Barley Snyder

How New SEC Guidance on Cybersecurity Risks Could Affect Your Business

PUBLISHED ON
March 8, 2018

While new cybersecurity guidance from the U.S. Securities and Exchange Commission (SEC) only directly affects publicly traded companies, the trickle-down effects could touch a much larger swatch of businesses of any size.

The new interpretive guidance lays out more clear definitions of a "cybersecurity incident" and details cybersecurity disclosure obligations for public companies. However, those public companies likely will require second and third-party vendors to enter into contracts detailing their responsibilities before, during and after an incident, meaning all businesses that deal with publicly traded companies are going to need to familiarize themselves with this guidance.

A "cybersecurity incident" is defined in the guidance as "an occurrence that actually or potentially results in adverse consequences to an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences." The guidance introduces several innovations, including that it comes from the commission level, rather than the staff level like the 2011 guidance issued by the SEC's Division of Corporate Finance. It also discusses the importance of having policies and procedures in place to identify cybersecurity incidents and to evaluate whether public disclosure is required. Related to these policies, the guidance requires procedures and controls for preventing insiders from trading the company's securities after the breach but before public disclosure is made.

The guidance suggests public companies formulate methods for determining the impact of an incident on the company's business, financial condition and results of operations. Investors must be informed of material risks in a timely fashion in the event of an incident, but also kept current through required periodic reports. Procedures for evaluating the significance of a risk or incident are also critical. That might depend on the nature and extent of compromised information, possible harm to customer and vendor relationships and harm to finances and reputation.

Companies that fall victim to cybersecurity incidents - on top of the significant costs of remediation - could face the additional costs of litigation and actions by state and federal authorities. Because of this guidance, publicly traded companies may require their business partners and vendors to have similar procedures in place for identifying risks and evaluating the significance of incidents. They may also seek contractual language that shifts the liability for an incident or the responsibility to remediate to the party responsible for the breach. Therefore, this guidance is instructive for all businesses.

If you have any questions on the new guidance or cybersecurity in general, please contact anyone in the Business Practice Group.