Cybersecurity and Resiliency Observations

OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS

U.S. SECURITIES AND EXCHANGE COMMISSION

CONTENTS

Cybersecurity threats come from many sources, are global in nature, and do not discriminate across the spectrum of securities and financial markets and market participants. The seriousness of the threats and the potential consequences to investors, issuers, and other securities market participants, and the financial markets and economy more generally, are significant and increasing. As markets, market participants, and their vendors have increasingly relied on technology, including digital connections and systems, cybersecurity risk management has become essential. Indeed, in an environment in which cyber threat actors are becoming more aggressive and sophisticated—and in some cases are backed by substantial resources including from nation state actors—firms participating in the securities markets, market infrastructure providers and vendors should all appropriately monitor, assess and manage their cybersecurity risk profiles, including their operational resiliency.

The SEC has focused on cybersecurity issues for many years, with particular attention to market systems, customer data protection, disclosure of material cybersecurity risks and incidents, and compliance with legal and regulatory obligations under the federal securities laws.[1] Among other things, the SEC maintains a Cybersecurity Spotlight webpage that provides cybersecurity-related information and guidance.[2] Cybersecurity is also a key priority for OCIE. OCIE has highlighted information security as a key risk for security market participants, and has included it as a key element in its examination program over the past eight years. OCIE has also published eight risk alerts related to cybersecurity.[3]

---

[1] For example, the SEC's Division of Enforcement established the Cyber Unit in September 2017, the SEC hosted a roundtable in 2014 to discuss cybersecurity issues, and the SEC's Office of Investor Education and Advocacy published Investor Alerts and Bulletins, such as Investor Alert: Identity Theft, Data Breaches and Your Investment Accounts, (Sept. 22, 2015) and Updated Investor Bulletin: Protecting Your Online Investment Accounts from Fraud, (Apr. 26, 2017).

[2] "Spotlight on Cybersecurity, the SEC and You" available at www.sec.gov/spotlight/cybersecurity. This page contains information for investors, issuers, and registered firms and organizations, including the Commission Statement and Guidance on Public Company Cybersecurity Disclosures, guidance from the Division of Investment Management, the Division of Trading and Markets, and Investor Alerts and Bulletins.

[3] *See* OCIE Safeguarding Customer Records and Information in Network Storage–Use of Third Party Security Features (May 23, 2019); Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P–Privacy Notices and Safeguard Policies (Apr. 16, 2019); Observations from Investment Adviser Examinations Relating to Electronic Messaging (Dec. 14, 2018); Observations from Cybersecurity Examinations (Aug. 7, 2017); Cybersecurity: Ransomware Alert (May 17, 2017); OCIE's 2015 Cybersecurity Examination Initiative (Sept. 15, 2015); Cybersecurity Examination Sweep Summary (Feb. 3, 2015); and Investment Adviser Use of Social Media (Jan. 4, 2012).

Through thousands of examinations of broker-dealers, investment advisers, clearing agencies, national securities exchanges and other SEC registrants, OCIE has observed various industry practices and approaches to managing and combating cybersecurity risk and the maintenance and enhancement of operational resiliency. These include practices in the areas of governance and risk management, access rights and controls, data loss prevention, mobile security, incident response and resiliency, vendor management, and training and awareness. Recognizing that there is no such thing as a "one-size fits all" approach, and that all of these practices may not be appropriate for all organizations, we are providing these observations to assist market participants in their consideration of how to enhance cybersecurity preparedness and operational resiliency.

GOVERNANCE AND RISK MANAGEMENT

Effective cybersecurity programs start with the right tone at the top, 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. While the effectiveness of any given cybersecurity program is fact-specific, we have observed that a key element of effective programs is the incorporation of a governance and risk management program that generally includes, among other things: (i) a risk assessment to identify, analyze, and prioritize cybersecurity risks to the organization; (ii) written cybersecurity policies and procedures to address those risks; and (iii) the effective implementation and enforcement of those policies and procedures.

OCIE has observed organizations utilizing the following risk management and governance measures:

- **Senior Level Engagement.** Devoting appropriate board and senior leadership attention to setting the strategy of and overseeing the organization's cybersecurity and resiliency programs.
- **Risk Assessment.** Developing and conducting a risk assessment process to identify, manage, and mitigate cyber risks relevant to the organization's business. This includes considering the organization's business model, as part of defining a risk assessment methodology, and working to identify and prioritize potential vulnerabilities, including remote or traveling employees, insider threats, international operations and geopolitical risks, among others.

- **Policies and Procedures.** Adopting and implementing comprehensive written policies and procedures addressing the areas discussed below and identified risks.
- **Testing and Monitoring.** Establishing comprehensive testing and monitoring to validate the effectiveness of cybersecurity policies and procedures on a regular and frequent basis. Testing and monitoring can be informed based on cyber threat intelligence.
- **Continuously Evaluating and Adapting to Changes.** Responding promptly to testing and monitoring results by updating policies and procedures to address any gaps or weaknesses and involving board and senior leadership appropriately.
- **Communication.** Establishing internal and external communication policies and procedures to provide timely information to decision makers, customers, employees, other market participants, and regulators as appropriate.

ACCESS RIGHTS AND CONTROLS

Access rights and controls are used to determine appropriate users for organization systems based on job responsibilities, and to deploy controls to limit access to authorized users. Access controls generally include: (i) understanding the location of data, including client information, throughout an organization; (ii) restricting access to systems and data to authorized users; and (iii) establishing appropriate controls to prevent and monitor for unauthorized access.

OCIE has observed strategies related to access rights and controls at organizations that perform the following:

- **User Access.** Developing a clear understanding of access needs to systems and data. This includes limiting access to sensitive systems and data, based upon the user's needs to perform legitimate and authorized activities on the organization's information systems, and requiring periodic account reviews.
- **Access Management.** Managing user access through systems and procedures that: (i) limit access as appropriate, including during onboarding, transfers, and terminations; (ii) implement separation of duties for user access approvals; (iii) re-certify users' access rights on a periodic basis (paying particular attention to accounts with elevated privileges including users, administrators, and service accounts); (iv) require the use of strong, and periodically changed, passwords; (v) utilize multi-factor authentication (MFA) leveraging an application or key fob to generate an additional verification code; and (vi) revoke system access immediately for individuals no longer employed by the organization, including former contractors.

- **Access Monitoring.** Monitoring user access and developing procedures that: (i) monitor for failed login attempts and account lockouts; (ii) ensure proper handling of customers' requests for user name and password changes as well as procedures for authenticating anomalous or unusual customer requests; (iii) consistently review for system hardware and software changes, to identify when a change is made; and (iv) ensure that any changes are approved, properly implemented, and that any anomalies are investigated.

DATA LOSS PREVENTION

Data loss prevention typically includes a set of tools and processes an organization uses to ensure that sensitive data, including client information, is not lost, misused, or accessed by unauthorized users.

OCIE has observed the following data loss prevention measures utilized by organizations:

- **Vulnerability Scanning.** Establishing a vulnerability management program that includes routine scans of software code, web applications, servers and databases, workstations, and endpoints both within the organization and applicable third party providers.
- **Perimeter Security.** Implementing capabilities that are able to control, monitor, and inspect all incoming and outgoing network traffic to prevent unauthorized or harmful traffic. These capabilities include firewalls, intrusion detection systems, email security capabilities, and web proxy systems with content filtering. Implementing an enterprise data loss prevention solution capable of monitoring and blocking access to personal email, cloud-based file sharing services, social media sites, and removable media such as USB and CDs.
- **Detective Security.** Implementing capabilities that are able to detect threats on endpoints. Considering products that can utilize both signature and behavioral-based capabilities and can identify incoming fraudulent communications to prevent unauthorized software or malware from running. Establishing policies and procedures to capture and retain system logs from systems and applications for aggregation and analysis. For software that provides automated actions, such as macros and scripts, enabling optional security features or following the security guidance that may be offered by third party software providers.

- **Patch Management.** Establishing a patch management program covering all software (*i.e.*, in-house developed, custom off-the-shelf, and other third party software) and hardware, including anti-virus and anti-malware installation.
- **Inventory Hardware and Software.** Maintaining an inventory of hardware and software assets, including identification of critical assets and information (*i.e.*, know where they are located, and how they are protected).
- **Encryption and Network Segmentation.** Using tools and processes to secure data and systems, including: (i) encrypting data "in motion" both internally and externally; (ii) encrypting data "at rest" on all systems including laptops, desktops, mobile phones, tablets, and servers; and (iii) implementing network segmentation and access control lists to limit data availability to only authorized systems and networks.
- **Insider Threat Monitoring.** Creating an insider threat program to identify suspicious behaviors, including escalating issues to senior leadership as appropriate. Increasing the depth and frequency of testing of business systems and conducting penetration tests. Creating rules to identify and block the transmission of sensitive data (*e.g.*, account numbers, social security numbers, trade information, and source code) from leaving the organization. Tracking corrective actions in response to findings from testing and monitoring, material changes to business operations or technology, and any other significant events.
- **Securing Legacy Systems and Equipment.** Verifying that the decommissioning and disposal of hardware and software does not create system vulnerabilities by using processes to: (i) remove sensitive information from and prompt disposal of decommissioned hardware and software; and (ii) reassess vulnerability and risk assessments as legacy systems are replaced with more modern systems.

MOBILE SECURITY

Mobile devices and applications may create additional and unique vulnerabilities. OCIE has observed the following mobile security measures at organizations utilizing mobile applications:

- **Policies and Procedures.** Establishing policies and procedures for the use of mobile devices.
- **Managing the Use of Mobile Devices.** Using a mobile device management (MDM) application or similar technology for an organization's business, including email communication, calendar, data storage, and other activities. If using a "bring your own device" policy, ensuring that the MDM solution works with all mobile phone/device operating systems.
- **Implementing Security Measures.** Requiring the use of MFA for all internal and external users. Taking steps to prevent printing, copying, pasting, or saving information to personally owned computers, smartphones or tablets. Ensuring the ability to remotely clear data and content from a device that belongs to a former employee or from a lost device.
- **Training Employees.** Training employees on mobile device policies and effective practices to protect mobile devices.

INCIDENT RESPONSE AND RESILIENCY

Incident response includes: (i) the timely detection and appropriate disclosure of material information regarding incidents; and (ii) assessing the appropriateness of corrective actions taken in response to incidents. An important component of an incident response plan includes business continuity and resiliency (*i.e.*, if an incident were to occur, how quickly can the organization recover and again safely serve clients?).

OCIE has observed that many organizations with incident response plans tend to include the following elements:

- **Development of a Plan.** Developing a risk-assessed incident response plan for various scenarios including denial of service attacks, malicious disinformation, ransomware, key employee succession, as well as extreme but plausible scenarios. Considering past cybersecurity incidents and current cyber-threat intelligence in developing business continuity plans and policies and procedures. Establishing and maintaining procedures that include: (i) timely notification and response if an event occurs; (ii) a process to escalate incidents to appropriate levels of management, including legal and compliance functions; and (iii) communication with key stakeholders.

- **Addressing Applicable Reporting Requirements.** Determining and complying with applicable federal and state reporting requirements for cyber incidents or events, such as requirements for financial institutions to file a suspicious activity report or for public companies to disclose material risks and incidents. For example, the organization should consider:
    - » Contacting local authorities or the FBI if an attack or compromise is discovered or suspected.
    - » Informing regulators and sharing information, including indicators of compromise (artifacts observed on a network or operating system indicating a potential intrusion), with the appropriate organizations.
    - » Notifying customers, clients, and employees promptly if their data is compromised.
- **Assigning Staff to Execute Specific Areas of the Plan.** Designating employees with specific roles and responsibilities in the event of a cyber incident. In doing so, identifying additional cybersecurity and recovery expertise in advance.
- **Testing and Assessing the Plan.** Testing the incident response plan and potential recovery times, using a variety of methods including tabletop exercises. If an incident does occur, implementing the plan and assessing the response after the incident to determine whether any changes to the procedures are necessary.

OCIE has observed the following strategies to address resiliency:

- **Maintaining an Inventory of Core Business Operations and Systems.** Identifying and prioritizing core business services. Understanding the impact on business services of an individual system or process failure. Mapping the systems and processes that support business services, including those over which the organization may not have direct control.
- **Assessing Risks and Prioritizing Business Operations.** Developing a strategy for operational resiliency with defined risk tolerances tailored to the organization. In developing a strategy, organizations consider: (i) determining which systems and processes are capable of being substituted during disruption so that business services can continue to be delivered; (ii) ensuring geographic separation of back-up data and avoid concentration risk; and (iii) the effects of business disruptions on both the institution's stakeholders and other organizations.

- **Considering Additional Safeguards.** Maintaining back-up data in a different network and offline. Evaluating whether cybersecurity insurance is appropriate for the organization's business.

VENDOR MANAGEMENT

Practices and controls related to vendor management generally include policies and procedures related to: (i) conducting due diligence for vendor selection; (ii) monitoring and overseeing vendors, and contract terms; (iii) assessing how vendor relationships are considered as part of the organization's ongoing risk assessment process as well as how the organization determines the appropriate level of due diligence to conduct on a vendor; and (iv) assessing how vendors protect any accessible client information.

OCIE has observed the following practices in the area of vendor management by organizations:

- **Vendor Management Program.** Establishing a vendor management program to ensure vendors meet security requirements and that appropriate safeguards are implemented. Leveraging questionnaires based on reviews of industry standards (*e.g.*, SOC 2, SSAE 18) as well as independent audits. Establishing procedures for terminating or replacing vendors, including cloud-based service providers.
- **Understanding Vendor Relationships.** Understanding all contract terms including rights, responsibilities, expectations, and other specific terms to ensure that all parties have the same understanding of how risk and security is addressed. Understanding and managing the risks related to vendor outsourcing, including vendor use of cloud-based services.
- **Vendor Monitoring and Testing.** Monitoring the vendor relationship to ensure that the vendor continues to meet security requirements and to be aware of changes to the vendor's services or personnel.

TRAINING AND AWARENESS

Training and awareness are key components of cybersecurity programs. Training provides employees with information concerning cyber risks and responsibilities and heightens awareness of cyber threats. OCIE has observed the following practices used by organizations in the area of cybersecurity training and awareness:

- **Policies and Procedures as a Training Guide.** Training staff to implement the organization's cybersecurity policies and procedures and engaging the workforce to build a culture of cybersecurity readiness and operational resiliency.
- **Including Examples and Exercises in Trainings.** Providing specific cybersecurity and resiliency training, including phishing exercises to help employees identify phishing emails. Including preventive measures in training, such as identifying and responding to indicators of breaches, and obtaining customer confirmation if behavior appears suspicious.
- **Training Effectiveness.** Monitoring to ensure employees attend training and assessing the effectiveness of training. Continuously re-evaluating and updating training programs based on cyber-threat intelligence.

ADDITIONAL RESOURCES

We are committed to working with federal and local partners, market participants, and others to monitor developments and effectively respond to cyber threats. In addition to checking the SEC's Cybersecurity Spotlight page (www.sec.gov/spotlight/cybersecurity), OCIE encourages SEC registrants, issuers, other regulated entities, and investment professionals, as well as other members of the cybersecurity community, to sign up for alerts published by the Cyber Infrastructure Security Agency (CISA), which is part of the U.S. Department of Homeland Security. CISA is responsible for protecting the nation's critical infrastructure from physical and cyber threats, and collaborates and coordinates among a broad spectrum of government and private sector organizations.

The following link can be used to sign up for CISA alerts: https://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new.

In addition to receiving CISA Cyber Alerts, many organizations participate in information-sharing groups through industry associations such as the Financial Services Information Sharing and Analysis Center (FS-ISAC, www.fsisac.com). Participation in these information sharing groups provides a mechanism for collaborating across industry and government—providing access to sector specific information about cyber best practices and early warning indicators related to cyber threats. Through such information sharing arrangements, OCIE believes that organizations are able to achieve greater cybersecurity resiliency.

Another key resource developed through the collaboration between government and industry is the National Institute of Standards and Technology Cybersecurity Framework (https://www.nist.gov/cyberframework). This voluntary framework provides a mapping of cybersecurity control objectives to industry standards, guidelines, and practices designed to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

CONCLUSION

In sharing these staff observations, we encourage market participants to review their practices, policies and procedures with respect to cybersecurity and operational resiliency. We believe that assessing your level of preparedness and implementing some or all of the above measures will make your organization more secure. OCIE will continue to focus on working with organizations to identify and address cybersecurity risks and encourages market participants to actively engage regulators and law enforcement in this effort.

U.S. Securities and
Exchange Commission
100 F Street NE
Washington, DC 20549
SEC.gov