A TOOL FOR BOARD MEMBERS

CYBERSECURITY
RISK MANAGEMENT OVERSIGHT

CENTER FOR AUDIT QUALITY

APRIL 2018

Introduction

Companies are facing not only increasing cyber threats but also new laws and regulations for managing and reporting on data security and cybersecurity risks. Boards of directors face an enormous challenge: to oversee how their companies manage cybersecurity risk. As boards tackle this oversight challenge, they have a valuable resource in Certified Public Accountants (CPAs) and in the public company auditing profession.

CPAs bring to bear core values—including independence, objectivity, and skepticism—as well as deep expertise in providing independent assurance services in both the financial statement audit and a variety of other subject matters. CPA firms have played a role in assisting companies with information security for decades. In fact, four of the leading 13 information security and cybersecurity consultants are public accounting firms.[1]

This tool provides questions board members charged with cybersecurity risk oversight can use as they engage in discussions about cybersecurity risks and disclosures with management and CPA firms.

The questions are grouped under four key areas:

I. Understanding how the financial statement auditor considers cybersecurity risk

II. Understanding the role of management and responsibilities of the financial statement auditor related to cybersecurity disclosures

III. Understanding management's approach to cybersecurity risk management

IV. Understanding how CPA firms can assist boards of directors in their oversight of cybersecurity risk management

This tool provides questions board members charged with cybersecurity risk oversight can use as they discuss cybersecurity risks and disclosures with management and CPA firms.

This publication 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.

Additionally, this tool may help board members with cybersecurity risk oversight learn more about other incremental offerings from CPA firms. One example is the cybersecurity risk management reporting framework developed by the American Institute of CPAs (AICPA).[2] The framework enables CPAs to examine and report on management-prepared cybersecurity information, thereby boosting the confidence that stakeholders place on a company's initiatives. With this voluntary, market-driven framework, companies can also communicate pertinent information regarding their cybersecurity risk management efforts and educate stakeholders about the systems, processes, and controls that are in place to detect, prevent, and respond to breaches.

1 See Martin Whitworth, "Information Security Consulting Services, Q1 2016," *The Forrester Wave* (January 2016).

2 See AICPA, "SOC for Cybersecurity" web page.

I. Understanding How the Financial Statement Auditor Considers Cybersecurity Risk

The Sarbanes-Oxley Act of 2002 (SOX) added a requirement, applicable to most public companies, that management annually assess the effectiveness of the company's ICFR and report the results to the public. In addition, SOX requires the audit committees of most large public companies to engage independent auditors to audit the effectiveness of their company's ICFR.

This tool will outline how the financial statement auditor considers cybersecurity in two key contexts: (1) the audits of financial statements and, if applicable, ICFR; and (2) other disclosures. The following are questions that board members with cybersecurity risk oversight may use when discussing roles and responsibilities of the financial statement auditor related to cybersecurity risks.

QUESTIONS

1. How does the financial statement auditor's approach to identifying and assessing risks of material misstatement for the financial statement and ICFR audits consider certain cybersecurity risks?

2. If, as part of understanding how the company uses information technology (IT) in the context of its financial statements and ICFR, the financial statement auditor identifies a cybersecurity risk, how does that risk get addressed in the audit process?

3. Why don't the financial statement auditor's procedures on an ICFR audit address all of the company's enterprise-wide cybersecurity risks and controls?

4. What impact does a cybersecurity breach have on the financial statement auditor's assessment of ICFR?

5. In the event of a cybersecurity breach that results in a potential need for a contingent liability that could be material, what is the audit response of the financial statement auditor?

The financial statement auditor considers cybersecurity in two key contexts: (1) the audits of financial statements and, if applicable, ICFR; and (2) other disclosures.

II. Understanding the Role of Management and Responsibilities of the Financial Statement Auditor Related to Cybersecurity Disclosures

In September 2017, Securities and Exchange Commission (SEC) Chairman Jay Clayton stated, "I recognize that even the most diligent cybersecurity efforts will not address all cyber risks that enterprises face. That stark reality makes adequate disclosure no less important."[3]

The SEC is focused on ensuring the adequacy of public company disclosures of cybersecurity risks and how those risks are managed. Investor groups have also asked company boards to strive for transparency in reporting efforts to prevent and mitigate cyber threats.[4]

In 2011, the SEC's Division of Corporation Finance (Division) issued disclosure guidance. Under that guidance, a company may determine it is necessary to disclose cybersecurity risks in various places throughout its Form 10-K (e.g., risk factors, management's discussion and analysis [MD&A], legal proceedings, business description, and/or financial statements).[5] While the 2011 SEC staff guidance remains applicable, in February 2018, the SEC updated its disclosure guidance to reinforce and expand on the 2011 guidance. The new guidance addresses two topics not developed in 2011 guidance—namely, the importance of cybersecurity

3. See SEC Chairman Jay Clayton, "Statement on Cybersecurity," (SEC, Washington DC, September 20, 2017).

4. Council of Institutional Investors, "Prioritizing Cybersecurity: Five Investor Questions for Portfolio Company Boards" (April 2016).

5. See "CF Disclosure Guidance: Topic No. 2" (SEC, Washington DC, October 13, 2011).

policies and procedures and the application of insider trading prohibitions in the cybersecurity context.[6] In the 2018 guidance the SEC emphasized the importance of ensuring that periodic reports such as the Form 10-Q continue to provide timely and ongoing information on material cybersecurity risks and incidents. The SEC also emphasized that companies must maintain disclosure controls and procedures, and management must evaluate their effectiveness.

The SEC staff has communicated publicly that it intends to focus more on companies' disclosures about cyber incidents and their cybersecurity programs. The following are questions that board members with cybersecurity risk oversight may use to clarify management's role and the auditor's responsibilities related to cybersecurity disclosures.

QUESTIONS

The Role of Management

1. In complying with the current SEC guidance, how has management considered cybersecurity risks in its ability to record, process, summarize, and report on information required to be disclosed in its SEC filings?

2. What disclosure controls and procedures are in place to help ensure that the disclosures comply with the SEC's guidance regarding the importance of a company being able to make accurate and timely disclosures of material cyber events?[7]

3. Have the design and operating effectiveness of the disclosure controls and procedures been evaluated to ensure they appropriately record, process, summarize, and report on information required to be disclosed in the company's SEC filings?

4. How is management considering the current SEC guidance with respect to cybersecurity on risk factors, MD&A, and financial statement disclosures?

> **"I recognize that even the most diligent cybersecurity efforts will not address all cyber risks that enterprises face. That stark reality makes adequate disclosure no less important."**
>
> *SEC Chairman Jay Clayton*
> *September 2017*

5. In the event of a cybersecurity breach, what processes and controls are in place to help ensure that appropriate levels of management and board members with cybersecurity risk oversight are involved in the review of the related disclosures, if appropriate?

6. Has the company considered its insider trading policies in the event of a material cyber incident? Are appropriate policies and procedures in place to guard against company executives and other insiders taking advantage of the period between the company's discovery of a cybersecurity incident and public disclosure?

QUESTIONS

The Role of the Financial Statement Auditor

1. What does the financial statement auditor consider related to cybersecurity disclosures included in the Form 10-K or other documents that include the audited financial statements?

2. How do those considerations differ when cybersecurity related information is included in another company document (e.g., a press release)?

---

6. See "Commission Statement and Guidance on Public Company Cybersecurity Disclosures" (SEC, Washington DC, February 20, 2018).

7. See SEC, "Commission Statement," 10-11: "In determining their disclosure obligations regarding cybersecurity risks and incidents, companies generally weigh, among other things, the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and of the impact of the incident on the company's operations. The materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations. The materiality of cybersecurity risks and incidents also depends on the range of harm that such incidents could cause. This includes harm to a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-US authorities."

3. If the company had a material contingent liability for an actual cyber incident, what is the financial statement auditor's responsibility with respect to the company's assessment of any related financial statement disclosure(s)?

4. What is the financial statement auditor's responsibility if a cyber incident material to the financial statements is discovered after the balance sheet date but before the auditor's report on the financial statements is issued?

III. Understanding Management's Approach to Cybersecurity Risk Management

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, all of which are susceptible to a cyber event. Consequently, C-suite executives and board members in a cybersecurity risk oversight role are increasing their oversight of management's development, implementation and monitoring of a comprehensive enterprise-wide cybersecurity risk management program.

The SEC has stated that disclosures regarding a company's cybersecurity risk management program and how the board of directors engages with management on cybersecurity issues allow investors to assess how a board of directors is discharging its risk oversight responsibility.

The following are broader cybersecurity-related questions (i.e., not specific to financial reporting) that board members in their oversight roles can use to better understand a company's cybersecurity risk management program.

QUESTIONS

1. What framework, if any, does management use in designing a cybersecurity risk management program (e.g., NIST, ISO/IEC 27001/27002, SEC cybersecurity guidelines, AICPA Trust Services Criteria)?

In 2017, the National Association of Corporate Directors (NACD) updated its *NACD Director's Handbook on Cyber-Risk Oversight*. The publication recommends strategies for bringing perspectives on cybersecurity matters into the boardroom, including "leveraging the board's existing independent advisors, such as external auditors and outside counsel." It also includes additional questions about cybersecurity (see appendix A) for the board to ask management, and it identifies five principles that boards should consider as they seek to enhance their oversight of cyber risks.[8]

1. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
2. Directors should understand the legal implications of cyber risk as they relate to their company's specific circumstances.
3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas.
4. Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.
5. Board-management discussions about cyber risk should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.

2. What framework, if any, does management use in communicating pertinent information about its cybersecurity management program?

3. What processes and programs are in place to periodically evaluate the cybersecurity risk management program and related controls?

4. What cybersecurity policies, processes, and controls are in place to detect, respond to, mitigate, and recover

8. See NACD, *Director's Handbook on Cyber-Risk Oversight*, 2017 ed. (Washington, DC: NACD, 2017), 4. Used with permission from NACD.

from—on a timely basis—cybersecurity events that are not prevented?

5. In the event of a cybersecurity breach, what controls are in place to help ensure that the IT department and appropriate senior management (including board members charged with governance) are informed and engaged on a timely basis—and that other appropriate responses and communications take place?

6. What policies, processes and controls are in place to address the impact to the company of a cybersecurity breach at significant/relevant vendors and business partners with whom the company shares sensitive information? Do those policies include risk identification and mitigation procedures?

7. Has the company conducted a cyber event simulation as part of its approach to enterprise risk management?

8. Has the company considered cost mitigation/risk transfer options in the form of cyber insurance coverage in the event of a cybersecurity breach?

9. Does the company have adequate staff with appropriate skills to design and operate an effective cybersecurity risk management program?

IV. Understanding How CPA Firms Can Assist Boards of Directors in Their Oversight of Cybersecurity Risk Management

The issues and challenges of cybersecurity are evolving rapidly. Although cybersecurity risk management practices are typically beyond the scope of a typical financial statement audit, CPAs are in a strong position to play an important role in informing the advancement of these practices. The CPA profession's commitment to continuous improvement, public service, and increased investor confidence has resulted in a greater focus on this area.

The questions below aim to foster a dialogue between auditors and those board members in a cybersecurity risk oversight role about identifying incremental offerings that CPA firms may provide to companies.

CPAs are in a strong position to play an important role in informing the advancement of cybersecurity risk management practices.

QUESTIONS

1. Since the financial statement auditor's focus is on IT risks that affect financial reporting, including disclosures and ICFR, what additional offerings can CPA firms with cybersecurity expertise provide to assist board members in executing their broader oversight responsibilities related to cybersecurity risks?

2. The AICPA recently issued a cybersecurity risk management reporting framework. How can this framework be used as a self-assessment tool to help management or the auditor (via a readiness engagement) identify opportunities for improvement in the company's cybersecurity risk management program?

3. How is the AICPA cybersecurity risk management reporting framework used by auditors as part of an attestation service to evaluate management's description of its cybersecurity risk management program and to determine whether controls within the program were effective to achieve the company's cybersecurity objectives?

4. What technical expertise do CPA firms possess that qualify them to perform a readiness engagement and/or an examination to validate effectiveness of controls specific to a company's cybersecurity risk management program?

5. The SOC for Cybersecurity examination (see sidebar on page 6) cannot prevent or detect a cybersecurity threat or breach. Accordingly, what is the goal of the cybersecurity examination?

6. What factors should be considered by the company and the CPA firm prior to engaging its financial statement

auditors to perform the readiness assessment or examination for entities subject to SEC independence rules?

7. What is the audit profession doing to help address cybersecurity risks from third party vendors or service providers?

8. What other types of engagements are available to help board members with cybersecurity risk oversight?

Conclusion

With the increased focus by regulators and investors on cybersecurity risk management and disclosures, company management and board members in their oversight roles are making enterprise-wide cybersecurity risk management a priority. While not an exhaustive list, the questions in this tool can help foster dialogue among board members responsible for cybersecurity risk oversight, company management, and auditors; they can also help clarify roles and responsibilities as well as actions that may be considered. This tool also aims to provide information about how those charged with cybersecurity risk oversight can leverage existing independent advisors—such as CPA firms—to help fulfill their fiduciary responsibilities.

INFORMATION SHARING

Distinguishing Between SOC 2 Examinations and SOC for Cybersecurity Examinations

The term *system and organization controls* (SOC), as defined by the AICPA, refers to the suite of services CPA practitioners may provide that relate to assurance over system-level controls of a service organization and system- or entity-level controls of other organizations. The AICPA's cybersecurity risk management examination discussed in this tool is also known as SOC for Cybersecurity.

A SOC 2 – SOC for Service Organizations examination is a separate and distinct offering. It may be used, for example, to report on the effectiveness of controls within a specific system occurring at an organization that provides outsourcing services to user entities.

To learn more about the difference between these two services, see the AICPA's 2017 whitepaper: *SOC 2® Examinations and SOC for Cybersecurity Examinations: Understanding the Key Distinctions*.[9]

WE WANT TO HEAR FROM YOU

So that we can provide resources that are informative and best address the needs of our stakeholders, we would appreciate your response to three, short questions.

SHARE FEEDBACK

Survey URL: https://thecaq.qualtrics.com/jfe/form/SV_1G36NECnA3wHmPH

9. The white paper is available at the AICPA website.

Appendix A

Questions for the Board to Ask Management About Cybersecurity

The following questions are reprinted with permission from NACD, Director's Handbook on Cyber-Risk Oversight, 2017 ed. (Washington, DC: NACD, 2017), 21-23.

SITUATIONAL AWARENESS

1. Were we told of cyberattacks that have already occurred and how severe they were?
2. What are the company's cybersecurity risks, and how is the company managing these risks?
3. How will we know if we have been hacked or breached, and what makes us certain we will find out?
4. Who are our likely adversaries?
5. In management's opinion, what is the most serious vulnerability related to cybersecurity (including within our IT systems, personnel, or processes)?
6. If an adversary wanted to inflict the most damage on our company, how would they go about it?
7. Has the company assessed the insider threat?
8. When was the last time we conducted a penetration test or an independent external assessment of our cyber defenses? What were the key findings, and how are we addressing them? What is our maturity level?
9. Does our external auditor indicate we have cybersecurity-related deficiencies in the company's internal controls over financial reporting? If so, what are they, and what are we doing to remedy these deficiencies?

STRATEGY AND OPERATIONS

1. What are the leading practices for cybersecurity, and where do our practices differ?
2. Do we have appropriately differentiated strategies for general cybersecurity and for protecting our mission-critical assets?
3. Do we have an enterprise-wide, independently budgeted cyber-risk management team? Is the budget adequate? How is it integrated with the overall enterprise risk management process?
4. Do we have a systematic framework, such as the NIST Cybersecurity Framework, in place to address cybersecurity and to assure adequate cybersecurity hygiene?
5. Where do management and our IT team disagree on cybersecurity?
6. Do the company's outsourced providers and contractors have cybersecurity controls and policies in place? Are those controls monitored? Do those policies align with our company's expectations?
7. Does the company have cyber insurance? If so, is it adequate?
8. Is there an ongoing, company-wide awareness and training program established around cybersecurity?
9. What is our strategy to address cloud, BYOD, and supply-chain threats?
10. How are we addressing the security vulnerabilities presented by an increasingly mobile workforce?

INSIDER THREATS

1. What are the leading practices for combating insider threats, and how do ours differ?
2. How do key functions (IT, HR, Legal, and Compliance) work together and with business units to establish a culture of cyber-risk awareness and personal responsibility for cybersecurity? Considerations include the following:

a. Written policies which cover data, systems, and mobile devices should be required and should be required for all employees.

b. Establishment of a safe environment for reporting cyber incidents (including self-reporting of accidental issues).

c. Regular training on how to implement company cybersecurity policies and recognize threats.

3. How have we adapted our personnel policies, such as background checks, new employee orientation, training related to department/role changes, employee exits, and the like, to incorporate cybersecurity?

4. How do our operational controls, including access restrictions, encryption, data backups, monitoring of network traffic, etc., help protect against insider threats?

5. Do we have an insider-incident activity plan that spells out how and when to contact counsel, law enforcement and/or other authorities, and explore legal remedies?

SUPPLY-CHAIN/THIRD-PARTY RISKS

1. How do we balance the financial opportunities (lower costs, higher efficiency, etc.) created by greater supply-chain flexibility with potentially higher cyber risks?

2. How much visibility do we currently have across our supply chain regarding cyber-risk exposure and controls? Which departments/business units are involved?

3. What will need to be done to fully include cybersecurity in current supply-chain risk management?

4. How are cybersecurity requirements built into contracts and service-level agreements? How are they enforced? Contracts and service-level agreements can be written to include requirements for the following:

a. Written cybersecurity policies

b. Personnel policies, such as background checks, training, etc.

c. Access controls

d. Encryption, backup, and recovery policies

e. Secondary access to data

f. Countries where data will be stored

g. Notification of data breaches or other cyber incidents

h. Incident-response plans

i. Audits of cybersecurity practices and/or regular certifications of compliance

5. How difficult/costly will it be to establish and maintain a viable cyber-vulnerability and penetration-testing system for our supply chain?

6. How difficult/costly will it be to enhance monitoring of access points in the supplier networks?

7. Do our vendor agreements bring new legal risks or generate additional compliance requirements (e.g., FTC, HIPAA, etc.)?

8. Are we indemnified against security incidents on the part of our suppliers/vendors?

INCIDENT RESPONSE

1. How will management respond to a cyberattack? Does the company have a validated incident-response plan? Under what circumstances will law enforcement and other relevant government entities be notified?

2. For significant breaches, is our communication adequate as information is obtained regarding the nature and type of breach, the data impacted, and the ramifications to the company and the response plan?

3. Are we adequately exercising our cyber-preparedness and response plan?

4. What constitutes a material cybersecurity breach? How will such events be disclosed to investors?

AFTER A CYBERSECURITY INCIDENT

1. How did we learn about the incident? Were we notified by an outside agency, or was the incident discovered internally?
2. What do we believe was stolen?
3. What has been affected by the incident?
4. Have any of our operations been compromised?
5. Is our cyber-incident response plan in action, and is it working as planned?
6. Whom must we notify about this incident (materiality), whom should we notify, and is our legal team prepared for such notifications?
7. What is the response team doing to ensure that the incident is under control and that the hacker no longer has access to our internal network?
8. Do we believe the hacker was an internal or an external actor?
9. What were the weaknesses in our system that allowed the incident to occur (and why)?
10. What steps can we take to make sure this type of event does not happen again?
11. What can we do to mitigate any losses caused by the incident?

CONTACTING EXTERNAL PARTIES

In addition to external counsel, boards and management teams should consider whether to notify the following:

- Independent forensic investigators
- The company's insurance provider
- The company's external audit firm
- Crisis communications advisors
- Law enforcement agencies (e.g., the Federal Bureau of Investigation, Department of Homeland Security, US Secret Service)
- Regulatory agencies
- US Computer Emergency Response Team (US-CERT)

Appendix B

Additional Resources

- AICPA: *Cybersecurity Resource Center*
- AICPA: *SOC for Cybersecurity web page*
- AICPA: *SOC 2® Examinations and SOC for Cybersecurity Examinations: Understanding the Key Distinctions* (December 2017)
- CAQ: *Cybersecurity Resource web page*
- CAQ: *The CPA's Role in Addressing Cybersecurity Risk* (May 2017)
- Council of Institutional Investors, *Prioritizing Cybersecurity: Five Investor Questions for Portfolio Company Boards* (April 2016)
- NACD: *Director's Handbook on Cyber-Risk Oversight* (January 2017)
- SEC: *Commission Statement and Guidance on Public Company Cybersecurity Disclosures* (February 2018)
- SEC: *CF Disclosure Guidance: Topic No. 2* (October 2011)
- SEC: *Office of Compliance Inspections and Examinations 2018 Examination Priorities*

About the Center for Audit Quality

The CAQ is an autonomous public policy organization dedicated to enhancing investor confidence and public trust in the global capital markets. The CAQ fosters high-quality performance by public company auditors; convenes and collaborates with other stakeholders to advance the discussion of critical issues that require action and intervention; and advocates policies and standards that promote public company auditors' objectivity, effectiveness, and responsiveness to dynamic market conditions. Based in Washington, DC, the CAQ is affiliated with the American Institute of CPAs.

THECAQ.ORG

WE WELCOME YOUR FEEDBACK | Please send comments or questions to info@thecaq.org.