PUBLICATION

Financial Industry Regulators Continue Crack Down on Cybersecurity

Authors: Matthew George White, Alexander Frank Koskey, III
September 20, 2021

On multiple fronts, the U.S. Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) continue to increase their focus on cybersecurity. This is understandable as headlines of recent data breaches and ransomware attacks are in the news almost daily. This alert will highlight several of the actions taken by these regulators and proactive measures that financial services companies can implement to avoid the regulatory scrutiny that may follow from a cyber incident.

In light of the heightened focus on these issues, firms should review their existing security controls, incident response plans, and other cybersecurity and data protection procedures to ensure that they are adequately protecting customer information.

A. The Regulators' Priorities

Each year the SEC and FINRA publish reports outlining their regulatory priorities. These reports relay their findings from examinations of firms and offer guidance on how firms can improve their operations. In this year's reports, the SEC and FINRA discussed the importance of information security and data privacy and how firms are more vulnerable now than ever before to cyber-attacks. The reports offer guidance and effective best practices to increase cybersecurity awareness among registered representatives.

SEC

The SEC's report focused on working with firms to improve their responses to cyber attacks and identifying potential risks within a firm's operation. Due to the pandemic, there was a sharp increase in remote operations. This led to an increased concern over security of data and sensitive client information. The SEC will review whether a firm has taken appropriate measures to:

1. Safeguard customer accounts and prevent unauthorized account intrusions, including verifying an investor's identity to prevent unauthorized account access;
2. Oversee vendors and service providers;
3. Address malicious email activities, such as phishing or account intrusions;
4. Respond to incidents, including those related to ransomware attacks; and
5. Manage operational risk as a result of dispersed employees in a work-from-home environment.

The SEC will work with firms to ensure that investor and firm records are protected by implementing controls surrounding the access and management of books and records.

Broker-dealer and investment advisory firms are not alone in this focus. For example, the SEC has announced that it plans to issue proposed rules in October to enhance issuer disclosures regarding cybersecurity risk

governance. In the wake of the SolarWinds attack, the SEC has also issued a letter formally asking public companies to disclose cyber attacks against them.

FINRA

FINRA's report strongly encourages its member firms to consider incorporating and tailoring its recommended practices into their compliance programs. Like the SEC, FINRA acknowledged that the pandemic and work-from-home environment have revealed weaknesses in firms' information security programs. Exam observations have highlighted these areas as vulnerabilities:

6. **Data Loss Prevention Programs**: Not encrypting all confidential data, including a broad range of non-public customer information, in addition to Social Security numbers (such as other account profile information and firm information).

7. **Branch Policies, Controls and Inspections**: Not maintaining branch-level written cybersecurity policies; inventories of branch level data, software and hardware assets; and branch-level inspection and automated monitoring programs.

8. **Training**: Not providing comprehensive training to registered representatives, personnel, third-party providers and consultants on cybersecurity risks relevant to individuals' roles and responsibilities, including phishing.

9. **Vendor Controls:** Not implementing and documenting formal policies and procedures to review prospective and existing vendors' cybersecurity controls and managing the lifecycle of firms' engagement with all vendors (*i.e.* from onboarding, to ongoing monitoring, through off-boarding, including defining how vendors will dispose of non-public client information).

10. **Access Management:** Not implementing access controls, including developing a "policy of least privilege" to grant system and data access only when required and removing it when no longer needed; not limiting and tracking individuals with administrator access; and not implementing multi-factor authentication (MFA) for registered representatives, employees, vendors, and contractors.

11. **Inadequate Change Management Supervision:** Insufficient supervisory oversight for application and technology changes (including upgrades, modifications to or integration of firm or vendor systems), which lead to violations of other obligations, such as those relating to data integrity, cybersecurity, books and records, and confirmations.

12. **Limited Testing and System Capacity**: Order management system, account access and trading algorithm malfunctions due to a lack of testing for changes or system capacity issues.

FINRA also observed increased numbers of cybersecurity- or technology-related incidents at firms, including systemwide outages; email and account takeovers; fraudulent wire requests; imposter websites; and ransomware. FINRA's report includes several best practices that firms should review to address these issues, including:

- **Insider Threat and Risk Management:** Collaborating across technology, risk, compliance, fraud, and internal investigations/conduct departments to assess key risk areas, monitor access and entitlements, and investigate potential violations of firm rules or policies with regard to data access or data accumulation.

- **Incident Response Planning**: Establishing and regularly testing written formal incident response plans that outlined procedures for responding to cybersecurity and information security incidents; and developing frameworks to identify, classify, prioritize, track and close cybersecurity-related incidents.

- **System Patching:** Implementing timely application of system security patches to critical firm resources (e.g., servers, network routers, desktops, laptops and software systems) to protect non-public client or firm information.

- **Asset Inventory:** Creating and keeping current an inventory of critical information technology assets, including hardware, software and data, as well as corresponding cybersecurity controls.

- **Change Management Processes**: Implementing change management procedures to document, review, prioritize, test, approve, and manage hardware and software changes, as well as system capacity, in order to protect non-public information and firm services.

B. SEC Enforcement

In addition to providing guidance in this area, the SEC has recently instituted enforcement actions against firms that have failed to implement effective cybersecurity policies and controls.

Late last month, the SEC announced that it was sanctioning eight firms for deficient cybersecurity procedures. All of the firms were registered broker-dealer or investment advisory firms. Each of the SEC's orders found that the firms violated Rule 30(a) of Regulation S-P, also known as the Safeguards Rule, which is designed to protect customer information. The circumstances surrounding each of these alleged violations provide insight into the SEC's heightened focus on firms' cybersecurity practices.

Against one group of related entities, the SEC alleged that cloud-based email accounts of the firms' personnel were taken over by unauthorized third parties, resulting in the exposure of personally identifying information (PII) of more than 2,000 customers. In its Order, the SEC found that none of these accounts were protected in a manner consistent with the firm's policies. The Order also found that the firm's breach notification letters to its customers included misleading statements implying that the notifications were provided much more quickly after the discovery of the incident than they were. This action highlights the importance of both having sufficient cyber-related policies and procedures and, importantly, ensuring that your company is actually implementing and following them. A pertinent example here is ensuring your company both requires the use of multi-factor authentication (MFA) and actually implements MFA in its access controls. This action also emphasizes the importance of carefully constructing any required incident notification letters. The requirements for incident notification vary in each of the 50 states and particular care must be given ensuring those requirements are met, and also in considering the precise language that will be used to describe the incident. Experienced outside counsel can be critical to ensuring these obligations are satisfied.

Against a second group of related entities, the SEC again alleged that cloud-based email accounts of firm personnel were taken over by unauthorized third parties, this time resulting in the exposure of PII of nearly 5,000 customers. According to the SEC's Order, while the firm discovered the incident in 2018, it failed to adopt and implement firm-wide enhanced security measures for cloud-based email accounts of its representatives until 2021, resulting in the exposure and potential exposure of additional customer and client records and information. This action highlights the importance of effective post-incident remediation. One of the hallmarks of an effective incident response program is ensuring that your firm learns from the incident, implements additional protective measures, and then tests those regularly. Cyber incident preparedness is a constantly changing process and firms must continue to evolve their policies and procedures to ensure they are protecting customer information.

Finally, against the remaining firm, the SEC alleged again that cloud-based email accounts were taken over by unauthorized third parties resulting in the exposure of PII of nearly 5,000 customers. According to the SEC's Order, the firm failed to adopt written policies and procedures requiring additional firm-wide security measures until well after the incident, and failed to fully implement those procedures for several months after that. Particularly instructive in this action is that the firm recommended, but did not require, the use of MFA. This is yet another example of the SEC focusing on the required implementation (or lack thereof) of effective cybersecurity measures.

C. Additional Guidance

FINRA also remains active in providing guidance on cyber-related issues. This summer FINRA has issued two regulatory notices (available here and here) alerting firms to phishing email campaigns. The first related to a series of fraudulent emails from "FINRA Support" originating from the domain name "westour.org" and the second related to a campaign using multiple imposter FINRA domain names (including "@finrar-reporting.org," "@Finpro-finrar.org" and "@gateway2-finra.org").

FINRA also recently issued Regulatory Notice 21-29 reminding firms of the supervisory obligations related to outsourcing to third-party vendors. Among the considerations in this area, FINRA in particular highlighted cybersecurity stating that:

"FINRA expects member firms to develop reasonably designed cybersecurity programs and controls that are consistent with their risk profile, business model and scale of operations. FINRA reminds member firms to review core principles and effective practices for developing such programs and controls, including Vendor management, from [FINRA's] Report on Cybersecurity Practices (2015 Report) and the Report on Selected Cybersecurity Practices – 2018 (2018 Report), as well as other resources included in the Appendix to [the] Notice."

D. Conclusion

It is clear that the regulatory focus on cybersecurity and data protection issues facing financial institutions is only increasing. The repeated pronouncements and actions from the SEC and FINRA certainly highlight this dynamic. Firms should review their cybersecurity and data protection policies and procedures in light of this focus and pay particular attention to their security controls and incident response planning. It is critical that firms regularly test and assess these procedures to ensure they are adequately protecting customer information.

If you have any questions regarding the SEC or FINRA actions in this area, or any other aspect of your cybersecurity or data privacy management program, please contact the authors, Matthew G. White, CIPP/US, CIPP/E, CIPM, PCIP, Alexander F. Koskey, CIPP/US, CIPP/E, PCIP, or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.