How audit committees are leading amid evolving cyber risks

As cybercriminals deploy new tools and techniques, audit committees will play a pivotal role in guiding management through this new environment.

The rise of AI-driven attacks has pushed cybersecurity beyond the realm of IT, making it a core issue of trust, reputation and governance. Cybersecurity remains a top concern for Canadian CEOs, according to our latest annual CEO Outlook.[1] And while most organizations recognize the importance of cybersecurity, audit committees have a crucial role to play in overseeing and guiding their cybersecurity practices.

> “
>
> Most organizations invest in cybersecurity, but many don’t have a cybersecurity program. Audit committees can help guide management toward developing and implementing an adaptable, evolving cybersecurity and attack recovery plan.

Alexander Rau
Partner, Advisory Services
– Cybersecurity, KPMG in Canada

The threat landscape is evolving

Cyber threat actors are so busy they’re abandoning the seasonal lulls once seen in cyberattacks and are using artificial intelligence (AI) chatbots to handle negotiations for their more routine ransomware attacks. They’re also becoming more aggressive and asking for higher ransoms—tactics that are paying off and encouraging even more crime.

In our 2025 CEO Outlook survey, 97 per cent of Canadian CEOs expressed concern about fraud, identity theft and cyber-attacks.[2] In the coming year, ransomware attacks are expected to remain elevated, in part because the percentage of targeted organizations paying ransoms has risen as threat actors target small and medium-sized enterprises (SMEs) that decide they can’t afford the downtime that comes with a protracted negotiation and data recovery process.

Organizations may not always have the right security controls in place, so it is imperative that they have a plan for how to respond to a ransomware attack or other breach. The audit committee can provide valuable guidance by questioning management as to when they might

[1] KPMG in Canada. “Leadership in the breach”. Accessed October 15, 2025

[2] KPMG in Canada. “Productivity in the deep”. Accessed October 15, 2025.

© 2025 KPMG LLP, an Ontario limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

pay a ransom, how much they'd be willing to pay, who is tasked with making decisions during an incident and how the organization plans to recover in the wake of an attack. They should also ensure management has a clear strategy for communicating transparently with impacted customers, regulators and other stakeholders to maintain trust and demonstrate accountability.

Business email compromises (BECs) are also expected to remain a significant threat. These attacks occur when cybercriminals infiltrate an organization's email system, impersonate a senior staff person and direct another person at the organization to provide them with sensitive information or to unwittingly direct payments to the threat actors. These attacks have become much more effective with AI, which is used to make phishing emails harder to detect. Cybercriminals can even add a personal touch by following up their emails with a phone call—increasingly with an AI-generated voice that mimics the person they're impersonating.

Despite advances in the technology being used by cybercriminals, the traditional approach of training employees in proper cybersecurity practices remains an important tool for preventing these attacks. Audit committees should ensure that management is providing ongoing cybersecurity education across the organization that addresses current threats as well as mitigation and reporting procedures.

Insurers are taking a closer look

As threat levels and payouts increase, cyber insurance companies are becoming more stringent when evaluating claims. In 2025, an insurer denied the claim of a Canadian organization that had experienced a major cyberattack. The insurer argued that the target organization had failed to implement multi-factor authentication as required by their insurance policy and this lapse was instrumental in allowing the attack to take place. As a result of the denial, the organization was forced to realize a material expense of several million dollars.

It's essential that organizations are able to offload the risk of cyber incidents as the costs can be large enough to threaten the organization's survival. Audit committees should ensure management is familiar with the insurance policy's clauses, including what's covered and for how much. Management must also thoroughly understand the limitations, exclusions and conditions of coverage and be sure the firm is complying with any

Questions audit committees should be asking:

- What is our plan in the event of a ransomware attack?
- How are we training our employees?
- How are we mitigating third-party risk?
- Who has accountability for cyber security?
- How are we evaluating the effectiveness of our cybersecurity measures?

© 2025 KPMG LLP, an Ontario limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

requirements outlined in the policy. It can be useful to conduct tabletop exercises for various attack scenarios and evaluate what would be covered by the policy and whether the coverage would be valid given the organization's current cyber defense practices.

Audit committees must monitor regulatory requirements

At a bare minimum, organizations should be complying with all applicable regulations. This past year saw regulatory developments in Canada and the EU that will create new reporting obligations and affect how organizations shape their cybersecurity programs. For example, the EU's Network and Information Security Directive (NIS2) mandates cyber risk governance, risk management and reporting requirements for certain European organizations. It was slated to be fully in force in 2025, but rollout has been uneven across member nations.

In Canada, Bill C-8 was introduced in June 2025. If passed, it will apply to organizations operating in critical sectors such as finance, telecommunications, utilities and transportation, requiring them to develop and implement a cybersecurity program that must be submitted for annual review. It will also require in-scope organizations to report cybersecurity incidents to the Canadian Centre for Cyber Security (CCCS) within 72 hours, allow the government to issue legally binding orders for organizations to take specific measures related to cybersecurity and impose significant penalties for non-compliance with the Bill.

Audit committees must keep abreast of new regulations globally and satisfy themselves that management is taking the appropriate steps to monitor emerging regulations, evaluating whether the organization is in scope and complying where it is. Though most audit committees at mature organizations have cyber expertise among their membership, many could still benefit from having a formal, ongoing process for the audit committee to track new and changing regulations.

In this regard, communication between organizations, mostly through industry bodies, is an emerging source of information sharing. Through this cooperation, organizations can exchange intelligence on new threats, mitigations and regulations. Audit committees may wish to discuss with management whether this would be a useful avenue to pursue, if they are not already participating.

Audit committees can guide organizations toward an evolving cybersecurity program

Meeting standards and regulations is not enough. A cybersecurity program should be risk-based and look at all potential cyber risks, addressing them in order of priority to the organization. Audit committees, with broad oversight of these risks and their importance to the organization, can offer insightful guidance when questioning management on their cybersecurity plan. Another lever through which the audit committee can shape cyber practices and exert its influence within the organization is through internal audit, which can hold management accountable for the cybersecurity program.

While most organizations have made significant investments in cybersecurity, many fail to implement a true cyber security program. The audit committee should ensure that management has developed a program that continuously evolves and adapts to meet new regulations, threats, threat actors and

© 2025 KPMG LLP, an Ontario limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

technologies. This plan should include a well-defined governance structure that makes clear which departments and individuals are accountable for cybersecurity and outline measures for testing and evaluating the effectiveness of the program. The committee should also satisfy itself that management is not just pursuing the most recent or high-profile regulations or threats at the expense of continuing to address other risks. Organizations must continue to cover the basics, such as making routine patches, while still tackling new risks.

Ironically, a cybersecurity program's past success can hinder its future success. Since effective cybersecurity programs will prevent attacks and mitigate the damage from those it doesn't, organizations can start to believe that cyber is not a threat and fail to devote sufficient resources to maintaining a robust cybersecurity program.

In an era where cyber threats are rapidly evolving and regulatory demands are intensifying, audit committees must move beyond compliance to actively challenge management on cyber preparedness, ensure robust incident response plans, and advocate for ongoing investment in cybersecurity. By taking a proactive role, audit committees can help their organizations stay resilient and ready for tomorrow's evolving threats.

Contact us

Alexander Rau

Partner, Advisory Services – Cybersecurity
KPMG in Canada
alexanderrau@kpmg.ca

kpmg.com/ca/audit

© 2025 KPMG LLP, an Ontario limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. 30954