Audit committees and cyber security: New threats, new tools and the fundamentals

Audit committees must ensure management has fundamental cyber security in place

By Hartaj Nijjar

Each year organizations become more digitally interconnected and each year, cyber risk evolves. Increasingly, audit committees are being tasked with oversight of cyber risk management and, as a result, they need to keep abreast of new developments. Among these are the increased risk from supply chains, the burgeoning use of AI to both perpetrate and combat attacks and the growing realization that cyber resilience must be more rigorously evaluated and managed.

Nation states and organized crime remain the primary threat actors. In the past year, heightened global geopolitical disruption drove an increase in state-sponsored cyber threats. At the same time, organized criminal activity, which had seen a brief lull, returned as strong as ever with a focus on recruiting corporate insiders in addition to traditional activities like ransomware attacks. Threat actors are also exploiting vulnerabilities in widely used digital products, allowing them to breach multiple organizations at once without a specific target.

Focusing attention on the supply chain

Audit committees are putting supply chain security higher on the agenda in the wake of several high-profile third-party compromises—where an organization's environment is breached through a vendor or supplier's IT systems. As the threat from these attacks intensifies, managementcan no longer treat them as just one of many points of failure. Instead, they must dig deeper, think creatively to anticipate these breaches and audit committees should evaluate whether the organization is taking sufficient steps to prevent, identify and mitigate them.

To start, management should be developing a comprehensive map of the organization's supply

> Don't forget the basics. Sophisticated new tools to combat cyber threats are only effective if basic cyber security practices are already in place.

Hartaj Nijjar
Partner, Service Line Leader, Cybersecurity

chain to identify where critical data and systems components intersect with suppliers. This will provide insight into critical dependencies at vendors and help locate potential points of failure. From here, experts can home in on the pathways to a potential breach, identify areas where the organization is too dependent on a supplier or set of suppliers and diversify vendors where required.

Organizations may also need to revisit how they profile third parties. Those using an annual or semi-annual checklist approach—a list of security measures and best practices that outlines how to protect their systems, data, and infrastructure from cyber threats—should consider a more thorough and continuous approach. This would help them fully understand whether the reported controls at the third party are actually in place and whether they meet the standards and expectations of the organization. Audit committees should encourage management to regularly examine whether the evaluation of third parties is being performed with suitable rigour.

AI brings new tools and new risks

Cyber threat actors are increasingly using AI to target and tailor their attacks and search for new vulnerabilities. They're producing sophisticated deepfakes of images, videos and voice, using those to trick people into helping them. For example, users have been targeted by sophisticated AI generated emails and voice calls in an attempt to compromise their email accounts. Call centres at banks have also been targeted in an attempt to get customer information. These types of attacks are expected to increase considerably, so management will need to ensure they're keeping up to date on the latest attack techniques and the many tools and services that are available to detect and mitigate them.

Sophisticated tools are needed to combat these attacks. While cyber threat actors are increasingly using AI, organizations are also applying AI to cyber defence. AI can sift through massive data sets in real time, derive actionable insights and be trained to take automatic defensive actions. It's being used to improve incident detection, assess vulnerabilities, manage access and assess third-party risks. However, AI comes with its own set of risks and creates a new avenue of attack for threat actors. Audit committees must ensure their organizations are using AI safely and securely and mitigating newly introduced privacy, reputational, regulatory and cyber security risks.

In our 2024 CEO Outlook, 80 per cent of Canadian CEOs agree that building a cybersecurity-focused culture is central to how they integrate AI in their organization. [1]

AI must be specifically designed for the cyber security task being performed, and only high-quality data should be used to train the models. Robust data integrity and privacy protocols must be in place, and access to the data and algorithms must be controlled. Audit committees should question management on how they're dealing with the unauthorized and ungoverned use of AI by individuals in the workplace and how they're keeping track of and complying with the myriad evolving regulations governing AI. To develop secure AI applications, organizations will need to upskill or outsource, and so will audit committees tasked with ensuring management has appropriately evaluated AI security.

[1] KPMG in Canada. "This means core". Accessed October 31, 2024. https://kpmg.com/ca/en/home/insights/2024/10/this-means-core.html

Questions audit committees should be asking:

- Are we thoroughly evaluating third-party risk?
- Is our use of AI secure and does it meet privacy standards?
- Are we rigorously testing our incident response and thoroughly vetting our MSSP?
- Do we have the skillset in the organization to implement and manage AI solutions, and does the audit committee have sufficient knowledge or access to outside experts to evaluate them?
- Is our cyber security reporting thorough and timely enough?

On the front lines: Incident detection and response

Incident detection is one of the first lines of defence in combating cyber attacks. It's critical for organizations to be able to spot suspicious activity and determine the type of attack that's occurring so they can respond quickly. Creating an environment where suspicious activity can be quickly detected is a complex undertaking requiring cyber threat intelligence, use case development, logging, monitoring and responding. Increasingly it involves automation and the use of AI.

Some organizations perform this function internally, using tools available in the market. While helpful, these tools are only as good as the use cases they're designed for, and they need to be monitored by qualified professionals to ensure their alerts are investigated. Organizations also risk becoming overly reliant on these tools rather than focusing on the process of threat detection and response.

Given these challenges, it's common to outsource these functions by engaging third parties such as Managed Security Service Providers (MSSPs). However, many organizations fall short when evaluating their MSSP, which often fails to meet the needs of the organization. Two-thirds of executives doubt their choice of MSSP, particularly when it comes to managed detection and response (MDR). [2]

The shortcomings in both internally managed incident detections and third-party services leave many organizations blind to certain attacks. To help mitigate this risk, it's imperative that audit committees encourage management to implement cybersecurity exercises between offensive and defensive cybersecurity teams, such as "red teaming" and "purple teaming". These exercises simulate attacks, detection and responses to foster collaboration and strengthen offensive and defensive capabilities. Audit committees must also ensure that management is providing thorough and timely reporting on threats, incidents and their response.

[2] KPMG in Canada. "The role of trusted and innovative MSSPs in empowering Canada's cybersecurity". Accessed October 31, 2024. https://kpmg.com/ca/en/home/insights/2024/03/role-of-trusted-and-innovative-mssps.html

Cover the basics

Although cyber threats are becoming more sophisticated, basic cyber security principles are still instrumental in securing an organization. It's crucial to have solid foundational security controls such as vulnerability management, configuration and compliance monitoring and good governance in place. Yet, many organizations don't have these fully covered. For instance, some still have difficulty managing timely security patches. Audit committees should question management on whether the organization has the base requirements in place for a sound cybersecurity environment.

Audit committees are increasingly being called upon to take a lead role in overseeing cyber security. To do so effectively, they must build their own cyber skillset and challenge management to understand the new avenues threat actors can take and the new tools for combatting them. They must also be sure that basic cyber security practices remain the foundation upon which new tools and techniques are applied.

Contact us

Hartaj Nijjar
Partner, Service Line Leader,
Cybersecurity
KPMG in Canada
416-228-7007
hnijjar@kpmg.ca