CAQ

CENTER FOR
AUDIT QUALITY

The Role of Auditors in Company-Prepared Cybersecurity Information: Present and Future

October 2020

About the Center for Audit Quality

The Center for Audit Quality (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.

Contents

Introduction

In December 2019, the Center for Audit Quality (CAQ) developed and issued a publication, *The Role of Auditors in Company-Prepared Information: Present and Future*, which provides a foundational understanding of the current role of auditors in various types of company-prepared and publicly disclosed information and discusses how auditors are positioned to enhance the reliability of decision-useful company-prepared information.

Cybersecurity can have pervasive impacts on companies. Organizations face numerous threats with varying consequences—all in an environment marked by rapid technological change. With technology advancing and the COVID-19 pandemic causing increased remote working arrangements, companies are facing new and evolving cybersecurity threats. In response, regulators, investors, and other stakeholders are increasingly interested in understanding more about the impact of cybersecurity on the global economy. In its July 2020 report, The World Economic Forum ranked "Cyber-attacks and data fraud due to a sustained shift in working patterns" as the third (of 10) most worrisome risk for companies.[1] It is a strategic imperative that companies promote cybersecurity resilience and build trust in their cybersecurity practices. Companies can differentiate themselves by providing greater transparency around how they are addressing cybersecurity risks.

In this publication, we will provide an overview of the types of company-prepared information—both required and voluntary—that have been observed in the marketplace to describe to stakeholders how companies are addressing cybersecurity risks. We will discuss the role auditors play in cybersecurity as it relates to the audit of the financial statements and how the auditor's role in cybersecurity could evolve beyond the financial statements to better meet the evolving needs of investors, senior management, boards of directors, and other pertinent stakeholders.

We also provide key questions board members can consider as they discuss company-prepared cybersecurity information with management and public company auditors.

1 See World Economic Forum's *5 principles for effective cybersecurity leadership in a post-COVID world.*

The Landscape of Company-Prepared Cybersecurity Information

As both public and private sectors grapple with cybersecurity, the investor and other stakeholder demands for and expectations of transparency about how companies are managing this risk are increasing. These calls for more information serve as potent drivers for improving the general level of cybersecurity risk management practices across the company-reporting ecosystem. Investors and other stakeholders are interested in understanding a company's cybersecurity risks, and strategies for mitigating those risks, for a multitude of reasons, including the following:

+ Investors want to understand cybersecurity risks that could threaten the achievement of the company's operational, reporting, financial, legal, and regulatory objectives. Failing to achieve these objectives may impair the company's brand reputation, which can have implications on the company's enterprise value.

+ Companies want to understand the cybersecurity protocols of their service providers to understand how they handle and protect sensitive information and/or their reliability as an important supply chain member.

+ Consumers want confirmation that their personally identifiable information will be secure.

Company-prepared cybersecurity information provides an opportunity for companies to communicate to stakeholders that they are taking cybersecurity seriously and have risk management programs in place to address cybersecurity risks.

REQUIRED PUBLIC COMPANY DISCLOSURES

Under disclosure guidance issued by the SEC's Division of Corporation Finance (the Division) in 2011, a company may determine it is necessary to disclose cybersecurity risks in various places throughout its Form 10-K. Ordinarily, that determination may result in certain disclosure included in risk factors, management's discussion and analysis (MD&A), legal proceedings, business description, and/or financial statements.[2] In February 2018, the SEC updated its disclosure

2 See *CF Disclosure Guidance Topic No. 2*.

guidance to reinforce and expand on the 2011 guidance. The 2018 guidance addressed the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in a cybersecurity context.[3] It also highlighted the importance of ensuring that periodic reports, such as the Form 10-K and Form 10-Q, as well as current reports, such as the Form 8-K, continue to provide timely and ongoing information on material cybersecurity risks and incidents. The SEC emphasized that companies must maintain disclosure controls and procedures, and management must evaluate their effectiveness. In addition to this guidance, the SEC Office of Compliance Inspections and Examinations has issued several risk alerts on cybersecurity topics. Those risk alerts draw attention to risks companies may want to consider when assessing their own cybersecurity risks and related disclosures. The SEC also issued an investigative report in October 2018 that highlighted the need to re-calibrate and maintain effective internal accounting controls to address evolving cybersecurity risks.[4]

Many public companies consider cybersecurity to be a risk to their business operations. An EY survey that looked at the cybersecurity disclosures of Fortune 100 companies found that 100 percent of these companies reported cybersecurity as a risk factor and 89 percent disclosed their risk oversight approach.[5] While the SEC guidance only requires disclosure of the most significant factors that make an investment in the registrant or offering speculative or risky, the guidance laid out by the Division provides suggestions for enhanced disclosure around cybersecurity.

VOLUNTARY DISCLOSURES ABOUT A COMPANY'S CYBERSECURITY RISK MANAGEMENT PROGRAM

While the vast majority of companies disclose some cybersecurity information in their SEC filings, the disclosures of many of those companies are limited to general information regarding cybersecurity risks and company cybersecurity-risk management programs to address them. For example, according to an EY survey, only 7 percent of Fortune 100 companies disclosed that they perform cyber-incident simulations or tabletop exercises; and only 16 percent of companies disclosed the use of an external independent consultant to help management with cybersecurity-related practices. Similarly, only 5 percent of companies disclosed board engagement with an external independent advisor.

As the threat of cybersecurity attacks increases, particularly in today's pandemic environment, so does the potential for severe implications

Fortune 100 Company Disclosures:

7%
disclose performance of cyber-incident simulations or table top exercises

16%
disclose the use of an external independent consultant to help management with cybersecurity-related practices

5%
disclose board engagement with an external independent advisor

3 See *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*.
4 See SEC's *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934*.
5 See EY's *What companies are disclosing about cybersecurity risk and oversight.*

to the company's operations and information and resources. Therefore, investors and other stakeholders may find information beyond those disclosures required by the SEC, as outlined above, helpful for decision-making. Swiss Re Institute recently conducted a series of interviews with 20 international leaders from Europe and North America at the board and executive level that addressed the importance of and demand for enhanced cybersecurity disclosures. The interviews revealed that respondents believe that shareholders currently do not have enough transparency about a company's cyber resilience to make an informed investment decision. None of the respondents ranked the current levels of transparency as "good" or "really good." Further, the majority of the respondents said that if one company reported on cyber resilience and another did not, it would make a difference to their own decision-making.[6]

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 the impact of the incident on the company's operations. The SEC expects companies to provide disclosures that are tailored to their particular cybersecurity risks and incidents.

As stakeholder interest grows, it may be helpful for companies to communicate key elements of its response to cybersecurity risk (sometimes referred to as a cybersecurity risk management program), such as its processes to prevent, detect, respond to, and recover from cybersecurity incidents. These communications could include, but are not limited to, the following:

- if the company has governance processes and controls over service providers
- the existence of incident response planning and how often this is reviewed
- any simulations run by the company and the results
- use of an independent advisor and the services provided.

6 See Swiss Re Institute's *Transparency Imperative or Security Nightmare? Cyber Resilience "ESG" Reporting*.

Cybersecurity and the Auditor's Role

WHAT IS THE AUDITOR'S CURRENT ROLE?

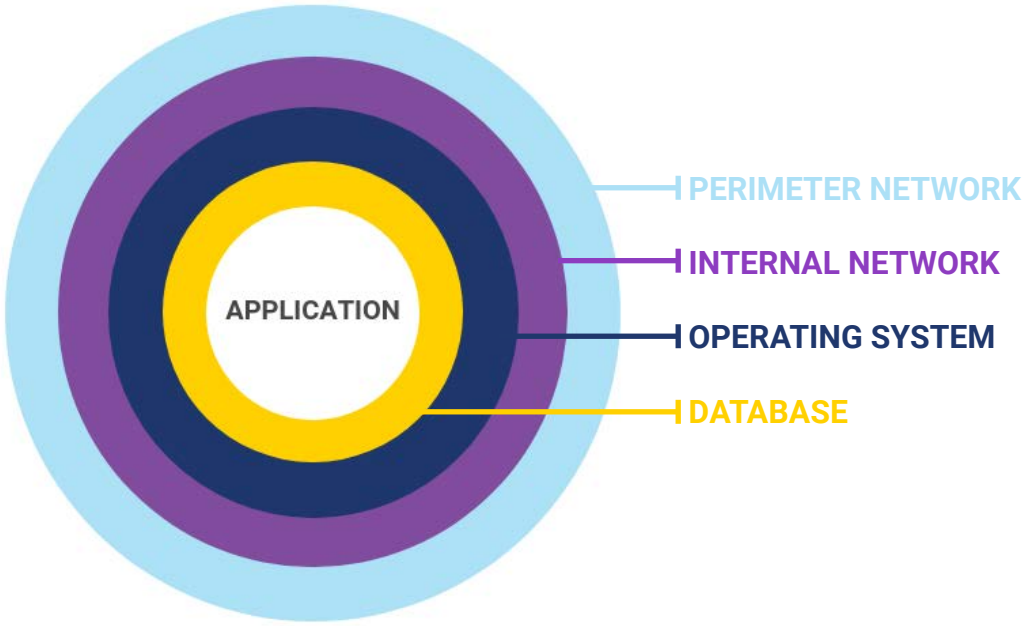
As cybersecurity risks evolve, the auditor should continue to evaluate the potential for cybersecurity incidents to have a material impact on the financial statements. Auditing standards require the financial statement auditor to obtain an understanding of how the company uses information technology (IT) and the impact of IT on the financial statements. This includes an understanding of the extent of the company's automated controls as they relate to financial reporting, the IT general controls that are important to the effective operation of automated controls, and the reliability of data and reports produced by the company and used in the financial reporting process. In assessing the risks of material misstatement to the financial statements—including IT risks resulting from unauthorized access—financial statement auditors are required to consider their understanding of the company's IT systems and controls.

In a company's IT environment, the systems and data in scope for most financial statement audits usually are a subset of the totality of systems and data used to support the company's overall business operations; the auditor's focus is on access controls and changes to systems and data, computer operations controls, and the reliability of company-prepared information using systems and data that could impact the financial statements and the effectiveness of internal control over financial reporting (ICFR).

It is important to remember that a company's overall IT platform includes systems and related data that address not only financial reporting processes but also the operational and compliance needs of the entire organization. The diagram on page 7 depicts the typical access path to an IT system.

The financial statement auditor's primary focus is on the controls and systems that are in the closest proximity to the application data of interest to the audit of the financial statements and when applicable of ICFR—that is, on those layers that, if breached, may allow access to the systems and applications that house financial statement–related data. Audit procedures are then developed to address each company's unique IT environment. Many cybersecurity incidents first occur through the perimeter and internal network layers, which tend to

Typical Access Path to an IT System



be further removed from the application, database, and operating systems that are typically included in access control testing of systems that affect the financial statements. However, the cybersecurity risk landscape has evolved, and the frequency and complexity of cybersecurity attacks continues to change. For example, there have been cybersecurity incidents resulting in the disbursement of unauthorized funds (e.g., a wire transfer) originating through the compromise of the company's email system. Such incidents may not necessarily be sophisticated in the use of technology; instead, they have adapted to exploit weaknesses in the company's policies and procedures that are vulnerable to cybersecurity risk today.

As part of risk assessment and planning, auditors would broadly consider cybersecurity risks that could have a material effect on the company's financial statements and, in an integrated audit, ICFR. Considerations related to cybersecurity risks include the potential financial impact of such risks on the financial statements and the inability of an organization to issue financial statements in a timely manner because of a breach of its financial reporting systems (e.g., due to a ransomware attack). For example, auditors may obtain an understanding of the company's business operations that give rise to cybersecurity risk and, to the extent such risks are deemed material to the company's financial statements, adjust their audit plan accordingly to address those risks. Common areas that may have exposure to cybersecurity risk include processes where bank accountant information is modified and funds are disbursed (e.g., wire transfer). In addition, certain technical controls are tested in areas of security, change management, and operations to address cybersecurity risk. Cybersecurity risk is a spectrum, and while the risk profile may vary across organizations, it is unlikely that a company is immune to cybersecurity risk in today's environment.

With respect to the company's cybersecurity disclosures, the auditor's responsibilities depend on whether the disclosures are included in the audited financial statements or elsewhere in the Form 10-K. If the disclosure is included in the audited financial statements, the auditor performs procedures to assess whether the financial statements, taken as a whole, are presented fairly, in all material respects. Included in the auditor's assessment are procedures specific to the financial statement disclosures.

For example, when a cybersecurity breach that has a material financial statement impact occurs, the auditor would perform procedures around the affected account balances and assess whether the disclosures related to material contingent liabilities, if any, are reasonable in relation to the financial statements taken as a whole. In addition, the auditor would need to consider the impact of this incident on management's assessment of ICFR.

In contrast, if the cybersecurity disclosure is presented outside the audited financial statements, such as MD&A, the auditor's responsibilities are different. The auditor would follow the guidance in paragraphs 4 and 5 of the Public Company Accounting Oversight Board (PCAOB) Auditing Standard 2710, *Other Information in Documents Containing Audited Financial Statements.* This auditing standard requires auditors to read the other information in documents containing the audited financial statements and consider whether such information or the manner of its presentation is materially inconsistent with information appearing in the audited financial statements or contains a material misstatement of fact. Note that reading and considering information involves substantially less work than that required in an audit. Even if a company has extensive disclosures in MD&A about its cybersecurity risk management program, the auditor is not required to perform any procedures in the audit of the financial statements or ICFR to evaluate the appropriateness of the design and implementation of the company's cybersecurity risk management program or its effectiveness or consider the broader cybersecurity risks that may affect the organization.

While cybersecurity is not explicitly addressed in auditing standards, the PCAOB has highlighted that cybersecurity risks will continue to be a focus of its inspections and has highlighted cybersecurity and the role of auditors in evaluating cybersecurity risks in board speeches and other communications.[7]

WHERE COULD AUDITORS PLAY A GREATER ROLE BEYOND THE AUDIT OF THE FINANCIAL STATEMENTS?

The scale and complexity of the cybersecurity challenge has grown exponentially. As a result, there has been an increasing call from stakeholders for information related to cybersecurity and for robust conversations on these topics. Everyone has a role to play in promoting cybersecurity resilience. Before exploring how auditors could play a greater role in cybersecurity disclosures beyond those included in the audited financial statements, it is important to consider the needs of the various stakeholders.

+ Analysts and investors may want to consider information about a company's cybersecurity measures when making investment decisions. This information can help them understand the cybersecurity risks that could threaten the achievement of the company's operational, reporting, legal, and regulatory objectives—each having the potential to impact a company's market value. According to an article from the World Economic Forum, cyber risk is rapidly becoming an important factor to consider when making investing decisions, as it is a key component of an enterprise's viability.[8]

+ To help fulfill their oversight responsibilities, boards of directors need information about the company's cybersecurity program and the cybersecurity threats the company faces. They also want information that will help them evaluate the company's effectiveness in managing cybersecurity risks.

+ Company management may need information about how business partners (e.g., vendors) with whom they do business manage their cybersecurity risks. This information can help management understand and assess the risks arising from doing business with such business partners (for example, a manufacturer needs to be able to rely on a key vendor's ability to provide goods/services in the event of a disruption to its IT

7 See the PCAOB's *Conversations with Audit Committee Chairs: COVID-19 and the Audit* and *Spotlight: Staff Update and Preview of 2019 Inspection Observations*.

8 See World Economic Forum's *Investors have a role in securing our shared digital future*.

systems). Likewise, business partners may need information about the company's cybersecurity program to evaluate the business relationship.

Auditors, in their public interest role, play a significant role in the flow of comparable and reliable information for decision-making, including disclosures about cybersecurity. Auditors can provide advisory or attestation services on company-prepared cybersecurity information that may bring discipline to management's voluntary cybersecurity disclosures and to the organization's cybersecurity risk management program. Some of those services may enhance the trust and confidence stakeholders—including boards of directors, investors, and business partners—have in the cybersecurity information that companies report. These services might include the following:[9]

+ **Assessment Engagements:** Accounting firms can provide services to help companies identify and assess key cybersecurity risk areas and design and develop effective cybersecurity risk management controls to address such risks. An example of such an engagement, often referred to as a readiness assessment, may be performed in advance of a cybersecurity examination. In a readiness assessment, an auditor performs procedures to obtain an understanding of the company's cybersecurity processes and controls and to identify any gaps in those processes and controls. Often, the auditor would make high-level recommendations about ways to strengthen existing cybersecurity controls.

+ **Attestation Engagements**: Auditors can perform an examination engagement in accordance with the American Institute of CPA's (AICPA's) attestation standards. In an examination engagement, a public accounting firm (auditors) uses a multidisciplinary team—made up of auditors whose core competencies can include credentialed IT and information security specialists—to perform the engagement. Based on the procedures performed and the evidence obtained, auditors provide an independent report on whether management's description of the company's cybersecurity risk management program is presented in accordance with the reporting framework and whether the controls within the program were suitably designed and operating effectively to achieve the company's cybersecurity objectives based on that framework.

Companies within the same industry can face different cybersecurity risks; therefore, their cybersecurity risk management programs are not identical. Consequently, companies and stakeholders can benefit from the use of a framework to promote a level of consistency among companies' cybersecurity disclosures while also enabling companies to communicate specific cybersecurity threats they face and how they are responding to them.

With respect to attestation engagements, to enable auditors to conduct the examination, the AICPA developed a reporting framework that provides a common approach to communicating, evaluating, and reporting on company's cybersecurity risk management program. The reporting framework, known as Systems and Organization Controls (SOC) for Cybersecurity, includes three key components designed to assist stakeholders in understanding a company's cybersecurity risk management program:

i. Management's description of the company's cybersecurity risk management program

ii. Management's assertion that the program meets the framework criteria

iii. The Practitioner's opinion

Management can use the framework to determine key components of the company's cybersecurity risk management program to communicate in order to meet the information needs of users. Additionally, auditors can use the criteria in the AICPA's SOC for Cybersecurity framework to opine on the cybersecurity risk management program's design and on the effectiveness of controls management has designed to achieve the organization's cybersecurity objectives. The practitioner's report (i.e., their opinion) may assist boards of directors, senior management, and other pertinent stakeholders as they evaluate the effectiveness of their organization's cybersecurity risk management programs.•

9 The permissibility of these services depends on if the accounting firm meets the applicable independence requirements, and certain services may need to be performed by CPAs.

Boards of Directors Considerations

Company boards face a significant challenge in overseeing how companies manage their cybersecurity risk. Board members charged with cybersecurity risk oversight may want to consider asking the questions outlined below as they engage in discussions about cybersecurity risks and disclosures with management and public company auditors. Note that the questions below are not meant to be all-inclusive or to be seen as a checklist; rather, they provide examples of the types of questions board members may ask of management and the financial statement auditor. This dialogue can help board members enhance their understanding of how the company is managing its cybersecurity risks. It can also help clarify the financial statement auditor's responsibility for cybersecurity risk considerations in the context of the financial statement audit and, if applicable, the integrated audit of ICFR. These questions also may help boards understand additional services accounting firms could provide over the company's cybersecurity risk management program and related disclosures.

CONSIDER THE CURRENT CYBERSECURITY LANDSCAPE

In assessing the company's current cybersecurity landscape, board members may want to consider asking:

- What aspects of the company's business and operations give rise to cybersecurity risk?
- Does the company have a comprehensive cybersecurity risk management program?
  - If yes, does the company follow a framework for managing its cybersecurity process and controls such as National Institute of Standards and Technology or International Organization (NIST) for Standardization?
- Does the company's cybersecurity program include a documented cybersecurity breach response plan?

- Does it involve all affected departments (e.g., legal, IT, public relations, c-suite executives, board)?
- How often is the cybersecurity breach response plan reviewed?

+ Has the company performed a simulation to practice and evaluate cybersecurity breach protocols? Has the Board observed and/or participated in such a simulation? How frequently are such simulation exercises performed?

+ Is cybersecurity risk oversight assigned to the full board, to a particular committee, or to a combination of those?
  - How much time is dedicated to cybersecurity and what is the degree of frequency of cybersecurity-risk deliberations?
  - Do select board members have cybersecurity expertise? If not, has the board engaged a third-party to independently provide expert advice?

+ Does the company evaluate the root cause of a cybersecurity breach to determine whether it resulted from a material weakness or significant deficiency in ICFR?

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

+ If a cybersecurity breach took place that had a material impact on the financial statements, how did the auditor assess the risk of material misstatement on the financial statements? Were any changes made to the audit procedures as a result of this breach?

CONSIDER POTENTIAL ENHANCEMENTS IN THE COMPANY'S CYBERSECURITY RISK MANAGEMENT PROGRAM AND RELATED DISCLOSURES

As cybersecurity risks evolve, companies may want to consider enhancing their cybersecurity risk management programs and related disclosures. In determining next steps, the board may want to consider the following:

+ Is there additional information the company could disclose in its public filings that might be useful to investors and other stakeholders? For example:
  - Do the disclosures include information about contingency plan reviews or simulations?
  - Does the disclosure include information about third-party reviews?
  - The education training efforts employed by the company to mitigate cybersecurity risks.
  - The board's engagement of an independent external advisor

+ Has the company engaged an auditor to assess its cybersecurity risk management program separate and apart from the financial statement audit?

+ Has the company engaged an auditor to provide assessment services to assist in identifying and assessing key cybersecurity risk areas and controls designed by management to address such risks?

+ Is the company ready for an independent third-party examination of its cybersecurity risk management program? If so, has the board considered whether the company would benefit from an auditor's examination (e.g., SOC for Cybersecurity report) and the enhanced confidence in the company's cybersecurity efforts that the examination may provide to key stakeholders?

Conclusion

Cybersecurity presents a significant risk for many companies. Investors and other stakeholders need accurate information about how the company is managing this risk to make informed decisions. Board members can play a key role in overseeing this critical area by monitoring management's cybersecurity risk management program and related disclosures. Involving auditors in this area could assist the board in its oversight and enable stakeholders to have increased confidence in company-prepared cybersecurity disclosures.

CAQ

THECAQ.ORG

WE WELCOME YOUR FEEDBACK

Please send comments or questions to info@thecaq.org