Bloomberg Law

The United States Law Week

INSIGHT: Cybersecurity Incident? Independent Financial Auditors Might Come Knocking

By William Ridgway and Andrew J. Fuchs April 1, 2019

Companies that experience a cybersecurity incident should not be surprised to hear from independent auditors. Two Skadden attorneys explain that auditors need to know if the incident requires changes to financial statements and companies need to plan to respond quickly.

Companies—particularly public companies—that experience a cybersecurity incident may be surprised by ensuing requests from their independent auditors seeking details about the incident.

This can complicate both the company's investigation into the incident and efforts to conclude the audit, especially if the company learns of the incident when the auditor is close to issuing an opinion on the company's financial statements or internal controls over financial reporting.

Independent auditors of a company's financial statements are generally focused on cybersecurity incidents for two reasons.

First, the auditors will want to understand whether the incident will require changes to the company's financial statements in the reporting period being audited or future periods. The company may need to record a liability or make financial statement disclosures for contingent liabilities for, as examples, expenses associated with remediating the incident, lawsuits or regulatory fines related to the incident, increased cybersecurity protection costs, or reduction to goodwill for anticipated negative impact to the value of the company's business or brand.

Relatedly, the company may need to disclose risks related to the cybersecurity incident in various sections of its periodic filings (such as its 10-K or 10-Q), including most notably in risk factors, management discussion and analysis, description of business, and legal proceedings.

As explained in a Securities and Exchange Commission release devoted to this topic, the need for disclosure depends on myriad factors, including the nature and magnitude of the incident and the expected consequences to the company's business and financial condition. (SEC Release Nos. 33-10459, 34-82746, Feb. 21, 2018.)

Second, and less intuitive in this context, auditors will also focus on the impact of an incident on the company's internal controls relating to financial reporting. Under applicable standards, including Sarbanes-Oxley, auditors must assess a company's information technology systems and controls in assessing the risks of material misstatements to the financial statements. In addition, many companies obtain an auditor's specific assessment of its internal controls over financial reporting (known as ICFR).

Common Threats

Companies may find this inquiry unexpected because most cybersecurity incidents involve theft of personal information or ransomware attacks that compromise a section of the company's network that usually does not include systems supporting financial reporting. In other words, such incidents rarely involve a manipulation of the company's financial data within the company's systems.

Another common threat is business e-mail compromise, where an employee is tricked into transferring funds to unauthorized recipients via a spoofed or compromised e-mail, purportedly from a company executive or vendor, that requests large fund transfers. Although such incidents come closer to impacting financial reporting, and have been subject to SEC scrutiny, it also is more akin to common theft and may not present a risk of material misstatement to the financial statements.

Indeed, anecdotal information from the PCAOB confirms cybersecurity incidents 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."

Despite this and the fact that auditor responsibilities seldom include assessing cybersecurity risks across a company's entire platform, external auditors remain vigilant, likely due to the emerging and evolving nature of cyber security incidents. As a result, they often seek detailed information to confirm that an incident does not touch on financial reporting systems.

This vigilance may also be due to PCAOB focus in this area. Recognizing that "[c]yber incidents and breaches of information systems continue to occur frequently while the complexity of cyber attacks on businesses is constantly evolving," the PCAOB recently announced that one of its areas for focus during its 2019 inspections will be to "continue to evaluate the audit procedures [audit] firms use to identify and determine whether cyber risks and actual breaches pose risks of material misstatement to companies' financial statements."

Determining Severity

To understand the incident and determine whether to use additional procedures to complete the audit, auditors will request information about the incident's cause and impact, as well as the remediation plan. These inquiries from external auditors present challenges if the company has not yet concluded its investigation.

In other words, while the company and its consultants and attorneys are conducting an often complex and extensive investigation, auditors may be pressing the company for immediate conclusions. These demands take on pressing significance because auditors may be unable or reluctant to conclude their audit with these questions unanswered or otherwise may assess a deficiency or weakness on the basis of information known to date.

Responding to these inquiries may require the company to accelerate its work and provide good-faith expectations about findings. As these investigations often are led by outside or in-house counsel, the information requests may risk waiving attorney-client or work-product privileges.

Given the importance of maintaining privilege when investigating a cyber incident, companies would be well served to evaluate carefully how best to respond to such requests to minimize the potential for exposing privileged communications and analyses to discovery.

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 an associate at Skadden in Chicago. He has extensive experience representing corporate and individual clients in complex commercial litigation.