



June 2018

Rethinking cybersecurity disclosures to investors

What executives and boards need to know about the SEC's guidance



The Securities and Exchange Commission (SEC) issued interpretive guidance in February 2018 that challenges senior executives and boards of directors to improve disclosures to their investors around cybersecurity risks and incidents. Understanding rising expectations in this arena is critical for companies as cybersecurity threats and incidents continue to grow more frequent and consequential.

Many senior executives and corporate boards face the challenge of answering a new call to action by the Securities and Exchange Commission (SEC) to improve disclosures to their investors around cybersecurity risks and incidents. The call to action came in the form of interpretive guidance on cybersecurity disclosures issued by the SEC in February amid growing market concerns around cyber incidents. How should senior executives and boards respond? Understanding what's new compared to the 2011 staff-level SEC guidance is the first step.

The updated guidance adds two specific considerations that were not addressed in the 2011 guidance:

1. It explains that firms should have policies and controls in place to detect and disclose material cybersecurity risks and incidents, and notes that existing certification requirements for chief executive officers (CEOs) and chief financial officers (CFOs) include certifying the effectiveness of these cyber policies and controls.
2. The guidance says firms should adopt policies to prevent employees from trading with knowledge of nonpublic information regarding cybersecurity risks and incidents, including when there is an ongoing cybersecurity investigation.



The guidance also explains that existing disclosure requirements around board oversight of risk management should include the board's role in overseeing material cybersecurity risks.

Perhaps most notably, the guidance acknowledges that most companies are including cyber-related content in their regular disclosures; however, the SEC noted that such disclosures mainly focus on broad risk factors and contain boilerplate language that does not provide investors with adequate level of detail describing how companies will handle cyber incidents.

To understand what the regulator expects of companies, [the SEC included in its guidance a number of examples of cyber disclosures companies could use when revisiting how they disclose cyber controls and policies.](#)

What the SEC guidance means for business

The SEC has made it clear that firms should be taking cybersecurity controls and policies seriously, informing firms of heightened standards moving forward. Firms should continue reassessing both the content of their disclosures and the controls, policies, and procedures they will use to monitor their cybersecurity risks. At a bare minimum, the SEC has clearly laid out expectations for senior leadership such as the C-level executives to attest to their cybersecurity programs and provide more information to the investing public in regularly scheduled disclosures. Further, the SEC's guidance will likely require additional internal audit functions, including internal assurance programs, performing a deep dive into the cybersecurity program review process.

Unlike companies in other sectors, financial institutions may have a head start addressing the SEC guidance as they have already been working to meet the New York Department of Financial Services' (NYDFS) cyber risk assessment, board reporting, and officer attestation requirements. Specifically, NYDFS requires that financial institutions conduct periodic cybersecurity risk assessments that identify cyber risks, evaluate existing controls, and provide mitigation procedures for such risks – and to have a member of senior management certify they are in compliance with the regulation.

Efforts to comply with the NYDFS requirement that firms present an annual report to the board on cyber risks and the effectiveness of the cybersecurity program will likely help financial institutions comply with the SEC's board oversight guidance.

Next steps for business leaders

Though the SEC's guidance may nudge reluctant firms into reassessing their cyber risk controls and policies, companies hoping to gain the trust of the investing public should have already begun increasing their cybersecurity measures. [A PwC investor survey](#) finds that investors believe cybersecurity should be the top priority for companies, [but only 25% of US consumers say they believe companies handle sensitive personal data responsibly](#).

A key challenge for CEOs is moving from awareness of cybersecurity challenges to proactive management of cyber risks. Only 52% of North American CEOs say they are investing in cybersecurity to a large extent and only 34% of North American CEOs say they are building trust with customers by increasing transparency in data use and storage to a large extent, [according to PwC research](#).

In addition to the SEC's guidance, corporate leaders face demand from the investing public to begin disclosing more information on how their organizations are handling cybersecurity risks.

In order for the board of directors to fulfill their risk oversight responsibility, they should be [holding executives accountable](#) in this area. Executives should have clear, actionable steps to address potential cyber risks and strengthen data privacy and protection. Ultimately, the cybersecurity discussion should be embedded in broader conversations that executives and directors conduct regarding the company's strategic plan.

Action steps executive leaders may want to proactively adopt include advanced authentication technology or cyber attestation reporting. For more information on how business leaders can change their approach to cybersecurity risk management, read [The Global State of Information Security® Survey](#).

Companies should also consider whether they need to revisit or refresh previous disclosures, including during the process of investigating a cybersecurity incident, and whether they need to file a Current Report on Form 8-K relating to information that reasonable investors would want to know.



To have a deeper conversation about the SEC's guidance

Joseph Nocera

Principal
(312) 298 2745
joseph.nocera@pwc.com

Douglas Bloom

Director
(617) 331 5563
douglas.b.bloom@pwc.com

Husam Brohi

Principal
(415) 205 8068
Husam.brohi@pwc.com

Michael Corey

Principal
(415) 498 7402
michael.j.corey@pwc.com