protiviti®
Face the Future with Confidence

Center for Audit Quality Issues Cybersecurity Risk Management Oversight Tool for Board Members

May 4,
2018

Cybersecurity has become a critical front-burner issue for boards of directors – one that is discussed at virtually every board meeting. The Center for Audit Quality (CAQ), an autonomous, nonpartisan and nonprofit public policy organization, is helping board members address this critical area with the release of its new publication, *Cybersecurity Risk Management Oversight: A Tool for Board Members*. According to the CAQ, this tool provides key questions board members can use as they discuss cybersecurity risks and disclosures with management and CPA firms.

The CAQ's tool is organized under four key areas:

1. Understanding how the financial statement auditor considers cybersecurity risk
2. Understanding the role of management and responsibilities of the financial statement auditor related to cybersecurity disclosures
3. Understanding management's approach to cybersecurity risk management
4. Understanding how CPA firms can assist boards of directors in their oversight of cybersecurity risk management

The tool also compiles cybersecurity-related resources from the CAQ, the American Institute of Certified Public Accountants (AICPA), the National Association of Corporate Directors (NACD), and other organizations.

The CAQ notes in its publication that it "… is not meant to provide an all-inclusive list of questions or to be seen as a checklist; rather, it provides examples of the types of questions board members may ask of management and the financial statement auditor. The dialogue that these questions spark can help clarify the financial statement auditor's responsibility for cybersecurity risk considerations in the context of the financial statement audit and, if applicable, the audit of internal control over financial reporting (ICFR). This dialogue can be

a way to help board members develop their understanding of how the company is managing its cybersecurity risks."

The paper is available for complimentary download at www.thecaq.org/cybersecurity-risk-management-oversight-tool-board-members.

Background

As has been well-documented, cybersecurity is among the most critical risks that organizations need to address today. Management and protection of organizational data, availability of critical systems and infrastructure, along with the enduring risk of cybersecurity threats are among the most pressing concerns for executive teams and boards of directors around the world, according to the *Executive Perspectives on Top Risks for 2018* report from Protiviti and North Carolina State University's ERM Initiative.[1]

The U.S. Securities and Exchange Commission (SEC) is among many regulatory authorities that have weighed in on the responsibilities of management and boards in regard to cybersecurity. In February 2018, the SEC published interpretive guidance to assist public companies in preparing their disclosures about cybersecurity risks and incidents. In its guidance, the SEC provides its views about public companies' disclosure obligations under existing law with respect to cybersecurity matters, and also addresses the importance of cybersecurity policies and procedures and the application of disclosure controls and procedures, insider trading prohibitions, and Regulation FD and selective disclosure prohibitions in the context of cybersecurity. Protiviti has published a Flash Report summarizing the SEC's guidance and its impact on public organizations.[2] The SEC's release can be found here.[3]

Our Point of View

It is clear from our client work and other interactions with corporate directors in a variety of forums that the cybersecurity issue is being elevated in almost every organization. This is a positive development and a reflection of response to customer and stakeholder concerns,

[1] For more information, visit www.protiviti.com/toprisks.

[2] "SEC Issues Interpretive Guidance on Public Company Cybersecurity Disclosures," Protiviti Flash Report, Feb. 26, 2018: www.protiviti.com/US-en/insights/sec-issues-interpretive-guidance-public-company-cybersecurity-disclosures.

[3] "SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures," Press Release, February 21, 2018, SEC: www.sec.gov/news/press-release/2018-22.

regulatory focus, and the acute awareness in the boardroom and C-suite that cyber risk is increasing.

At its core, the CAQ is suggesting greater communication among stakeholders in the enterprise. We support that view completely. The issues around cybersecurity risk are numerous, complex and ever-changing. The question set provided by the CAQ is helpful in starting, focusing and sustaining that conversation.

Insofar as discussions with the external audit firm are concerned, it is important for board members to understand what the audit firm does and does not do, whether during the financial statement audit or other attestation engagements. More importantly, directors should understand that management has the primary responsibility for managing cyber risks. This means that cybersecurity measures and incident response programs must be supported by the primary risk owners (first line of defense) and coordinated under the direction of a senior-level executive responsible for establishing, maintaining and reporting upon the organization's cybersecurity framework, e.g., a chief information security officer (as the second line of defense). There is also an important role for internal audit to play, through the performance of assurance and advisory activities, in evaluating and reporting on cybersecurity effectiveness. All of these components must be in place to properly inform executive management and the board in advancing cybersecurity risk management practices. Accordingly, in discharging its fiduciary and risk oversight responsibilities, the board should not rely on the external auditor as a sole source of assurance. Indeed, as the CAQ notes, "a company's overall IT environment includes systems, networks and related data that address not only financial reporting needs but also operational and compliance needs," requiring an organization to take a view of cybersecurity risk that is likely far broader than risk to financial reporting.

We believe an important part of any conclusion a company draws on its cybersecurity risk is to perform a formal risk assessment for their organization to identify the threats and vulnerabilities specific to the organization. It is essential to have as inclusive a view to the risk as possible, and we advise that both a "business" and "technology" perspective be integrated in that definition. We also believe it is helpful to have an independent view of the completeness and effectiveness of the controls the organization puts in place to manage that identified risk.

Further, the pace of change in the technology environment, coupled with the impressive rate at which organizations are leveraging technology to enhance customer engagement, improve operations, digitize products and services, and capture and analyze ever-increasing volumes of data, suggests that the risk assessments be done at least annually or perhaps even more frequently to obtain real-time updates on risk (through a tool such as the Protiviti Risk Index),[4] so they can track/reflect the implications of the changes to their cyber risk profile on an ongoing basis as part of the overall risk dialogue within an organization.

Summary

In defining its expectations for management in the cyber space and establishing clear accountabilities for results, the board should certainly avail itself of multiple sources of input. The external audit process as well as the organization's internal audit activities are two such sources that can inform the board's cybersecurity oversight. The CAQ provides directors with example questions for initiating and sustaining a dialogue with CPA firms, other external advisors and the chief audit executive regarding the role of management, the role of the financial statement audit and other forms of assurance available.

About Protiviti

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

[4] For additional information, visit www.protiviti.com/RiskIndex.

protiviti®