KPMG

# Cyber Risk Governance and the Board's Role

## Integrating Cybersecurity into the Corporate Strategy.

**The cyber threat landscape is constantly evolving, and so are the expectations and obligations of the Board of Directors. As the ultimate stewards of the company's strategy, performance, and reputation, the board has a critical role to play in overseeing and guiding the company's cybersecurity risk management.**

Cybersecurity should be seen as part of a broader data governance framework that includes privacy and AI considerations. Understanding what data is collected, how it is used by people and AI technologies, and how it is protected is critical.

Boards should require regular reporting on cybersecurity risks and the effectiveness of the organization's cybersecurity program. This will allow the board to monitor the organization's cybersecurity posture and make informed decisions.

The board should ensure management integrates cybersecurity risks into their strategy and takes appropriate measures to manage this risk while promoting business agility and the ability to recover swiftly from a cyber attack.

The board needs to have confidence that regulatory concerns are managed and the organization is compliant with all relevant laws.

> **Directors should approach cyber risk, not as a one-time event or set of questions, but rather by providing comprehensive, ongoing oversight to ensure management has a holistic, adaptive cyber risk strategy aligned to the organization's business goals, focused on delivering long-term value - an investment in the organization's future"**
>
> ***— John Heaton***
> ***Cyber Partner, KPMG in Canada***

## Things to Consider in 2024:

**01** The Securities and Exchange Commission (SEC) has adopted new rules that will require more cybersecurity disclosures from US-listed public companies starting December 2023. They must disclose within four business days that they have sustained a material incident.

Additionally, they will be required to disclose risk management and governance information as related to cybersecurity in annual disclosures.

**02** Cybersecurity continues to face a talent shortage, impacting recruitment and retention. High-stress roles can cause fatigue and burnout. Boards should address this gap, providing resources and ensure management is thinking about succession planning.

**03** Generative AI offers opportunities but also new risks. It is the responsibility of the boards to ensure the safe and ethical use of this technology. It will be used by organizations to address the talent shortage but also by threat actors for improved phishing and fraud attempts.

**04** There is continued growing value placed on resilience. Even the best security can't guarantee 100% protection. Resilience measures ensure continuity of operations even in the wake of a successful breach. Response and recovery capabilities are more important than ever.

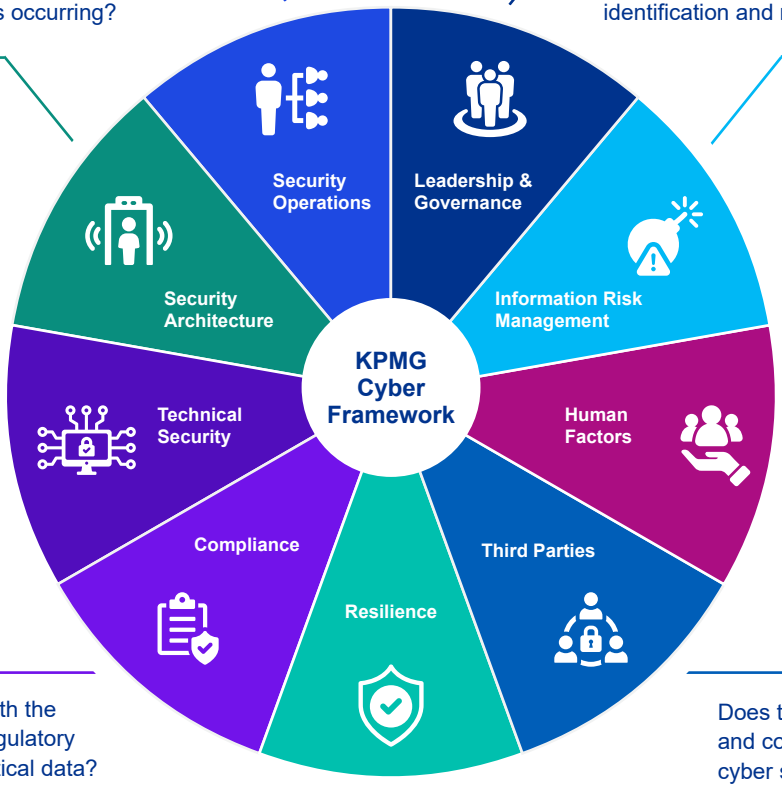
# Key questions the board should be asking about Cyber Risk

Does the organization have procedures and controls that protect key data and minimize the likelihood of a cyber security breach? Can it detect when a potential breach is occurring?

Has the organization assigned a qualified executive to take responsibility for cyber security? Is there a team in place to support risk identification and mitigation?

Are the organization's information systems and processes aligned with business objectives?

Is the organization identifying and prioritizing its critical data? Does it know where this data resides?




Has the organization implemented appropriate technical security solutions to address identified cyber risks?

Does the organization educate and train staff on cyber risks such as phishing? Does the organization monitor for insider threats?

Does the organization comply with the various contractual, legal and regulatory requirements that apply to its critical data?

Does the organization have procedures and controls to identify and manage cyber security risks throughout the lifecycle of a supplier?

Is the organization conducting regular tests of its crisis management and incident response plans to make sure that it is prepared for cyber security breaches and to minimize impacts on the organization?

**Given the strategic importance of this issue, oversight should be a responsibility of the board.**

As in all board risk management matters, it's clear that director education is critical to help ensure that the board, as a whole, is up to speed on the topic. Whether the board has or seeks directors with cyber expertise or uses outside experts is an issue for each board to consider.

# Contact us

For more information, please contact:


## John Heaton

Partner, Cyber Security
KPMG in Canada

(416) 476- 2758
johnheaton@kpmg.ca

## Adil Palsetia

Partner, Cyber Security
KPMG in Canada

(416) 777 8958
apalsetia@kpmg.ca