ThompsonKnight

Client Alert *February 6, 2020*

THE SEC PROVIDES A ROADMAP TO BETTER CYBERSECURITY

Businesses seeking cybersecurity advice encounter a cascade of disparate, often conflicting advice. Some advice doesn't go far enough – patching software frequently and requiring the use of complex passwords are necessary but not sufficient – and some advice is too elaborate to be meaningful. Not every business is ready to implement the 50-page NIST framework in full or to adopt ISO 27001 standards.

The SEC's latest cybersecurity report can help. The SEC's Office of Compliance Inspections and Examinations ("OCIE") has been reviewing the cybersecurity efforts of broker-dealers, investment advisers, and others for more than five years and continues to list cybersecurity as one of its key annual exam priorities (we wrote about OCIE's 2020 examination priorities in a recent Client Alert). On January 27, 2020, OCIE issued a report summarizing the types of cybersecurity practices being implemented by organizations it has reviewed. While the report is presented as a set of observations, SEC Chairman Jay Clayton "encourage[s] market participants to incorporate this information into their cybersecurity assessments," and it is reasonable to expect the SEC to consider these practices to be the baseline for public company cybersecurity programs in the future, including when examining registrants and in connection with investigations and enforcement actions.

In the report, OCIE divides cybersecurity programs into the following seven components and provides examples of common practices for each component:

- **Governance and Risk Management**, including senior level engagement; comprehensive policies and procedures; and continuous testing, evaluation, and policy updates
- **Access Rights and Controls**, including limiting access to sensitive data, requiring strong and periodically changing passwords, and monitoring user access
- **Data Loss Prevention**, including vulnerability scanning, encryption, and securing legacy software
- **Mobile Security**, including mobile device management, multi-factor authentication, and employee training
- **Incident Response and Resiliency**, including developing an incident response plan covering various scenarios, testing and assessing the plan through tabletop scenarios, maintaining back-up data, and considering cybersecurity insurance
- **Vendor Management**, including contract review (particularly for vendor outsourcing and cloud-based services) and vendor monitoring
- **Training and Awareness**, including continuously re-evaluating and updating training programs based on cyber-threat intelligence

For each of the seven component areas, the report elaborates on the practices listed above and several others. Cybersecurity practices observed by OCIE also include monitoring, testing, and updating all aspects of a cybersecurity program, including hardware, software, written policies, and employee training. Companies that once thought of cybersecurity implementation as a one-time business activity (and a one-time expense) must now understand that cybersecurity is an ongoing and critical aspect of business planning, risk-management, and board oversight.

The OCIE report provides a comprehensive and practical checklist of the cybersecurity measures that every company, public or private, should consider adopting. Directors and officers can use this overview as a helpful benchmark by which to assess their company's efforts and identify potential gaps in security. Based on that assessment, management can pursue additional steps that may be necessary.

The SEC's Division of Enforcement has begun investigating and taking action against registrants where there are material lapses in cybersecurity practices that impact investors or the markets. In 2017, the Division of Enforcement launched the Cyber Unit to confront cyber threats throughout the markets. Since forming the unit, the Division has investigated and pursued misconduct involving, for example, cyber intrusions, hacking to obtain material non-public information, and violations of Regulation Systems Compliance and Integrity (Reg SCI). To learn more about the Division's enforcement actions and efforts in the cyber-space, visit https://www.sec.gov/spotlight/cybersecurity-enforcement-actions.

As OCIE points out in its latest report, "the seriousness of the threats and the potential consequences . . . are significant and increasing." Companies must ensure their cybersecurity programs and defenses respond effectively to the threat.

The Cybersecurity and SEC teams at Thompson & Knight can help with most aspects of a cybersecurity program, including developing and testing an incident response plan, reviewing cyber insurance coverage, assessing vendor relationships, and implementing training programs. We work frequently with forensics and other experts who can assist with technical aspects of the program. If you have any questions about implementing a cybersecurity program, please contact the Thompson & Knight attorney with whom you regularly work or one of the attorneys listed below.

CONTACTS:

Jessica B. Magee	**Michael C. Titens**	**Michele (Mitch) L. Gibbons**
214.969.1375	214.969.1437	713.653.8621
Jessica.Magee@tklaw.com	Michael.Titens@tklaw.com	Mitch.Gibbons@tklaw.com

This Client Alert is sent for the information of our clients and friends. It is not intended as legal advice or an opinion on specific circumstances.