Boardroom Questions

Cyber Security – what does it mean for the board?

According to KPMG`s Swiss Cyber Security Survey 2017, 88 percent of the respondents suffered from a cyber-attack in the past 12 months. These attacks disrupted business processes in 56% of the participating companies.

Source: Clarity on Cyber Security 2017 Edition, KPMG Switzerland

Over recent months many global organisations have been victims of cyber crime.
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, focussed and preventative?

Potential Impact and Possible Implications for Boards

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

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

Penalties, which may be legal or regulatory fines such as regulatory fines eg 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 organisation business to its previous levels.

Focusing on the following 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 board members be on top of this issue?

- Does my organization meet all of its obligations for information assurance?
- Is data secure in my organization?
- Do we fully understand our current 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 organization is responsible for cyber security issues and can they and the management team answer the following questions?

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

- What should our response be?
- How effective has our response been?
- What do you know about the people/organizations 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?

So, what can the board do about it?

KPMG believes in five principles that can help organisations manage the cyber threat proactively:

- Prepare – understand and improve the current state of preparedness against cyber attack.
- Protect – design and implement a cyber defense infrastructure.
- Detect – respond and investigate cyber attacks.
- Integrate – embed cyber security in the culture and decision making to help ensure it stays one step ahead
- Transformation – organize and deliver a wholesale program of change to improve an organization's cyber security
- 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 attack.

How can the board become more proactive, focussed and preventative?

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.

- 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 security part of the Board's strategy discussions?
- Does our CIO know when to act? Which tactical option to pursue? Has it been effective?

Contact

KPMG AG
Badenerstrasse 172
PO Box
8036 Zurich

kpmg.ch/blc

Matthias Bossardt
Partner
Head of Cyber Security

+41 58 249 36 98
mbossardt@kpmg.com

Yves Bohren
Director
Cyber Security

+41 58 249 48 95
ybohren@kpmg.com