Boardroom questions

Cyber-security – what does it mean for the boards?

Board Leadership Center (India)

Why cyber-security risk is an everyday business consideration?

Companies are under an 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, there has been an increasingly challenged environment for boards as, investors, governments and regulators expect board members to actively demonstrate diligence in this area. Regulators also expect personal information to be protected, systems to be resilient to both accidents and deliberate attacks and risks arising due to third parties, vendors and outsourcing being managed.

Organisations cannot afford to be held back by cyber risks.They need to make bold decisions and feel confident that their cyber strategy, defences 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 organisations are leveraging digital technology, such as robotics, Artificial Intelligence (AI) and mobility, and are introducing new systems, exposing them to data risks.

A dynamic threat landscape, where an increasing range of highly professional attackers are innovating faster than many businesses can improve their defences.

Restoring trust and minimising reputation damage is key for many industries – a data breach may result in regulatory fines and sanctions that can affect trust, reputation and stakeholder value.

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 stakeholders 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 organisation 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 organisations become more proactive, focussed and preventative to take control of cyber risk in a competent way.

- What are key cyber-security threats and risks and their affect on our organisation?
- Is our organisation's cyber-security programme ready to meet the challenges of evolving cyber-threat landscape?
- Do we fully understand our current vulnerabilities and what processes do we have in place to deal with cyber threats?
- 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 have the appropriate talent/cyber-security professionals to manage cyber-security risks of the organisation and extending it to the ecosystem of suppliers and partners?
- Does our organisation meet all of its obligations for information assurance and do we fully comply with applicable regulations such as the Information Technology (IT) Act, Federal Information Security Management Act (FISMA), EU General Data Protection Regulation (GDPR) and HIPAA (Health Insurance Portability and Accountability Act)?
- Is cyber a part of the board's strategy discussions and when was the threat last examined by the board?
- How do we move from reacting to anticipating cyber attacks?
- Are our competitors ahead of us? If so, does this give them an advantage?
- Do we need cyber insurance to cover our business liability to compensate in case of a cyber-security incident?
- Do we have a conscious cyber culture within the organisation for adherence to both the values and hygiene of good cyber practice?

Questions for senior management

- How are we demonstrating due diligence, ownership and effective management of risk?
- To what level have we created a security culture across the organisation that empowers and ensures the right people, skills, culture and knowledge, which enable cyber security?
- How effective is our approach to achieve comprehensive and effective risk management of information throughout the organisation and its delivery and supply partners?
- Are we prepared for a security event? How do we prevent or minimise the impact through crisis management and stakeholder management?
- What control measures do we have to address identified risks and how effective are these to prevent or minimise the impact of compromise?
- 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 cyber-security strategy.

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-crime, looking at:

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

KPMG in India contacts:

Nilaya Varma
Partner and Leader
Markets Enablement
T: +91 124 669 1000
E: nilaya@kpmg.com

Akhilesh Tuteja
Partner and Head
Risk Consulting
Global Co-lead - Cyber Security
T: +91 1243074800
E: atuteja@kpmg.com

Ritesh Tiwari
Partner
Risk Consulting
Leader, Board Leadership Center
T: +91 124 336 9473
E: riteshtiwari@kpmg.com

Atul Gupta
Partner and Head
IT Advisory
Cyber Security Leader
T: +91 124 307 4134
E: atulgupta@kpmg.com

home.kpmg/in

Follow us on:
home.kpmg/in/socialmedia

#KPMG josh