Cyber in the boardroom

Board Leadership Centre

Companies face growing demands to embrace and implement new technologies in order to remain competitive within the market. In Saudi Arabia, this trend is particularly expedited by Vision 2030 initiatives which aim to diversify the economy through digital transformation. In this publication, we present the role that board members can play for their organizations.

Board members are facing pressure from regulators and authorities such as the Saudi Central Bank (SAMA), the National Cybersecurity Authority (NCA), the Saudi Data and Artificial Intelligence Authority (SDAIA) to actively demonstrate diligence in the area of cybersecurity.

Regulators emphasize the protection of personal information and the need for resilient systems that can withstand incidents and deliberate attacks. Furthermore, value chain partners seek a trustworthy and transparent approach to manage cybersecurity and privacy risks.

Organizations cannot afford to be held back by cyber risks, therefore, they must make bold decisions and have confidence in their cyber strategy, defenses and recovery capabilities. The steps in this document provide guidance for boards to understand more about their cyber defense mechanisms to help protect their business and effectively support their growth strategies.

The importance of regularly reviewing cyber strategies

The challenge that companies face to find new customers and stay ahead of existing and disrupting competitors means that many companies are embracing digital technology such as robotics, artificial intelligence, mobility, while introducing new systems that expose them to data risks.

There is a growing range of highly professional attackers in the current threat landscape, who continue to innovate faster than businesses can adapt to protect themselves.

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

Potential impact and implications for boards

- Potential losses of patented and trademarked material, client lists, and commercially sensitive data poses a significant risk.
- Reputational losses can result in a decline in the market value, loss of goodwill, and erosion of trust among customers and suppliers.
- Data privacy breaches can lead to penalties in the form of legal or regulatory fines. Compensation may be required for effected customers and contractual obligations.
- Dealing with the aftermath of a breach involves investigating losses, keeping shareholders informed, and cooperating with regulatory authorities (financial, fiscal and legal).
- Property losses of stock or information can lead to delays or failure to deliver, impacting operational eficiency and customer satisfaction.
- Administrative resources to correct the impact of a breach requires restoring client confidence, communications to authorities, replacing property, and restoring the organization to its previous levels.

Important questions to ask in the boardroom

The board's awareness level of emerging cyber threats and direct involvement in determining the response is critical. Leveraging threat intelligence can help organizations become more proactive, focused, and preventative to take control of cyber risk in an innovative approach. Consider the following questions to ensure a strong cybersecurity governance:

- **Who is responsible for cybersecurity issues in our organization ?**
- **What are our critical business assets?**
- **What are the new cybersecurity threats and risks, and how do they affect our organization?**
- **How are we demonstrating due diligence, ownership, and effective management of cyber risks?**
- **Is our organization's cybersecurity program ready to meet the current and future cyber threat landscape challenges?**
- **What key risk indicators should I be reviewing at the executive management and board levels to perform effective risk management in this area?**
- **Does our organization meet all of its obligations for information assurance and do we fully comply with cybersecurity regulations and the Personal Data Protection Law (PDPL)?**
- **Is cybersecurity part of the board's strategy discussions and when was the threat last examined by the board?**
- **Are we prepared for a security event? How do we prevent or minimize the impact through crisis management and stakeholder management?**
- **How do we move from reacting to anticipating cyber attacks?**
- **Are our competitors ahead of us? If so, does this give them an advantage?**

Recommendations for boards

Understanding and addressing cyber risks using aggregated cyber data and communicating in their language is becoming increasingly critical, also in the board room.

To enhance this understanding of cyber risk and improve strategic decision-making, we recommend the following approaches:

1 Assess your current cyber risk posture structure

Assess your organization's governance, human factors, information risk management, business continuity, and crisis management.

2 Identify your crown jewels

Identify your critical assets, considering that attackers can value assets from different perspectives. Examine the lifecyde of your critical information assets from development to retirement.

3 Select and steer your defense

Select and evaluate your defenses using a risk based approach. Prioritize the protection of your identified critical assets. Know the threat landscape and use cyber dashboards to create insightful risk reports to steer your risk mitigation investments.

4 Enhance monitoring and incident response

Strengthen your security monitoring, threat intelligence, and incident response with a specific focus on related threats landscape, maintaining a risk register and establishing sustainable processes.

5 Periodic performance measurement

Enhance your cybersecurity key performance indicators and key risk indicators to measure and track the effectiveness of the organization's cybersecurity program.

Contacts

Ton Diemont
Partner, Cybersecurity & Data Privacy
E: antondiemont@kpmg.com

Arbab Choudhary
Director, Cybersecurity & Data Privacy
E: arbabchoudhary@kpmg.com

Board Leadership Centre

The KPMG Board Leadership Centre offers support and guidance to non-executive directors, whether managing a portfolio non-executive career or embarking on a first appointment. We aim to equip you with the tools you need to be highly effective in your role, enabling you to focus on the issues that really matter to you and your business.

Abdullah Akbar
Partner, Audit & Head of Board Leadership Centre
E: amakbar@kpmg.com

Dr. Samer Abdallah
Partner, Advisory
E: samerabdallah@kpmg.com

Kamran Sial
Partner, Tax
E: ksial@kpmg.com

Mohammad Alkhlaiwi
Partner, Audit
E: malkhlaiwi@kpmg.com

kpmg.com/sa