INSIGHT: Watch for Auditors to Assess Future Risk of Cybersecurity Incidents

Oct. 15, 2019

By William Ridgway and Andrew Fuchs

Companies need to be mindful of auditors' increased focus on risks related to cybersecurity incidents. Skadden attorneys look at recent comments from a member of the Public Company Accounting Oversight Board and say her views contemplate an expanded role for auditors, assessing future risk, that may result in uncertainty for companies.

Independent auditors traditionally sought information from companies that suffered a cybersecurity incident to assess the need to record a liability or make financial statement or risk disclosures related to the incident. But now, auditors could be interested in looking for risks that could lead to future cybersecurity incidents.

Auditors often probe whether an incident touches on internal controls relating to financial reporting and related material misstatement of the financial statements, even though cybersecurity incidents seldom involve manipulation of a company's financial data.

According to anecdotal information from the Public Company Accounting Oversight Board (PCAOB), cybersecurity events at companies whose audits were inspected in 2016 were not "related to the risks of material misstatement of the financial statements, including disclosures, [and did not lead] to the identification of material weaknesses in ICFR."

The PCAOB staff nevertheless have cautioned that "[r]isks remain, however, that future cyber attacks may affect issuer financial statement reporting, and as a result, Inspections staff view this as an evolving risk area that requires ongoing focus."

Auditors Role Expanding

Although not a statement on behalf of the PCAOB, one of its board members recently signaled her view of an even more expansive role for auditors—they should not only assess the impact of an incident on a company's financial statements, but also evaluate the risk that a possible future cyber security event could cause a company's financial statements to be materially misstated.

In a May speech, Kathleen Hamm, a board member of the PCAOB, expressed her expectation that—whether or not a cyber-incident has occurred—an auditor "should consider any cybersecurity risks that could have a material effect on the company's financial statements. If the auditor identifies a risk related to cybersecurity that could have a material effect on a company's financial statements, the auditor should then design and execute procedures to address those risks."

As part of this risk assessment, Hamm mentioned that "an auditor must obtain an understanding of the company and its external and internal environment." In her view, "the auditor should also understand the methods used by the company to prevent and detect cyber-incidents that could have a material effect on the financial statements," as well as "how the company ensures appropriate escalation to the board and timely consideration of disclosure obligations to investors and others."

Finally, Hamm explained that "an auditor should be clear-eyed about the risk that attackers can operate under the guise of legitimate users, ultimately accessing a company's systems or subsystems that support the financial reporting process."

Assessing Risk

These views contemplate an expanded role for auditors that may result in uncertainty for the companies they audit. Indeed, it remains unclear what risk of material misstatement Hamm contemplated or how auditors could assess that risk.

First, industry observers have not recognized a connection between the prospect of future cyber-attacks and the risk of material misstatement of the financial statements. As noted in information from the PCAOB, cyberattacks do not generally involve the manipulation of a company's financial data, so the risk of company financial data integrity issues appears to be remote. Most cyberattacks involve theft of private information or ransomware attacks, compromising an area of the company's network that usually does not include systems supporting financial reporting. In other words, to-date there is little evidence of attackers "ultimately accessing a company's systems or subsystems that support the financial reporting process."

Second, the technical level at which auditors would perform such a risk assessment remains unclear. Hamm's speech mentions that auditors should understand "potential access points into [the company's] systems, as well as the logical access controls over the system," and "the company's processes that block and identify attempted unauthorized transactions or access to assets, as well as employees' familiarity with those processes."

Thus, she appears to contemplate a highly technical risk assessment of a company's cybersecurity vulnerabilities, even though auditors have not typically received specialized training in this area and the expertise to undertake this sort of risk assessment typically lies in an entirely different category of consulting firms with deep experience and knowledge of the technical issues and challenges.

Given the foregoing, companies should be mindful of auditors' increased focus on risks related to cybersecurity incidents. Despite the growing expectation that auditors should focus on these issues, there is substantial uncertainty about the proper focus and steps needed to accomplish their objectives.

This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.

Author Information

William Ridgway is a partner at Skadden in Chicago. A former federal prosecutor and experienced trial and appellate lawyer, he focuses on cybersecurity and data privacy matters, white collar crime, and intellectual property litigation.

Andrew J. Fuchs is a counsel at Skadden in Chicago. He has extensive experience representing corporate and individual clients in complex commercial litigation.