THE REVIEW OF
SECURITIES & COMMODITIES REGULATION
AN ANALYSIS OF CURRENT LAWS AND REGULATIONS AFFECTING THE SECURITIES AND FUTURES INDUSTRIES

Vol. 53 No. 3 February 12, 2020

# CYBERSECURITY CONSIDERATIONS FOR PUBLIC COMPANY AUDITORS

*Federal and state agencies, and self-regulatory organizations, continue to highlight their cybersecurity enforcement efforts. Considerations for public company auditors in the event of a cybersecurity incident at an audit client, however, have received comparatively less attention. The author discusses such considerations in light of continued regulatory scrutiny of cybersecurity, internal controls over financial reporting, and concerns with management integrity.*

By Brian Neil Hoffman *

By Brian Neil Hoffman From the IT data room to the C-Suite and boardroom, public companies and their personnel must remain vigilantly focused on cybersecurity issues. Much has already been written about public company disclosure and other obligations in the event of a cybersecurity incident. Comparatively less attention, however, has been focused on considerations for public company auditors when a cyber event occurs at an audit client.

Even the most vigilant cybersecurity defensive system cannot forever prevent a cybersecurity incident. And regulators continue to scrutinize cybersecurity preventative and incident responsive steps. It thus is only a matter of time before auditors find themselves more squarely in the cybersecurity enforcement crosshairs. By no means exhaustive, discussed below are several considerations for auditors concerning internal controls, the financial statements, and management integrity.

## CONTINUED REGULATORY SCRUTINY

Cyber issues receive multi-faceted, layered enforcement oversight. And the recent significant activity in and focus on cybersecurity matters only serves to raise the bar when dealing with these agencies. Put simply, enforcement agencies no longer view these as novel issues, so expectations for respondents are heightened.

To start, the U.S. Securities and Exchange Commission includes cybersecurity among its enforcement priorities.[1] In September 2017, the SEC announced the creation of the Cyber Unit, a specialized unit within the Division of Enforcement. Together, the Division of "Enforcement, with leadership from the Cyber Unit, has continued to focus on cybersecurity threats to public companies and the resulting harm to

[1] Testimony of SEC Commissioners, "Oversight of the Securities and Exchange Commission: Wall Street's Cop on the Beat," Sept. 24, 2019.

* *BRIAN NEIL HOFFMAN, formerly an SEC Enforcement attorney, is now a partner with Holland & Hart LLP. His practice focuses on securities enforcement and litigation matters. At the ALI-CLE Accountants' Liability Conference in October 2019, Brian participated on a panel discussing the topics covered in this article. His e-mail address is bnhoffman@hollandhart.com.*