Audit committees need to look internally to fight cyber threats

Defending against cyberattacks starts with looking at an organization's processes, controls and partners

By Hartaj Nijjar

Hacks and breaches can be costly, damage the reputation of a company and open it to litigation—making cybersecurity one of the most pressing issues facing organizations today. Companies must have a cyber strategy both to protect their operations and to secure customer data. Audit committees, overseeing many of the company's activities and performance, must be certain management is keeping up with the evolving threat landscape and has sound strategies in place to identify and mitigate risk.

The threat landscape is ever-evolving

In the latest KPMG *CEO Outlook*, 85 per cent of Canadian CEOs surveyed said that having a strong cyber strategy is critical to building trust with key stakeholders. But building a strong cyber strategy is challenging as the threat landscape continuously evolves. We're seeing a rise in hacks on mobile devices, as well as nation-state hacking and deep fakes being used for political gain. Cybercriminals are also selling turnkey solutions to less tech-savvy threat actors so they can gain access to organizations and do damage.

In light of the current geopolitical unrest, organizations are paying more attention to potential threats to their operational technology and the effects that attacks on critical infrastructure could have on their own business and beyond.

Regulators are governing the use of personal information

A major evolution taking place globally isn't necessarily a new threat, but a new regulatory environment. In line with this global movement–and inspired by regulations such as the General Data Protection Regulation (GDPR) in Europe—Quebec introduced Bill 64, *An Act to modernize legislative provisions respecting the protection of personal information.* The first set of requirements was rolled out on September 22, 2022, and the remaining requirements will be rolled out in 2023 and 2024.

> The audit committee plays a strategic oversight role of risk management activities and monitoring procedures related to cybersecurity. A growing remote workforce, adoption of cloud services, and accelerated digital transformation have made their role even more critical.

Hartaj Nijjar
Partner, Cyber Security
KPMG in Canada

Bill 64 applies to Quebec-based companies and out-of-province companies doing business in Quebec that either collect, process or hold the personal information of Quebec residents. It forces companies to be more rigorous and transparent with their personal data practices by setting out new regulations around such things as breach reporting, privacy officers, consent and anonymization of data. Audit committees will want to question management on the ramifications for their organization and ensure there's a plan to be compliant.

Organizations should also view the Quebec legislation as a bellwether. Similar legislation is expected to be rolled out Canada-wide, and if other jurisdictions offer a hint of what's to come, the fines for non-compliance may be material. Beyond satisfying regulatory requirements, organizations should use this new bill as a catalyst to examine their data and privacy practices.

One of the first steps is to determine what data they need to be collecting. They'll also need to consider how they're collecting the information and where all the personally identifiable data sits within the organization, including structured and unstructured storage. They should also ensure they have adequate access controls and implement procedures and processes to monitor and track data.

This requires examining the data lifecycle from ingestion to destruction, and ensuring controls are wrapped around the data at each point it touches the organization. If data is being stored in the elsewhere, then the controls of third and fourth parties may need to be audited. Large organizations likely have many distributed systems of controls. Where this is the case, the aim should be to centralize controls across the whole enterprise as much as possible which would make it easier to enforce a standard set of controls.

Questions audit committees should be asking:

- How rigorous is our data protection strategy and is it sufficient in the face of growing regulation?
- How are we identifying blind spots?
- How are we vetting third and fourth parties and ensuring their continued compliance with our requirements?
- How are we protecting our automated processes and verifying that the bots we're using throughout the company have not been tampered with?

This initiative will be resource-and time-intensive. But the biggest hurdle most firms will face is directing the investment needed and finding the right talent. Audit committees should be asking management about their data and privacy controls, and ensuring the company is directing sufficient resources to implement these measures and hire the necessary talent.

Organizations are looking for blind spots

Companies also need to devote resources to identifying blind spots. These are 'black swan' events that they haven't thought of yet. For example, recent high-profile cloud and telco outages interrupted the operations of large swaths of customers. These outages have prompted organizations to ask where they potentially have blind spots that might affect their operations and then develop resiliency to ensure they can weather the next event.

There's no real science to this exercise. It involves brainstorming potential catastrophes and imagining how and where they might impact the organization. This should start with the most critical processes, tracing them from beginning to end, and examining interconnections with people, processes, infrastructure, and applications. The aim is to identify points where something could go wrong (internally or externally), to put controls in place at these points and then create fail-safe plans in case these controls break down. Audit committees will want to ask management what the company is doing to identify potential disruptive events and what resiliency plans they're putting in place to mitigate risk.

Third-party risk is on the agenda

The search for blind spots is made more necessary because almost all organizations are reliant on third parties for services or data. This exposes them to the risk of third-party outages that could affect vital services. But it also exposes them to the risk that a cyber breach in their value chain could extend into the organization. Identifying and managing third-and even fourth-party risk is on the agenda of most boards and audit committees.

Traditional practice is to have vendors fill out questionnaires about their controls and data protection practices and sign contracts stipulating they will maintain certain safeguards and controls. But it's difficult, costly and time-consuming to verify these third-party practices and there's no guarantee that vendors are in turn vetting their third parties—leaving them, and your organization, exposed to risk.

Audit is automating

There's a strong push to automate as organizations look to become more efficient or move employees to higher-value functions. Increasingly, automation is being used for operational monitoring and control executions, which means audit committees need to understand how management has confidence in the efficacy of these automated controls—that they've been implemented properly and are being operated effectively.

Automation is also being employed in the audit function. Audits are time-consuming and labour-intensive, so audit teams are turning to automation to continuously assess subsets of controls (rather than picking samples from periods during the year). This increases quality and allows audit teams to focus on more complex control assessments.

While automation in these areas is helping to drive efficiencies, it also introduces new targets for potential cyber attacks. Audit committees need to ensure that management has a solid understanding of how bots are being used in the company and can recognize signs of potential tampering.

Developing a strong cyber strategy often starts with looking at an organization's own processes, controls and partners. Audit committees looking to gain reassurance around cybersecurity and privacy protection will want to be sure management has examined their processes from beginning to end, identified areas of potential vulnerability, and put in place plans for controls.

Explore the Accelerate article series

Contact us

Hartaj Nijjar
Partner, Cyber Security
KPMG in Canada
416-228-7007
hnijjar@kpmg.ca