The audit committee's role in cybersecurity vigilance

Cybersecurity is a process—and audit committees play a pivotal role throughout

By John Heaton

Cybersecurity is a process, not just a project—and audit committees have a role to play throughout. That means ensuring management is continually identifying critical data and the threats to that data, protecting it, and planning for breaches.

Identify key data and understand vulnerabilities

Effective cybersecurity begins with understanding the organization's data flow and clearly identifying its critical data and systems. Management must determine what data, intellectual property and personal information customers and suppliers are sharing with the organization and what obligations exist to protect that data. Audit committees need to ensure management has a process for identifying critical data internally and across the organization's digital supply chain.

Management also needs to identify vulnerabilities in the digital supply chain and understand any potential impacts on the organization. That means understanding who has access to the organization's most sensitive data and what controls third parties have in place to protect it. The audit committee should question management on third-party assurances that data and systems are protected both internally and throughout the supply chain.

Ideally, assurance will come from formal third-party validation such as ISO 27001 certification or a SOC 2 report. Smaller companies that can't provide this certification or reporting may need to be assessed by the organization's internal auditors. Increasingly, firms are adopting a continuous assurance approach to monitoring third parties and using tools that will monitor vendors for security breaches.

> Understanding your data flow and clearly identifying your critical data and systems is at the root of all cybersecurity. It's crucial knowledge that management and audit committees need to identify vulnerabilities, protect that data and know which regulations will apply.

John Heaton
Partner, Advisory
KPMG in Canada

Monitor the threat landscape

The audit committee should be apprised of the threat landscape and question management on their processes for monitoring it and identifying vulnerabilities. The threat actors targeting organizations are primarily cybercriminals using ransomware to extort money and nation-states targeting industries to perform reconnaissance or shut down critical infrastructure. Organizations must monitor threats to both operational technology (OT) and IT, since OT can be used to gain access to IT and has been used successfully by nation-states to attack infrastructure.

Cybercriminals are continuously innovating. For example, they've developed techniques to obtain one-time passcodes for multi-factor authentication and they're using generative AI to enhance their attacks. They're also revictimizing their targets. That means organizations need to stay one step ahead of potential attackers.

Have a plan

The audit committee should ensure management can clearly articulate its plan in the event of a cyber incident. In addition to operational risks, the firm could face substantial reputational and regulatory risks. To mitigate this, there should be a clearly designated senior officer who is accountable for contacting privacy and financial regulators, law enforcement, affected individuals and, in most cases, the media with prepared communications.

Organizations are practicing their cyber response processes by using cyber tabletop exercises to improve their ability to respond to cyber incidents. These are essentially cyber fire drills where participants practice prescribed responses to a threat and then debrief afterward. Companies are also using AI and machine learning to monitor for attacks or unusual activity and then respond more quickly. For example, if a laptop is compromised it can be automatically quarantined and the user notified.

It can be more difficult for the business side to recover from an attack than IT. In the IT department, there are often redundancies and backups. But recovery on the business side entails validating the affected data and ensuring that it's still accurate, integrated and reconciled. This may mean ensuring pricing, accounts payable and payment records are up to date, and determining when the last transaction was posted and where to obtain the data needed to rerun any missing transactions. These are business activities that IT can't help with, so the audit committee will need to ensure that business processes are in place to restore data integrity after a cyber incident.

Questions audit committees should be asking:

- Do we understand the data flow of the organization and have we identified critical data and systems?
- What are the risks we face based on our data, threats and vulnerabilities?
- What controls do we have in place and what gaps might we have?
- What's our plan to respond in the event of an incident?
- Do we have a process for managing regulatory reporting in a consolidated, structured fashion?

Report incidents

Cyber incidents are typically reported to the audit committee on a priority basis. For instance, a ransomware attack on the financial reporting system would be reported immediately while an infection on an employee's laptop might be reported quarterly. Some incidents will need to be reported to governments and regulators, and the audit committee will want to review this reporting before it's submitted.

Audit committees should be asking management about the reporting requirements across its operations and locations, and what the process is for managing all of these in a consolidated, structured fashion. Here again, an inventory of the organization's data is essential in knowing which regulations will apply to the organization.

The audit committee needs to ensure that management is also monitoring and preparing for new regulations. For instance, beginning in December 2023, the U.S. Securities and Exchange Commission (SEC) will require registrants and foreign private issuers to disclose material cybersecurity incidents and report annually on their cybersecurity risk management, strategy and governance [1].

In Canada, Bill C-26, The Critical Cyber Systems Protection Act, was introduced on June 14, 2022 [2]. While it's not yet law, it's currently designed to apply to sectors 'that are vital to national security or public safety,' and it will bring reporting requirements to these organizations [3].

Align cybersecurity with the business

Cyber strategy must be aligned with the business and not operate in silos. The cyber team must be involved in the business planning process. It's imperative that customers and other stakeholders have trust in new solutions and processes, and the cyber team can help ensure these are secure if they're engaged early in the design and implementation process. The audit committee needs to question management on how they plan to ensure that trust is embedded in new solutions and processes.

Cyber is a major risk for organizations, but it's only one of many areas that audit committees must monitor. That's why the cyber team and audit committee must focus on the 'digital crown jewels.' Like the approach to internal control over financial reporting (ICFR), it's important to focus on the most critical systems and data—and not every application. To be more effective, discussions with management should focus on risks and risk mitigation and not as heavily on the technical aspects of attacks and protection.

Cybersecurity is an ongoing process and audit committees have a role throughout in ensuring management is identifying and protecting key data, looking ahead and adapting to the evolving threat landscape.

Contact us

John Heaton
Partner, Advisory
KPMG in Canada
416-476-2758
johnheaton@kpmg.ca

[1] SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, Washington D.C., July 26, 2023

[2] BILL C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, First Session, Forty-fourth Parliament, 70-71 Elizabeth II, 2021-2022

[3] Bill C-26.