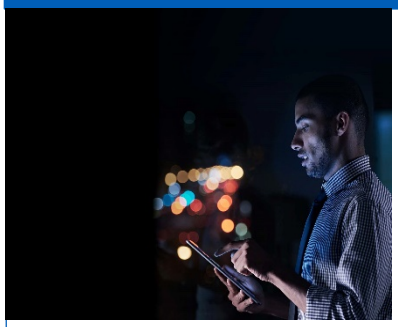
KPMG

Boardroom Questions

Cybersecurity – what does it mean for the Board?

Why cybersecurity risk is an everyday business consideration



Companies are under increasing pressure to **adopt** and **deploy new technology** in order to remain **competitive** within their markets, with technology opening opportunities to **differentiate customer experience**, reduce **operational costs**, and increase **competitive advantage**.

At the same time, **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**.

Organizations cannot afford to be held back by cyber risks. They need to make bold decisions and feel confident that their **cyber strategy, defenses and recovery capabilities** will **protect their business** and **support their growth strategies**

Business pressures: why companies should consider reviewing their cyber strategy

Pressure to find **new customers** and compete with existing and **disrupting competitors** means many companies are **leveraging digital technology** such as Robotics, Artificial Intelligence, mobility and introducing new systems **exposing the company to data risks**

A mutating threat landscape where an increasing range of highly professional **attackers are innovating faster than many businesses can improve their defenses**

Restoring trust and minimizing **reputation damage** is key for many industries – a data breach could affect **trust, reputation** and **share price**

Potential impact and possible implications for Boards

Intellectual property losses including patented and trademarked material, client lists and commercially sensitive data

Reputational losses causing the market value to decline; loss of goodwill and confidence by customers and suppliers

Penalties, which may be legal or regulatory fines 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 the organization to its previous levels

Boardroom Questions

Board level awareness of emerging cyber threats and direct involvement in **determining the response** is critical. Threat intelligence can help organizations become more **proactive, focused and preventative** to take control of cyber risk in a unique and positive way.

1. What are the **new cybersecurity threats** and risks, and how do they affect our organization?
2. Is our organization's **cybersecurity program ready** to meet the challenges of today's and tomorrow's cyber threat landscape?
3. Do we fully understand our **current vulnerabilities** and what **processes** do we have in place to deal with cyber threats?
4. What **key risk indicators** should I be reviewing at the executive management and Board levels to perform effective risk management in this area?
5. Does our **organization** meet all of its obligations for information assurance and do we **fully comply with applicable privacy & cybersecurity laws and regulations**?
6. Is cyber part of the Board's **strategy discussions** and when was the threat last examined by the Board?
7. How do we move from **reacting to anticipating** cyber attacks
8. Are our **competitors** ahead of us? If so, does this give them an **advantage**?

Questions for senior management

1. How are we **demonstrating** due diligence, ownership, and **effective management of risk**?
2. To what level have we created a **security culture** across the organization that **empowers and ensures** the right people, skills, culture and knowledge to enable cybersecurity?
3. How effective is our approach to achieve comprehensive and **effective risk management** of information **throughout the organization** and its delivery and **supply partners?**
4. Are we **prepared** for a security event? How do we **prevent or minimize the impact** through crisis management and stakeholder management?
5. What **control measures** do we have to address identified risks, and **how effective** are these to prevent or minimize the impact of compromise?
6. Do we have a clear **understanding of the legal and regulatory environment** within which we operate? How do we effectively **demonstrate our compliance** to our supply chain, customers and business partners?

What actions could the Board consider?

Consider developing a strategy that is more than just security through combining people, privacy, information governance and business resilience. The questions above will help to identify gaps in your current cybersecurity strategy.

KPMG's Cyber Maturity Assessment (CMA) provides an in depth review of an organization's ability to protect its information assets and its preparedness against cyber-crime, looking at:

- Leadership and governance
- Business continuity
- Human factors
- Operations and technology
- Information risk management
- Legal and compliance.

Contact us:

Henry Shek
Head of IT Advisory
Risk Consulting
KPMG China
T: +852 2143 8799
E: henry.shek@kpmg.com

Richard Zhang
Partner, IT Advisory,
Cybersecurity
KPMG China
T: +86 (21) 2212 3637
E: richard.zhang@kpmg.com

Bhagya Perera
Director, IT Advisory,
Cybersecurity
KPMG China
T: +852 2140 2825
E: bhagya.perera@kpmg.com

Click here for more information
kpmg.com/cn/cyber