Patterson Belknap Webb & Tyler LLP

Privacy & Data Security Alert February 2018

SEC Refreshes Cyber Guidance: Key Takeaways

It's been seven years since the U.S. Securities and Exchange Commission (Commission) issued its initial guidance to public companies on cybersecurity disclosure.

And last week – in the midst of Form 10-K filing season – the Commission released updated interpretive guidance urging companies to be more transparent in disclosing cybersecurity risks in their public filings; to disclose material data security incidents in a "timely fashion;" and to implement safeguards such as trading bans to prevent insiders from selling securities after a breach is detected but before it is publicly disclosed. The guidance also underscores the responsibilities of senior management and boards in cyber risk oversight. While the guidance becomes effective once published in the Federal Register, it makes clear that cybersecurity risk disclosure and management is now one of the top priorities for the Commission.

The SEC's updated guidance reiterates and reinforces the Commission's Staff guidance issued in 2011 by the Division of Corporate Finance, which called for companies to assess what disclosures might be required about cybersecurity risks and incidents. But the new guidance – issued by the Commission itself – underscores the "grave threats to investors" and our financial systems posed by cybercrime and the uptick in the sophistication and severity of cyber-attacks on public companies. It also encourages focused and tailored cyber disclosures based on an assessment of a company's risk profile rather than general boilerplate disclosures.

The updated guidance focuses on four key areas:

Pre-Incident Public Disclosure

Although the updated guidance does not require detailed disclosures about a company's IT systems or vulnerabilities – to avoid giving a roadmap for mischief – but advises a holistic assessment based on the overall materiality of cyber risk to an organization and its operations. In particular, the Commission advises companies to consider among the following in preparing cyber risk disclosures:

- Prior cybersecurity incidents including their severity and frequency
- Probability of incident occurrence and potential magnitude of an incident
- Limitations on the company's ability to prevent or mitigate cyber risk
- Particular industry specific or third-party vendor/supplier risk
- Potential for reputational harm
- Legal risks and costs of enforcement actions by other regulatory bodies (specifically referencing New York's new cybersecurity regulations for financial institutions and insurance companies)

When deemed material, the Commission advises that proxy statements contain disclosures about a board's role and engagement in cyber risk oversight. The Commission also noted that cyber risk disclosures might, depending on the circumstances, be reflected not only in risk factor disclosures but in the company's MD&A, description of its business,

disclosure of legal proceedings, and financial reporting "to provide reasonable assurance that information about the range and magnitude of the financial impacts of a cybersecurity incident would be incorporated into its financial statements…."

Data Security Incident Disclosure

One of the most challenging and practical questions for any organization is the public disclosure of a data security incident. Although the guidance makes clear that timely disclosure of material cybersecurity incidents is required, it concedes that "some material facts may not be available at the time of the initial disclosure." Cooperation with law enforcement and incident investigation – which the Commission acknowledges is "often … lengthy" – will affect the scope of any disclosure. That said, the guidance warned that cooperation with law enforcement or ongoing investigations does not, "on its own," provide a basis for not disclosing a material cybersecurity incident.

Controls and Procedures

As has been the trend with state-level data security regulations, the guidance also focuses on the role of senior corporate leaders and a company's board of directors. To that end, the guidance encourages the following steps:

- Assess existing disclosure controls and procedures to ensure that cyber risk and incident information "is processed and reported" to critical stakeholders "including up the corporate ladder" so that senior management is able to make informed disclosure decisions and compliance certifications, together with controls to assess compliance with such controls and procedures on a regular basis

- If such controls are lacking, develop and implement a process so that important cyber risk and incident information is collected and elevated to senior levels for appropriate decision-making and oversight

Insider Trading and Regulation FD

Finally, the guidance reminds companies of the risk posed by insiders who trade securities between the time a breach is discovered and when it is publicly disclosed. The Commission "encourages" public companies to put in place policies and procedures to prevent trading on material non-public information relating to cybersecurity risks and incidents including trading restrictions to avoid even the "appearance of improper trading during the period following an incident and prior to the dissemination of disclosure."

The Commission encourages "companies to consider how their codes of ethics and insider trading policies take into account and prevent trading on the basis of material nonpublic information related to cybersecurity risks and incidents."

The guidance also warns against disclosing cybersecurity incident information selectively and reminds companies to disclose incident information on Form 8-K to manage the risk of selective disclosure.

Commission Perspective

Commission Chair Jay Clayton, in a statement accompanying the release of the guidance, noted the evolving cybersecurity landscape and said the Staff will "continue to carefully monitor cybersecurity disclosures as part of their selective filing reviews. We will continue to evaluate developments in this area and consider feedback about whether any further guidance or rules are needed."

Two commissioners – Kara M. Stein and Robert Jackson – issued separate statements noting that the new guidance did not go far enough and created "a false sense of comfort that we, at the commission, have done something more than we have."

Key Takeaways

- Revisit and, if necessary, refresh data security related public disclosures to ensure compliance with the new guidance

- Consider adequacy of internal controls and procedures for identifying cybersecurity risks and incidents as part of the design and effectiveness of a company's disclosure controls and procedures

- Update existing enterprise-wide data security policies, plans, and procedures

- Ensure that controls are in place to escalate cyber risk and incident engagement and oversight by senior corporate leaders and the board

- Review data security incident disclosure process to ensure key stakeholders are notified of significant data security incidents and establish a decision-making process and protocol to timely disclose material cybersecurity incidents

- Revise codes of conduct and internal securities trading policies to ensure that, as appropriate, securities trading restrictions are put in place upon the detection of a material cybersecurity incident

We will continue to monitor this area and provide updates as necessary.

Craig A. Newman	**212-336-2330**	**cnewman@pbwt.com**
Herman H. Raspé	**212-336-2301**	**hhraspe@pbwt.com**