Deloitte.

The SEC's Focus on Cybersecurity

Key Insights for Investment Advisers

The growing number and complexity of cybersecurity risks facing investment advisers (IAs) has triggered an increased interest in cyber risk management by the United States Securities and Exchange Commission (SEC). Cyber risks and the SEC's related focus are particularly relevant for mutual funds, hedge funds, and private equity managers.

It is clear that cybersecurity is not just an information technology issue. Rather, cybersecurity represents a challenge that has broader business, operations, regulatory, and risk implications for IAs. Many of these implications arise from the additional risks associated with third parties that may make up the extended enterprise (e.g., prime brokerage, transfer agent, and distribution operations), the repercussions of external disclosure of trading and investment strategies, and brand damage resulting from the loss of sensitive data.

Traditional methods of addressing cyber risks have focused predominantly on preventing cyber incidents through defensive security strategies (e.g., "defense in depth"), often through a compliance-oriented lens. While breach prevention remains paramount, our approach to advising IA clients on cyber risk emphasizes the importance of understanding the landscape of existing and emerging threats, focusing a comprehensive cyber program on threats of greatest potential impact to the IA's particular business, and establishing agility in detecting and responding to attacks. The end goal is for IAs to remain secure, vigilant, and resilient against cybersecurity threats.

Secure: Focusing security controls, preventive measures, and compliance initiatives on high-risk assets.

Vigilant: Maintaining a high level of situational awareness about the types of attacks that might occur, threat trends across industry sectors, and an IA's specific business risks.

Resilient: Acknowledging the certainty that a cyber incident will occur and having the capacity to rapidly contain the damage and mobilize the cross-functional business and technical resources needed to minimize the impact of the attack.

Each organization's unique cybersecurity program requires active risk-and-threat-aware governance to adjust as the business, technology, and threat landscapes change. It is important for IAs to establish a program to become secure, vigilant, and resilient, that holistically addresses the regulatory aspects of cybersecurity readiness. The SEC has consistently reinforced its expectations in the cyber arena in 2014, including as part of its published examination priorities, in a cybersecurity-dedicated Risk Alert as well as in other communications and initiatives.

Background

Cybersecurity was highlighted early in the year as part of the 2014 National Exam Program (NEP) Examination Priorities released by the SEC's Office of Compliance Inspections and Examinations (OCIE).[1] Subsequently, OCIE's cybersecurity priorities were discussed in more detail in connection with the SEC's Compliance Outreach Program (the "Outreach").[2] During the Outreach, members of OCIE's leadership communicated a strong interest in assessing two areas: the adequacy of resources IAs spend to manage cybersecurity risks and the effectiveness of policies and procedures (P&Ps) designed to mitigate these cyber risks.

In March 2014, the SEC held its first-ever Cybersecurity Roundtable (the "Roundtable").[3] Leading cybersecurity risk management practices identified by SEC staff during the Roundtable include (i) implementing a formal written response plan separate from business continuity plans to address cybersecurity incidents and data breaches, (ii) conducting penetration tests, documenting the results, and addressing areas for improvement, (iii) risk-prioritizing sensitive data and critical infrastructure and identifying appropriate process and security controls to protect the data and infrastructure, and (iv) engaging in peer intelligence sharing, rather than viewing cybersecurity as a competitive advantage.[4]

[1] For the last two years, OCIE has published the NEP Examination Priorities, signaling to the industry the areas upon which SEC examiners will focus in that particular year. The 2014 NEP priorities were released in January and can be found at http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2014.pdf.

[2] A description of the Outreach can be found at https://www.sec.gov/info/complianceoutreach_ia-funds.htm. One component of the Outreach is a National Seminar highlighting compliance-related issues that are relevant to chief compliance officers (CCOs) and other senior executives of IAs and investment companies. In 2014, the National Seminar took place on January 30th.

[3] Additional information about the Roundtable can be found at http://www.sec.gov/spotlight/cybersecurity-roundtable.shtml.

[4] This may include participation in industry groups (e.g., the Financial Services Information Sharing and Analysis Center).

In April 2014, OCIE released a Risk Alert highlighting its cybersecurity initiative that includes a planned sweep of over 50 registered IAs and broker-dealers focusing on cybersecurity.[5] The Risk Alert builds on prior SEC cyber guidance and contains important information regarding OCIE's examination expectations.

Outlined below are key considerations arising from the Risk Alert in preparing for an OCIE cybersecurity examination and leading practices for IAs to utilize when addressing cybersecurity threats.

OCIE cybersecurity exams

In the Risk Alert, OCIE provided a sample document request that details the areas, divided into six categories, that OCIE examiners plan to evaluate when conducting cybersecurity exams. Deloitte[6] believes this information is important for IAs, not only because it may help compliance personnel prepare for the SEC cybersecurity sweep, but also because the documents contained in the sample document request describe the underlying processes and controls examiners expect IAs to have in place to address cybersecurity threats. By understanding the documentation and the underlying processes and controls, IA professionals can assess the effectiveness of existing supervisory, compliance, and risk management systems and controls, identify vulnerabilities, and implement changes to mitigate such vulnerabilities.

1. Identification of risks/cybersecurity governance

Examples of the types of documentation examiners may request as part of the sweep with respect to an IA's risk identification processes and overall approach to cybersecurity governance include (i) documentation of a formalized cybersecurity governance structure and operating model, (ii) formal security P&Ps, and (iii) cyber insurance documentation. In this regard, the SEC staff has highlighted the importance of reviewing, testing, and updating cybersecurity playbooks and P&Ps frequently.[7]

Deloitte believes that IAs should be able to demonstrate to examiners a clear accountability for managing cybersecurity risks that is documented and reinforced by effective P&Ps. IA professionals should also have a deep understanding of the composition of the computing environment (including, for example, areas that are accessed by third parties), the data that resides within the environment, and the importance of the firm's technology infrastructure and data resources to the IA's overall business and individual client relationships. A leading practice that IAs should consider is assessing whether the internal configuration/reporting lines make sense for the business and dedicating personnel with accountability for managing cybersecurity within a well-defined operating model that engages the business units.

In connection with cyber insurance, a leading practice that IA professionals should consider is periodically reviewing the firm's cyber insurance strategy. This approach will not only address OCIE's interest in reviewing cyber insurance documentation, it should also assure that current cyber insurance coverage meets the IA's business requirements. This practice is particularly important because a cyber insurance strategy, not unlike the complexity of cyber risks, can change rapidly as a result of evolving IA-specific and/or insurance industry requirements.

2. Protection of firm networks and information

When assessing an IA's ability to protect firm networks and information, some of the documents examiners may request include (i) documentation supporting the use of published cybersecurity risk management process standards, including those issued by the National Institute of Standards and Technology (NIST)[8] and the International Organization for Standardization for security architecture and processes, (ii) "classic" security controls, including training and awareness, access management and certifications, patch management, data protection-in-transit/at-rest, distributed denial of service protection, secure software development life cycle, and resilience planning and testing, and (iii) compliance with P&Ps.

Deloitte believes IAs will likely need to demonstrate to examiners their understanding of relevant risk management process standards and controls. In particular, IAs will likely need to demonstrate that their existing security architecture is comprehensive and leverages

[5] NEP Risk Alert on OCIE Cybersecurity Initiative, released April 15, 2014, and available at: http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf.

[6] As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

[7] Roundtable.

[8] The NIST Framework for Improving Critical Infrastructure Cybersecurity resulted from the Executive Order on Critical Infrastructure (CI) released by the White House in February 2013 in an effort to "promote partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk based standards." NIST was directed to produce a framework that could improve the cybersecurity posture of CI operators. Deloitte professionals facilitated NIST Cybersecurity Framework Workshops, leveraged our experience in cybersecurity policy and risk management standards by contributing to several sections of the framework document and met with chief information officers and chief information security officer level operators of CI to discuss the framework. As a result of this executive outreach effort, Deloitte collected C-suite feedback and provided recommendations to NIST to enhance and/or broaden its adoption.

a standards-based approach, that data is protected across the data management lifecycle (including data destruction), that employees have a current understanding of how to properly manage data and that effective data access controls are in place (i.e., that only those who require access to specific data have access). The SEC staff has also highlighted training as a key component of network and information protection.[9] IA professionals should train staff on topics pertaining to sensitive information and implement controls to contain information within the firm's infrastructure, including controls around safe usage, management, and storage of sensitive data (e.g., printing, emailing, and storing in shared files). The scope of the training should also include procedures for working with third parties.

Deloitte believes that in addition to developing and implementing training, a holistic approach to protecting firm networks and information requires IAs to assess the current talent mix to determine employees' familiarity with cybersecurity risks and analyze the organization's hiring strategy to determine whether the organization should be seeking new and/or different cyber resources.

3. Risks associated with remote customer access and funds transfer requests

To assess how an IA manages risks associated with remote access and fund transfer requests, OCIE examiners may request documentation of fraud controls (e.g., multifactor authentication and standard operating procedures governing fraud management).

Deloitte believes that IAs should be able to demonstrate to examiners that effective controls are in place to provide safe and secure online access to clients and that the IA's technology infrastructure includes secure customer verification mechanisms. In addition, for IAs, including those to mutual funds, hedge funds, and private equity funds, the business ecosystem is a sophisticated extended enterprise comprising systems directly owned and operated by the IA and systems owned and operated by multiple third parties. Deloitte believes that with the increasing complexity of the extended enterprise, IAs face the substantial challenges of connecting (in a somewhat trusted manner) to environments that they do not control. Accordingly, IAs must enhance monitoring capabilities to better differentiate between normal and anomalous behavior since traditional authentication methods may not detect or prevent every compromise. Detection of anomalous behaviors often requires leveraging and correlating many different data points (e.g., using geo-location data to determine if an unauthorized party is accessing the IA's systems from an atypical location).

4. Risks associated with vendors and other third parties

OCIE examiners may request documentation of third-party security assessments and third-party oversight when assessing an IA's management of risks associated with vendors and other third parties.

Third-party risks are heightened in the investment management context given the key functions that may be outsourced to third parties. Accordingly, we believe that it is imperative for IAs to establish a secure extended enterprise that incorporates an approach to managing vendor and third-party risks. The approach should emphasize the IA's ownership of third-party risks and acknowledge that although certain functions can be outsourced, cybersecurity risks associated with doing business with third parties cannot be outsourced.

5. Detection of unauthorized activity

Examples of the types of documentation examiners may request when assessing processes and controls that are designed to detect unauthorized activity include (i) threat awareness, (ii) threat detection, (iii) event correlation, (iv) data loss prevention, and (v) penetration/vulnerability testing.

We believe that one aspect of cyber risk management that may be particularly challenging is determining that measures designed to mitigate cybersecurity risks are consistent with the IA's overall enterprise risk model (i.e., that continuity exists between the two). Cybersecurity professionals, such as incident responders, security operations center personnel, security architects, ethical hackers, internal compliance audit professionals, and chief information security officers, for example, may not speak the language of enterprise risk professionals, including chief risk officers and their teams, and vice versa. Potential consequences of such a communication gap include the misidentification of or the failure to identify specific risks to which the IA may be exposed. IA professionals need to provide cyber risk guidance to technical teams who translate the guidance into continuously adapted effective operational capacities.

IAs should also be able to demonstrate to OCIE examiners the existence of active, holistic monitoring activity processes and, as noted above, that professionals across business functions have an understanding of normal/expected activity and unauthorized activity and know how to respond to activity that does not appear normal or expected.

[9] Roundtable

6. Other Information (e.g., experiences with certain cybersecurity threats)

Examples of other types of documentation examiners may request in connection with the cybersecurity sweep include (i) written supervisory procedures that include those that comply with the Identity Theft Red Flag Rules under Regulation S-ID,[10] (ii) documentation of prior security incidents (e.g., malware, spear phishing, rogue employees, and fraud), (iii) documentation of loss of client information, and (iv) documentation of threat intelligence monitoring for insider threats (i.e., privileged user monitoring) and global threats (i.e., actors, malware, phishing).

Deloitte believes examiners' interest in reviewing these documents is consistent with our secure, vigilant, and resilient approach to managing cyber risks. Specifically, tracking prior cyber incidents, the loss of client information, and continuous monitoring for insider threats should help position IAs to better understand and remediate potential weaknesses in their cybersecurity infrastructure.

Conclusion

Deloitte expects the SEC and its staff to continue to focus on cybersecurity, particularly as the results of the sweep exams unfold. Given the fast and evolving pace of cyber threats, long-term implementation plans designed to address cybersecurity risks over the near to mid-term may become obsolete very quickly. As a consequence, it is critical that IAs not only meet SEC expectations in the cybersecurity arena, but also invest in a program to become secure, vigilant, and resilient in the face of emerging cybersecurity risks.

Deloitte has a dedicated team of professionals who advise IAs about how to manage cybersecurity risks. Our team is composed of individuals with technical cyber risk expertise, enterprise risk management experience, and deep investment management regulatory knowledge, who can help IAs to address the issues raised in this piece.

Contacts:

Leadership

Patrick Henry
Vice Chairman
U.S. Investment Management Leader
Deloitte & Touche LLP
+1 212 436 4853
phenry@deloitte.com

Paul Kraft
U.S. Mutual Fund Leader
Deloitte & Touche LLP
+1 617 437 2175
pkraft@deloitte.com

Ed Powers
National Managing Partner
Cyber Risk Services
Deloitte & Touche LLP
+1 212 436 5599
epowers@deloitte.com

Authors

Vikram Bhat
Principal
Deloitte & Touche LLP
+1 973 602 4270
vbhat@deloitte.com

Mark Nicholson
Principal
Deloitte & Touche LLP
+1 201 499 0586
manicholson@deloitte.com

Garrett O'Brien
Principal
Deloitte & Touche
+1 212 436 5250
gobrien@deloitte.com

Peter Poulin
Principal
Deloitte & Touche LLP
+1 617 585 5848
pepoulin@deloitte.com

Daniel Soo
Principal
Deloitte & Touche LLP
+1 212 436 5588
dsoo@deloitte.com

Megan Roudebush
Manager
Deloitte & Touche LLP
+1 312 486 0826
mroudebush@deloitte.com

[10] Regulation S-ID, available at http://www.sec.gov/rules/final/2013/34-69359.pdf, requires financial institutions to implement a written Identity Theft Prevention Program. The SEC staff has also emphasized the importance of complying with Regulation S-P in connection with cyber risks. Regulation S-P, available at http://www.sec.gov/rules/final/34-42974.htm, imposes notice requirements and restrictions on a financial institution's ability to disclose nonpublic information about consumers.