SEC Implements Stricter Cyber Breach Reporting for Public Companies Why Private Companies Also Need to Pay Attention

PUBLISHED ON
July 31, 2023

On Wednesday, July 26, 2023, the U.S. Securities and Exchange Commission (SEC) implemented new rules requiring public companies to disclose certain material cybersecurity incidents within a four (4) day period of discovery. The new rule also requires certain annual reporting around cybersecurity risk management practices and executive experience. The new rules took effect with no surprise to public companies, as the SEC first proposed these new rules in March of 2022. However, private companies may not be immediately aware of these new rules despite these new rules potentially affecting their business relationships with public companies.

We know that private companies often do business with, and are vendors of, public companies. Private company vendors may be critical to a public company - for instance, it may host or process sensitive and/or proprietary information for the public company. The contracts governing these relationships between public and private companies often require the private company vendor to provide notice to the public company of certain material adverse changes to the private company, including the vendor providing notice of cybersecurity incidents to the public company. Often, these requirements included a reporting period that vaguely tie to the public company's legal requirements; for instance, requiring the vendor to provide notice of such circumstances to the public company in order to allow the public company to meet its own legal requirements. Prior to the new SEC rules, the legal requirements regarding cybersecurity incidents and breach notification were governed solely by state laws or more generous federal laws, which allowed breach notification "without unreasonable delay" or within a period of time prescribed by state (which is often 30 days or more). Often, these contracts between public companies and vendors also include indemnification and similar remedies in favor of the public company permitting the public company to seek recourse from the vendor to the extent the vendor's act or omission created liability to the public company. Now that the SEC has implemented this new rule requiring disclosure in as few as 4 days, vendors must complete their own discover and reporting of a cybersecurity incident without delay. A vendor's failure or delay will adversely affect a public company's reporting capabilities, causing the public company to be in violation of these new SEC rules. In such case, a private company vendor could find itself with a terminated contract, reduced revenue, and indemnification liability owing to the public company.

It is worth noting that regulators designed these new rules to help investors make informed investment decisions by providing investors with more information about the cybersecurity risks facing public companies. These new rules also aim to encourage public companies to take steps to improve their cybersecurity posture. Therefore, we should expect that public companies will continue to engage in strict due diligence around vendor management, and will cull

from its stable of vendors whose own cybersecurity posture increases the public company's risk.

If you are a private company doing business with public companies, which includes hosting or processing its sensitive and/or proprietary information, you need to ensure that your own cybersecurity posture is on par with your public company customers in order mitigate this contract risk and to survive the heightened scrutiny and due diligence that public companies will continue to embark on its private company vendors in response to these new rules.

If you have any questions about the SEC's new disclosure rules relating to cybersecurity incidents or have interest in reviewing your business's cybersecurity policies, please reach out to Partner Donald Geiter or any member of the Barley Snyder Cybersecurity Service Team.

WRITTEN BY:

Donald R. Geiter, J.D., M.S.L. (Cybersecurity Law & Policy), CIPP/US, CIPM

Partner

Tel: (717) 399-4154

Email: dgeiter@barley.com