ALSTON & BIRD

WWW.ALSTON.COM

Cybersecurity Preparedness & Response and Investment Management, Trading & Markets ADVISORY ■

JULY 11, 2018

SEC Prioritizes Data Security and Expects More Mature Cybersecurity Programs

by Kim Peretti, Tim Selby, and Kate Hanniford

In the first half of 2018, the Securities and Exchange Commission (SEC) has reaffirmed its focus on data security and the importance of cybersecurity preparedness through its draft Strategic Plan for fiscal years 2018 through 2022 and interpretative guidance for public company disclosures. Taken together with preexisting guidance, it is clear that the SEC expects more mature cybersecurity programs from its registrants and that it will continue to prioritize data security as fundamental to the U.S. capital markets and market participants.

Multiple divisions and offices of the SEC have now provided guidance and a series of risk alerts regarding its cybersecurity regulations, including the Office of Compliance Inspections and Examinations (OCIE), Division of Investment Management, and, most recently, Division of Corporation Finance. In addition to numerous speeches by commissioners and division directors and an enhanced website, the SEC's approach to cybersecurity risk management and compliance continues to leverage existing regulations and statutes to police market participants' preparedness and responses to new and emerging cyber threats.

Because of the importance of "data collection, storage, analysis, availability, and protection," market participants can expect the SEC to continue to use all tools at its disposal to ensure that market participants "are actively and effectively engaged in managing cybersecurity risks" for the foreseeable future. In addition, the SEC will seek to ensure that market participants as well as public companies "are appropriately informing investors and other market participants of these risks and incidents." For instance, public companies are expected to disclose material risks and material cybersecurity events, a process that usually depends on internal procedures and controls for assessing materiality and disclosure thresholds. For public companies not otherwise subject to OCIE examination, the SEC has limited its activities to the oversight of disclosures via enforcement action in cases where it has deemed the disclosure of a material cybersecurity event to have been inadequate.

Investment Advisers and Broker-Dealers Under Scrutiny

Written guidance, OCIE examinations of investment advisers and broker-dealers, and the increasingly active Division of Enforcement's Cyber Unit are the key ways the SEC is addressing cybersecurity preparedness for its registrants. In recent remarks, SEC Chairman Jay Clayton reiterated the work of the Division of Enforcement's Cyber Unit, and in particular

noted that intrusions into online retail brokerage accounts are an area of focus for the specialized unit. Coupled with the FBI's recent release of its 2017 Internet Crime Report, it is clear that both regulators and law enforcement are focused on cybersecurity threats that rely on investment services platforms and resources to target or harm the investing public. For registered investment advisers and broker-dealers, the primary implication of this focus is that the SEC will continue to expect more mature cybersecurity programs that adapt to the changing threat environment and appropriately manage and communicate risks to investors and other market participants, as discussed below.

Over the last three years, the SEC has sanctioned firms for a range of specific alleged cybersecurity-related violations. These have included the reliance on ineffective limitations on access rights that failed to prevent a firm employee from inappropriately accessing confidential customer data and for failing to audit or test those limitations to access rights. Other allegations have included the failure to conduct periodic risk assessments, employ firewalls to protect servers that contain sensitive personally identifiable information (PII), encrypt PII at rest, and establish procedures for responding to a cybersecurity incident. The SEC has also brought an action alleging that an adviser's policies and procedures failed to designate a responsible supervisor and address how customer records and information are to be handled when transmitted, were incomplete, and were not tailored to the actual practices of a firm.

The SEC continues to be focused on technology-based market disruptions as well. In June 2016, the Division of Investment Management released guidance following an August 2015 market disruption caused by a systems malfunction at a financial institution that affected hundreds of mutual funds and exchange-traded funds. The SEC guidance noted that "some funds could have been better prepared for the possibility that one of their critical service providers would suffer an extended outage." The guidance suggested that advisers of fund complexes, CCOs, and fund boards should reexamine their oversight of critical service providers as they strengthen their business continuity and disaster recovery plans, with a particular focus on communications protocols across the fund complex, with the board, and externally with the affected service provider and other stakeholders. The guidance highlighted the importance of understanding how the business continuity plans of the critical service providers relate to the fund and how that impacts the fund's backup procedures. Finally, the guidance suggested that funds consider how a variety of critical service provider disruptions could impact fund operations and investors and to be prepared to manage the response, whether the disruption occurs at a critical service provider or at the fund itself.

The SEC's settlement with the New York Stock Exchange (NYSE) and its affiliated exchanges earlier this year underscores the degree to which there can be serious consequences for the failure to maintain backup and recovery capabilities. In its first enforcement action based on alleged violations of Regulation SCI, which applies to self-regulatory organizations (SROs) and certain alternative trading systems, among others, the SEC fined the NYSE exchanges $14 million for violations of Regulation SCI and other provisions specifically applicable to automated trading centers and SROs. The March 2018 settlement order alleges that the NYSE exchanges failed to meet Regulation SCI's minimum requirements for business continuity and disaster recovery from its compliance date of November 2015 through late November 2016.

Although unregistered initial coin offerings have dominated the more recent cybersecurity-related enforcement efforts, rather than the kind of Regulation S-P or Regulation S-ID violations described above, for example, OCIE examiners continue to prioritize cybersecurity preparedness. Senior SEC officials have stated that the failure to maintain reasonably designed cybersecurity policies and procedures presents an enforcement risk and that OCIE and the Division of Enforcement coordinate closely on these issues. For SEC registrants, this can be a challenging area of compliance both due to the rapid evolution of cybersecurity threats on one hand and the pace and expense of technological innovation to respond to those threats on the other. Striking the right balance in reasonable design

can be difficult. Although the SEC relies on flexible standards for compliance and, ultimately, enforcement, gauging whether a registrant's practices continue to meet the reasonableness standard over time involves an appreciation of the need to reassess and boost cybersecurity preparedness as appropriate, subject to the reality of financial and operational constraints. Given that the reasonableness standard is not defined, OCIE guidance and enforcement actions provide useful insights to benchmark the standard for reasonable design.

Practical Considerations

The evolution of OCIE's guidance suggests that the SEC is focused on more mature topics of cybersecurity. Earlier guidance focused on basic cyber hygiene and empowering compliance professionals by providing questions they could use to assess their firms' cybersecurity preparedness. In contrast, newer guidance summarizes the improvements to firms' cybersecurity preparedness that OCIE examiners have observed over the past couple of years and for some topics assumes basic measures—such as policies and procedures to protect customer data—are already in place but could be strengthened.

As OCIE's Cybersecurity Initiative approaches its fifth year, it has offered increasingly detailed guidance on the relative strength of registered investment adviser, investment company, and broker-dealer cybersecurity programs. In contrast to early Cybersecurity Initiative risk alerts that focused on high-level compliance topics and the establishment of cybersecurity programs with written policies and procedures, more recent risk alerts focus on the adequacy of measures already in place and the need to periodically reassess and adapt to evolving threats and technological advancements, signaling raised expectations for the relative sophistication of examined entities' cybersecurity programs. OCIE is expected continue to prioritize cybersecurity, and the SEC's draft Strategic Plan suggests that OCIE will continue its current trend of increasing the number of examinations it performs each year, particularly given the rapid growth in the investment adviser sector.

In its most recent guidance, OCIE has identified certain hallmarks of robust cybersecurity programs:

- Maintenance of an inventory of data, information, and vendors so that a firm has identified all assets that are to be protected and it can manage and apply information security to those assets as appropriate.
- Third-party vendor management that includes the classification of risks, vulnerabilities, data, business consequences, and information regarding each service provider and vendor, as appropriate.
- Detailed cybersecurity-related procedures that specifically address penetration testing, security monitoring and system auditing, access rights, and incident reporting.
- Maintenance of prescriptive schedules and processes for testing data integrity and vulnerabilities. This includes performing vulnerability scans of core IT infrastructure and prioritizing any resulting action items that relate to the firm's key systems. For patch management, this includes beta testing of a proposed patch with a subset of users and servers before full deployment, an analysis of the problem the patch is intended to address and any risks associated with the patch, and the method in which the patch will be applied.
- Established and enforced controls to access data and systems. These include policies and procedures for acceptable use, restrictions, and controls for mobile devices that connect to a firm's systems, prompt termination of access for separated employees, and the enforcement of those policies, procedures, and restrictions. This also includes periodically requiring third-party service providers to provide logs of their activities on the firm's networks.

- Mandatory periodic employee training so that employees are aware of cybersecurity risks as well as their obligations under firm policies and procedures.
- Engaged senior management so that senior members of the firm vet and approve the cybersecurity policies and procedures.

In addition to identifying certain elements that indicate a strong controls environment, OCIE has also flagged certain issues as raising Regulation S-P compliance concerns, in which case market participants may not be adequately safeguarding customer records or information. Specifically, OCIE has identified inadequate system maintenance, including latency in patch and vulnerability management, as a general area of concern based on its examinations. Similarly, the use of outdated operating systems that cannot support necessary security patches and the failure to timely and fully remediate high-risk findings from penetration testing or vulnerability scans also raise compliance concerns. Finally, the recent settlement with the NYSE exchanges serves as a useful reminder for SEC registrants to continue to maintain recovery and resiliency capabilities that are aligned with industry standards, even if not directly subject to Regulation SCI.

Because OCIE may identify deficiencies and the Division of Enforcement may pursue actions even if there is only a risk of harm due to inadequate safeguards, market participants may find that by focusing their efforts on proactive system maintenance (i.e., patch and vulnerability management) to meet or exceed OCIE expectations for robust controls as listed above, as well as for vulnerability detection and management policies and procedures, they are better positioned to identify and remediate cybersecurity threats. Coupled with diligent attention to recovery and resiliency planning, market participants may also be in a stronger position to demonstrate the reasonable design of their cybersecurity programs.

The Global Reach of Regulators

The SEC draft Strategic Plan explicitly reiterates the global reach of cybersecurity risk and the technological interdependency in both the U.S. and global securities markets more broadly. In this way, the draft Strategic Plan, together with recent guidance, has cemented the issues of data security and data transmission as applicable to all SEC registrants, not simply those with critical market infrastructure. Similarly, the implementation of the EU General Data Protection Regulation (GDPR) as of May 25, 2018, significantly widens the scope of regulatory oversight of securities market participants and beyond. The GDPR applies extraterritorially to any entity that offers goods or services to EU data subjects or processes EU data subject personal data for purposes of monitoring underlying EU data subjects.

Given the breadth of the regulation, entities that obtain any EU-sourced personal data in connection with offering goods or services to EU data subjects or profiling EU data subjects may want to assess whether they can be considered data controllers or processors under the GDPR and therefore subject to restrictions and conditions for how, when, and why they handle personal data, and to investigation and sanction for violations. In addition, U.S. entities may find that even if they are not directly subject to the GDPR, their clients are. It is also possible that U.S. affiliates of companies with a European presence may choose to comply with the GDPR in the interest of enterprise-wide consistency. Investment advisers and broker-dealers that contract with or provide services to clients that qualify as controllers or processors under the GDPR may be required to implement additional data security measures—such as pseudonymization and encryption of personal data and enhanced resiliency capabilities—even when otherwise fully compliant with applicable SEC regulations. While the GDPR's enforcement mechanism is relatively untested and the full impact of implementation is yet to be determined, the GDPR presents a dramatic shift in expectations for data security and data privacy compliance for U.S.-based entities that will be subject to its application.

You can subscribe to future *Cybersecurity Preparedness & Response* and *Investment Management, Trading & Markets* advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information please contact your Alston & Bird attorney or any of the following:

Cybersecurity Preparedness & Response

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

Jim Harvey
404.881.7328
jim.harvey@alston.com

Investment Management, Trading & Markets

David Baum
202.239.3346
david.baum@alston.com

Willa Bruckner
212.210.9596
will.bruckner@alston.com

Kristin Hinson
704.444.1332
kris.hinson@alston.com

Laura Pruitt
202.239.3618
laura.pruitt@alston.com

Michael Saarinen
212.210.9441
michael.saarinen@alston.com

Timothy Selby
212.210.9494
tim.selby@alston.com

Follow us: @AlstonPrivacy | www.AlstonPrivacy.com

www.alstonsecurity.com

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86 10 8592 7500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: 2828 North Harwood Street ■ 18th Floor ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ 5th Floor ■ East Palo Alto, California, USA, 94303-2282 ■ 650-838-2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333