

Boardroom Questions



Cyber security – what does it mean for the Board?

Why cyber security 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 cyber security threats** and risks, and how do they affect our organization?
- ② Is our organization's **cyber security 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 General Data Protection Regulation (GDPR)?**
- 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 cyber security?
- 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 cyber security 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
- Human factors
- Information risk management
- Business continuity
- Operations and technology
- Legal and compliance.

Contact us:



Akhilesh Tuteja
Global Co-Leader, Cyber Security
KPMG International
T: +91 124 3074800
E: atuteja@kpmg.com



Greg Bell
Global Co-Leader, Cyber Security
KPMG International
Principal, Digital Solutions and Enablement
KPMG in the US
T: +1 404 222 7197
E: rgregbell@kpmg.com



Click here
for more information
www.kpmg.com/cyber-security

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.

© 2019 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Create Graphics | CRT101561A January 2019