; Brock Bosson (Partner) at 212.701.3136 or bbosson@cahill.com; or Kayla Gebhardt (Associate) at 212.701.3251 or kgebhardt@cahill.com; or email publicationscommittee@cahill.com.

---

[7] FINRA Letter of Acceptance, Waiver, and Consent, *In re Bolton Global Capital* (November 3, 2023), https://www.finra.org/sites/default/files/fda_documents/2021072622201%20Bolton%20Global%20Capital%20CRD%2015650%20AWC%20gg%20%282023-1701649196662%29.pdf

[8] *Id.*