Cyber-related risk a top concern for audit committees

Automation and AI can help tackle growing cyber threats and talent shortage

By Hartaj Nijjar

Cybersecurity is among the most complex and rapidly evolving issues facing organizations. New research from KPMG finds that only 38 percent of Canadian companies feel cybersecurity is "deeply embedded" into all aspects of their governance and management processes. As cyber threats grow more sophisticated, so does the audit committee's responsibility for cybersecurity risk oversight. It's critical that audit committees have a fundamental understanding of the organizational risks and vulnerabilities associated with a remote workforce, adoption of cloud services, and accelerated digital transformation.

The rise of insider threats

Phishing continues to evolve and create new risks for organizations. Cyber attackers are starting to use new tactics, such as bribing employees, to gain access to a corporate network. While the threat of insider attacks is nothing new, there is growing concern about disgruntled employees who refuse to abide by mandated workplace vaccine policies and may be susceptible to bribes from cyber attackers.

We've seen a spike in phishing and ransomware attacks since the start of the pandemic when employees started working from home en masse. But cyber attackers aren't just targeting financial institutions and multinational companies; they're also going after hospitals, universities, government agencies and critical infrastructure. The recent Colonial Pipeline ransomware attack that took down the largest fuel pipeline in the U.S. was the result of a single compromised password.[1]

Audit committees need to ensure controls are in place to identify potential insider threats, detect malicious activity—including an employee who

> **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

[1]Turton, William; Mehorotra, Kartikay, June 4, 2021, *Hackers Breached Colonial Pipeline Using Compromised Password*, Bloomberg

provides network access to an unauthorized external party—and respond to a breach. That's why identity management is becoming a critical component of any cybersecurity strategy. A Zero Trust framework, for example, is an approach that eliminates 'trust' and requires all users to be authenticated, authorized and validated before gaining access (and maintaining that access) to data and applications.

Managing risk in the cloud

At the same time, many organizations have accelerated their digitalization plans during the pandemic, such as moving key services to the cloud. But in many cases, they're trying to migrate to the cloud as quickly as possible or centralize their cloud services, without enough consideration of cloud security. While cloud providers do offer a base level of security, it's up to tenants to secure their data, applications and user access (and, depending on the type of cloud, their virtual network traffic). Many organizations rely too much on the cloud provider, without recognizing they share responsibility for security.

Some organizations are moving their 'crown jewels' to the cloud while others are taking a more measured approach; it depends on their appetite for risk. Audit committees need to ensure controls are in place to manage which data and applications can be migrated to the cloud (and by whom) and to secure data and applications once in the cloud. But there's no definitive guide or framework on how to do this—and those that do exist are open to interpretation—which poses another challenge for audit committees.

What should audit committees be asking?

- Have we identified which threats are most relevant to our organization and our industry?
- How are we evaluating and monitoring those risks?
- How are we staying on top of evolving risks, such as employee bribery?
- What are we doing to prioritize our remediation around the key areas of risk?
- What are we doing about cyber talent and securing our fair share?
- Are there any areas where we can use automation to simplify controls?

Addressing the lack of cyber talent

Another risk that audit committees need to consider is the severe shortage of cyber talent in the market. Every organization, in every industry, is competing for the same talent, making it difficult to recruit and retain the very people who know how to keep threats at bay and execute a cybersecurity incidence response plan.

Artificial intelligence (AI) and automation solutions can help fill the talent void and build a more resilient organization, as can working with third-party security providers. And while automation may not replace employees it can allow them to focus more on the issues that require significant attention.

Building a strong foundation for security

Organizations can't protect everything—and they can't necessarily prevent all breaches—so they need to take a risk-based approach to cybersecurity. That means understanding what's most important to the organization, where sensitive data resides and who has access to that data. Organizations also need to get better at detecting suspicious activity and fraudulent behavior. More mature organizations are investing in fusing cyber together with other data sources to provide a next-gen approach centered around threat intelligence, advanced analytics and state-of-the-art technology like AI to detect, investigate and mitigate threats through a single, integrated platform.

But first, they need a strong foundation for cybersecurity. According to KPMG, only 39 percent of companies are "very confident" in their ability to detect and respond to an attack. Audit committees need to ensure that foundation is in place and then identify any gaps (such as an inability to find cyber talent or to recognize potential insider threats). To become a truly resilient organization, they need to focus on response, not just prevention. That means ensuring they have a strategy to respond and recover when—not if—a security breach occurs.

Contact

Hartaj Nijjar
Partner, Cyber Security
KPMG in Canada
416-7228-7007
hnijjar@kpmg.ca

Let's do this. home.kpmg/ca/audit