Cybersecurity - what does it mean for the Board?

Boardroom questions

Investors, governments and regulators are increasingly challenging board members to actively demonstrate diligence in this area. Regulators expect personal information to be protected and systems to be resilient to both accidents and deliberate attacks.

For Boards, this sort of attack generates questions:

- What are the **implications** of a cyber attack for the Board?
- What should **the Board do** if such an attack occurs? Is the Board **prepared**?
- What types of **losses** could be incurred? What is the scale?
- How can we be more **proactive, focused and preventative**?

Potential impacts for Boards

Intellectual property losses including patented and trademarked material, client lists and commercially sensitive data, which could have a significant financial impact.

Reputational losses causing a decline in market value; loss of goodwill and confidence by customers and suppliers.

Penalties, which may be legal or regulatory, such as fines for data privacy breaches and customer and contractual compensation for delays.

Time, lost due to investigation of the losses, keeping shareholders advised and supporting regulatory authorities (financial, fiscal and legal).

Property losses of stock or information leading to delays or failure to deliver.

Administrative resources to correct the impact, such as restoring client confidence, communications to authorities, replacing property and restoring business to its previous levels.

Boardroom Questions

What are the new cybersecurity threats and risks and how do they affect our organisation?

Do we have an up to date, detailed snapshot of the current cyber threat landscape that is understood by all? Do we understand the cybersecurity aspects of core business decisions, cutting through the technical jargon?

Is my organisation's cybersecurity program ready to meet the challenges of today's (and tomorrow's) cyber threat landscape?

Do we have a cybersecurity program with the required technical capability and processes across the organisation? Are we doing enough to mitigate risks based on our risk profile?

What key risk indicators should I be reviewing at the executive management and board levels to perform effective risk management in this area?

Do we understand the key operational issues and our current risk posture to assess if we are doing the right thing?

Are cybersecurity aspects considered in our major business decisions, such as mergers and acquisitions, partnerships, new product launches?

Are we able to assess the specific cyber risks associated with key business decisions? Is there a sound process to provide reliable information on the cyber risks associated with specific business choices?

Is there an ongoing, organisation wide awareness and training program established around cybersecurity?

Can we be confident that everyone in the organisation understands their role and responsibilities for managing and reporting on cyber risks and potential incidents?

kpmg.com.sg/socialmedia

Contact us

Daryl Pereira
Partner, Cybersecurity
T: +65 6411 8116
E: darylpereira@kpmg.com.sg

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.