CAHILL

March 5, 2020

SEC's OCIE Publishes Cybersecurity and Resiliency Observations

I. SUMMARY

On January 27, the Securities and Exchange Commission's ("SEC") Office of Compliance Inspections and Examinations ("OCIE") published a report on its observations of cybersecurity and resiliency practices in securities and financial markets.[1] Developed through its examinations of thousands of broker-dealers, investment advisors, clearing agencies, national securities exchanges, and other SEC registrants, the OCIE's observations laid out its views on industry best practices and focused its attention on challenges and risks arising from:

- governance and risk management;
- access rights and controls;
- data loss prevention;
- mobile security;
- incident response and resiliency;
- vendor management; and
- training and awareness.

As the OCIE more generally observed, technology has become increasingly vital for markets, market participants, and their vendors, and cybersecurity threats are likewise becoming progressively more sophisticated and aggressive. Information security has therefore become a key element in the OCIE's examination program over the past eight years, and the OCIE hopes these observations will assist market participants in considering how to enhance cybersecurity preparedness and operational resiliency.

II. GOVERNANCE AND RISK MANAGEMENT

The OCIE's focus on governance emphasizes a "tone at the top" on cyber risks, "with senior leaders who are committed to improving their organization's cyber posture through working with others to understand, prioritize, communicate, and mitigate cybersecurity risks." The OCIE expects organizations to implement appropriate cybersecurity programs and processes, including (i) regular risk assessments to identify, analyze, and prioritize cybersecurity risks to an organization, (ii) written cybersecurity policies and procedures to address those risks, and (iii) operations for actively monitoring information security systems to detect procedure violations and optimize enforcement of those policies and procedures.

The OCIE states several measures taken by organizations in this area. First, organizations generally have board and senior level leadership and attention in setting strategy and overseeing the cybersecurity programs. Second, organizations have developed a process to identify, manage, and mitigate risks while considering potential vulnerabilities specific to the organization's business model, such as remote or traveling employees, insider threats, and international operations, especially with the proliferation of threats from sophisticated and well-resourced state actors. Next, organizations have established comprehensive written policies and procedures with respect to all practice areas outlined. Lastly, organizations consistently test and monitor the procedures, evaluate and adapt

[1] *See OCIE Cybersecurity and Resiliency Observations, United States Securities and Exchange Commission, Jan 27, 2020, available at* https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf. Unless otherwise specified, quoted statements in this memorandum are taken from the report.

policies and procedures to address weaknesses, and communicate promptly with decision makers, customers, employees, market participants, and regulators.

III. Access Rights and Controls

Access rights and controls need to identify and control physical and electronic access to an organization's systems based on the users' job responsibilities with the objective to regulate access for authorized users in ways that are both practical and secure. The OCIE states that effective access rights and controls require understanding the location of specific systems and data, restricting access to authorized users, and implementing appropriate controls to prevent and monitor unauthorized access. Multi-factor authentication continues to be a key element of secure access control.

The OCIE classifies several strategies based on its observations. One strategy is to determine who needs legitimate authorized access to what sensitive systems and data and then require periodic account reviews to confirm. Second, organizations need to develop systems and procedures for access management. This includes (i) limiting access as appropriate, such as during onboarding, transfers, and terminations, (ii) having a separation of duties for approvals to user access, (iii) re-certifying user access rights periodically, (iv) requiring strong passwords and periodic password changes, (v) requiring multi-factor authentication, and (vi) promptly revoking system access for employees who no longer need access. Third, organizations need to monitor access and develop procedures to review failed attempts and lockouts, ensure the proper handling of requests for unusual changes to the system hardware and software, such as login credentials, and approve such changes and investigate anomalies as required.

IV. Data Loss Prevention

Data loss prevention requires employing apt tools and processes to ensure that an organization's sensitive data is not lost, misused, or accessed without authorization. The OCIE observes the following key strategies in this area. The first is vulnerability scanning, which calls for routine scans to detect possible vulnerabilities in software code, web applications, servers and databases, workstations, and endpoints. Another is enacting perimeter security, which provides methods to control, monitor, and inspect all network traffic, such as fire walls and intrusion detection systems, or uses enterprise data loss prevention solutions to monitor access to personal email, cloud sharing services, social media, and removable storage devices. Organizations can also use detective security, which uses technology to detect fraudulent communications in progress. Encryption and network segmentation are other common methods; the former encrypts all data internally and externally, both "in motion" and "at rest," while the latter implements segmentation across networks and systems and configures access-control lists to limit data availability across systems. Insider threat monitoring programs increase the frequency of testing, create rules to identify and block transmission of sensitive data, and take corrective actions based on the results. The OCIE furthermore identifies other methods such as patch management programs, maintenance of critical hardware and software inventory, and securing and disposing of legacy hardware and software.

V. Mobile Security

The OCIE states that mobile device access can create a variety of security risks, particularly where a bring-your-own-device policy is in place. Mobile devices can be managed using fully compatible mobile device management applications, or other similar technology, for an organization's internal tools such as emails, calendar, data storage, and others. Other mobile security measures include multi-factor authentication, controls for preventing printing, copying, pasting, or saving information to personal devices, and the ability to remotely clear data and content from devices. Lastly, establishing mobile-specific policies and procedures and training employees on such policies and procedures are essential.

VI. Incident Response and Resiliency

Planning for cyber and security incidents before they happen is a theme in the OCIE's observations, and effective plans generally include technology and processes for timely detection, appropriate disclosures, and proper assessments of corrective actions as a response. Procedures that allow for business continuity and resiliency are also crucial to resume service for clients without — or with minimal — interruption.

Incident response can include various strategies. Generally, a response plan is developed based on the assessed risk of specific attacks and incidents in light of past cybersecurity incidents and current cyber-threat intelligence. A plan should include timelines for notification and response, processes for escalation, and plans for communicating with key stakeholders. This requires identifying and understanding all applicable federal and state reporting requirements for cyber incidents and having protocols for contacting the authorities, regulators, customers, clients and employees, as appropriate, if cyberattacks occur or secure data is compromised. A trained staff with assigned roles, expertise and responsibilities is also needed to execute the plan. Lastly, testing the plan, for example through tabletop exercises, and drawing from lessons learned post-incident is vital.

The OCIE identifies several factors for improving resiliency as well. First, organizations can maintain an inventory of core business operations and systems. By doing so, they can prioritize the business services and map the systems and processes to understand the impact of any failures. In turn, organizations can develop a tailored strategy with defined risks that considers what systems and processes can be substituted during a disruption to continuously provide services, how to geographically separate backup data, and what effects business disruptions will have on stakeholders. Organizations are also seen generally considering additional safeguards such as having backup data in different networks or offline and considering cybersecurity insurance.

VII. Vendor Management

Because most companies share or outsource at least some secure data processing and management to vendors, the OCIE notes a variety of risks and best practices for managing vendor relationships and security. Key items include conducting diligence on vendors and monitoring and overseeing a vendor's selection, policies, and contract terms. A vendor management program ensures vendors meet security requirements and implement appropriate safeguards. Vendor questionnaires can be used to check for industry standards (SOC 2, SSAE 18), independent audits can be conducted, and procedures can be implemented for terminating or replacing vendors. Successful vendor management requires understanding all the relevant contract terms in place to know how the vendor addresses risk and security. Lastly, closely monitoring the vendor relationship, ensuring all security requirements are continuously being met, and being aware of service or personnel changes are important.

VIII. Training and Awareness

The OCIE's final observation point focuses on security training and awareness for employees. So-called "phishing" emails (emails that contain links with malicious code) present increasing security risks to organizations of all kinds. Providing risk-focused information within an organization about cyber risks and employees' responsibilities helps to heighten the awareness of threats and familiarity with procedures to be followed during an incident. Organizations that have leading information security programs develop training guides and user-friendly materials outlining policies and procedures and implement specific hands-on training, such as sending mock phishing emails to employees. Driven by the tone at the top, an organization's willingness to monitor, re-evaluate, and update programs, as appropriate, is essential.

IX. CONCLUSION

The OCIE makes clear that its observations do not carry the weight of laws, rules, or regulations, noting that it is not prescribing a "one size fits all approach." Rather, the SEC uses the results of the OCIE examinations to inform rule-making initiatives, identify and monitor risks, improve industry practices and pursue misconduct. For market participants and potential civil litigants alike, the OCIE guidance is helpful for identifying best practices among companies. However, operationalizing these best practices and determining the appropriate degree of implementation can be challenging. Companies should seek the guidance of experienced counsel for assistance in navigating the implementation of these best practices and in "right-sizing" the implementation so that the company's information security program is tailored to its operations and resources.

* * *

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, please do not hesitate to email publications@cahill.com or call or email Bradley Bondi at 202-862-8910 or BBondi@Cahill.com; Brockton Bosson at 212-701-3136 or BBosson@Cahill.com; David Owen at 212-701-3955 or DOwen@Cahill.com; or Jason Yeoun at 212-701-3850 or JYeoun@Cahill.com.

This memorandum is for general information purposes only and is not intended to advertise our services, solicit clients or represent our legal advice.