KPMG
cutting through complexity

Boardroom questions:

Cyber security – what does it mean for the Board?

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 your market value to decline; loss of goodwill and confidence by customers and suppliers.

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

Time, lost due to investigating 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 resource to correct the impact such as restoring client confidence, communications to authorities, replacing property and restoring business to its previous levels.

How can Board members be on top of this issue?

To gain assurance that cyber risk is being managed, Board members need to be able to answer the right questions:

- Does my organisation meet its obligations for **information assurance**?
- Is **data secure** in my organisation?
- Do we fully understand our **current threats and vulnerabilities**?
- Do any of our **supply chain partners** put us at risk?
- Do we meet the information security requirements to bid for **government contracts**?
- Are our **competitors** ahead of us? If so, does this give them an advantage?
- Who in our organisation is responsible for **cyber security issues** and can they and the management team answer the following questions?
- Do we understand where our **sensitive data** is located, who can access it and how it is controlled?

Does your management team know what to do if your organisation is attacked?

- What should **our response** be?
- How effective has our response been?
- What do you **know about the people/organisations** responsible for the attacks and how do they operate?
- Are there any **patterns** regarding cyber attacks that make our information and assets more **vulnerable at certain times**?
- Who should we be **sharing threat intelligence** with and how? How do we establish an **effective Security Operation Center**?

Focusing on these questions at the Board level and incorporating them into the enterprise risk strategy is critical. By doing so, leaders can **quickly start to identify gaps in the current cyber security strategy** and encourage an organisation-wide approach to countering cyber crime.

How can the Board become more proactive, focused and preventative

Board level awareness of emerging cyber threats and direct involvement in determining the response is critical. Threat intelligence can help organisations become more proactive, focused and preventative.

- How do we move from **reacting to anticipating** cyber attacks?
- How do we **make sense** of the cyber threats we face?
- How do we demonstrate the **return on investment** of our cyber security measures?
- When was the cyber threat last **examined by the Board**?
- Is cyber part of the **Board's strategy** discussions?
- Does our management know **when to act**? Which tactical option to **pursue**? Has it been **effective**?

These questions are highly relevant for organisations that are seeking to take action against a cyber adversary.

So, what can the Board do about it?

KPMG believes in five principles that can help organisations manage the cyber threat proactively and help reduce the risk to customers, shareholders and employees. These are:

- **Prepare**: understand and improve the current state of preparedness against cyber attack.
- **Protect**: design and implement a cyber defence infrastructure.
- **Detect**: identify existing and potential attacker behaviours and their presence on your networks.
- **Respond**: implementation of a transparent cyber incident response plan.
- **Transformation**: organise and deliver a wholesale program of change to improve an organisation's cyber security capabilities.

KPMG's Cyber Maturity Assessment (CMA) provides an in-depth review of an organisation's ability to protect its information assets and its preparedness against cyber attack capabilities. It takes a rounded view of people, process and technology and is designed to enable clients to understand areas of potential vulnerability.

Contact us

Mark Tims
Partner, Technology, Risk & Assurance
+61 2 9335 7619
mtims@kpmg.com.au

Gary Gill
Partner in Charge, Forensic
+61 2 9335 7312
ggill@kpmg.com.au

kpmg.com.au