SQUIRE
PATTON BOGGS

Cybersecurity Alert: SEC Staff Weighs in on Common Issues and Best Practices

Following an initiative in which the Securities and Exchange Commission (SEC)'s Office of Compliance Inspections and Examinations examined cybersecurity practices at 75 SEC-registered firms, the SEC staff issued a Risk Alert highlighting observations of common issues and best practices on August 7, 2017.[1] The Risk Alert provides a useful guidepost for any financial services firm evaluating its cybersecurity program.

Most regulatory agencies, including the SEC, have not prescribed cybersecurity program requirements that regulated entities must implement. As a result, companies are left to piece together what regulators might look for in a cybersecurity program, especially in the wake of a breach. In the absence of detailed regulatory requirements, companies will want to pay particular attention to the guidance offered by this Risk Alert.

An Improved Baseline

The SEC staff's cybersecurity exam initiative was the second such initiative in the last three years. In this most recent sweep, the SEC staff focused particularly on (1) the examined firms' written policies and procedures regarding cybersecurity; (2) the implementation and operation of those policies and procedures; and (3) the firms' level of preparedness for cybersecurity risks and events.

As compared to a 2014 sweep, the SEC staff noted that a majority of the firms examined had basic cybersecurity program components in place. In particular, they observed that most, if not all, firms:

- Documented their policies to address shareholder/customer records
- Conducted periodic risk assessments, penetration tests and vulnerability scans
- Used data loss prevention tools
- Scheduled system maintenance procedures to ensure current security patches were applied to systems
- Developed incident response plans
- Evaluated vendors' cybersecurity programs

We recommend that companies ensure that their cybersecurity programs feature these elements at a bare minimum.

Common Issues

Despite these improvements, the SEC staff noted common shortcomings among the firms that they examined. In particular, the Risk Alert highlights two fundamental issues.

First, the SEC staff observed a frequent disconnect between the firms' written policies and procedures and the facts on the ground. They noted, for example, that policies and procedures were often not reasonably tailored to firms' actual operations and offered little guidance on how employees should implement the policies and procedures in practice. The SEC staff also observed many instances in which protocols called for by the firms' policies (such as periodic security reviews) were not actually followed and purported mandates (such as employee training) were not enforced.

We strongly recommend developing policies and procedures that apply to your organization, implementing such policies and procedures, and periodically auditing implementation to ensure continued adherence to policies.

Second, the SEC staff observed that firms failed to take steps to protect their systems from *known* cybersecurity risks. For instance, they noted that some firms designed system maintenance schedules to ensure security patches would be applied, but ran outdated operating systems for which manufacturers were no longer providing security patches, creating ongoing, high-risk vulnerabilities. They also noted instances in which firms neglected to remediate significant risks that had been identified by their own penetration tests and vulnerability scans.

Best Practices

Importantly, the Risk Alert also highlights six elements that the SEC staff noted at firms with robust cybersecurity controls and invites other firms to consider these elements in connection with their own cybersecurity programs.

1. **Cybersecurity Asset Inventory**: The SEC staff noted that some policies and procedures included a complete inventory of data, information and vulnerabilities (including all vendors with access to such data and information). An asset inventory is often viewed as an important initial component of a cybersecurity program. While creating such an inventory can be a complex exercise, it brings significant value and efficiency to incident response efforts.
2. **Detailed Instructions**: The SEC staff observed that some policies and procedures contained detailed information about firm systems as well as instructions in order to facilitate penetration testing, periodic system monitoring, and breach reporting. They also favorably viewed detailed access control policies, including documenting requests for heightened system access.

[1] *See* OCIE, *Observations from Cybersecurity Examinations* (Aug. 7, 2017) (available at https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf).

3. **Schedules and Processes for Testing Data Integrity and Vulnerabilities**: In this area, the staff commented favorably on policies requiring methodical evaluation and beta testing of security patches before their implementation.
4. **Strong Access Controls**: The SEC staff observed that firms with robust cybersecurity programs established and enforced controls for mobile access to their systems, required vendors to provide periodic logs of activity on the firms' networks and promptly cut off access rights for terminated employees. This requires close coordination between IT and HR, so that IT can immediately disable account and device access when an employee has departed.
5. **Mandatory Training**: The SEC staff noted that some firms required all new employees to complete information security training and required periodic refresher training thereafter. They also noted that those firms adopted measures to ensure actual *compliance* with their training requirements.
6. **Senior Management Engagement**: Lastly, the SEC staff observed that senior management at the firms with robust cybersecurity programs vetted and approved their firms' policies and procedures. Establishing a well-crafted cybersecurity governance function in a firm ensures top-down enforcement of cybersecurity mandates.

Conclusion

The SEC staff's general observation that organizations' cybersecurity programs are more mature in 2017 than they were in 2014 is generally true across most sectors. It is important to recognize, however, that formalizing and documenting security policies and procedures, while essential, is only the first step in building a strong program. Policies must be tailored to your organization and followed in practice. Companies can test their policies and procedures by conducting mock exercises and seeking review of such policies and procedures – as documented and implemented – by outside experts.

We help organizations identify what they are missing, create appropriate business cases for improvements and build resilience around a company's cybersecurity protocols. This will help avoid significant reputational harm and other costs down the road – whether from the SEC, other regulators, international authorities, customers or partners.

Contacts

Tara Swaminatha
Partner, Data Privacy & Cybersecurity
Washington DC
T +1 202 457 6031
E tara.swaminatha@squirepb.com

Coates Lear
Principal, Government Investigations & White Collar
Washington DC/Denver
T +1 303 894 6141
E coates.lear@squirepb.com

The contents of this update are not intended to serve as legal advice related to individual situations or as legal opinions concerning such situations, nor should they be considered a substitute for taking legal advice.