Cyber Advisory Practice

Cyber Risk Management
Six questions for leaders

Traditionally the management of cyber risks has been the responsibility of Information Technology (IT) teams. Ultimate responsibility for these issues in fact lies with the Executive Leadership Team (ELT) and the Board. Organisations need to be seen to be acting towards ongoing resolution. **These are six questions that trusted advisors, the ELT and Boards should be asking immediately:**

1 Which types of events do you consider to be cyber incidents?

Cyber incidents take many forms and the severity depends on the nature of the organisation. Key impacting incidents can be:

- Loss and/or breach of confidential data
- Business interruption due to resources becoming unavailable
- Financial harm due to fraud and social engineering
- Identity theft and misrepresentation

2 Is your organisation prepared for a cyber incident?

Few organisations are adequately prepared for a cyber incident if at all. Actions for preparation include:

- An assessment of the current cyber risk management strategy including system testing
- Perform an incident readiness assessment and be involved in the preparation and ongoing management of a cyber incident response plan
- Analyse and consider cyber insurance for financial risk transfer and incident response

3 Have you engaged with the key stakeholders that can answer these questions?

Leaders should be asking the stakeholders of cyber risk management for detailed explanations and updates regarding status and exposures.

Leaders must have a working relationship with the stakeholders to ensure communication of potential issues and remediation/ minimisation strategies.

4 Have you been fully briefed on the organisation's cyber risk exposures, controls and remediation measures?

Operationally mature organisations manage cyber risk registers and integration of cyber risks into the Enterprise Risk Management framework. Whilst smaller organisations may not have these formal processes in place it is important that the function of regularly briefing leadership on cyber risk is performed.

The best process is for leaders to engage independent cyber risk management advisors that explain cyber risks without jargon. A cyber incident can happen at any time and unbriefed leadership teams have been seen to make the impact of an incident worse, especially in relation to regulatory issues and reputation. This has included misrepresentation to the public, inadequate oversight of controls and lack of involvement in incident response planning.

5 Does your organisation have a Cyber Incident Response Plan?

Leaders need to be ready to hear that there has been a cyber incident and know what steps they should take when they are informed. They also need to be assured that they will be involved, and that the most appropriate response strategies are being executed.

Due to the potential ramifications, leadership is becoming increasingly concerned about cyber risk and working to ensure that they are in a good position to explain their organisation's cyber risk management posture.

6 Do you understand your leadership liabilities with respect to cyber risk?

Leaders, outside of IT, are increasingly being held accountable for cyber incidents. This is especially the case with poorly managed cyber risks where there are impacts to the organisation financially and reputationally. These are not "IT problems", they are the operational responsibility of executives under Board governance.

Globally there has been a sharp increase in scrutiny of the role of Directors and Officers in cyber risk management. This will continue.

Executive leadership and Boards should be concerned about the potential impact to them in terms of:

Fines & penalties around:

- Data breach notification
- Failure to implement strategies for data protection
- General privacy violations

Civil action against organisations and directly to Directors and Officers:

- Privacy violations
- Negative impact on share value due to failures of cyber risk management strategies
- Failure to disclose risks to stakeholders

Some other areas of concern are:

- Leadership team and Board restructures of individuals failing to fulfill their operational and fiduciary duties around cyber risk
- Irreversible brand and reputation damage bringing impact to the organisation's financial value, sometimes forcing an organisation to shut down

The global trend towards more stringent regulation in this area, and the increase in successful civil actions, means leaders need to be aware of where their responsibilities lie, what they can expect in future and the steps their organisations are undertaking to reduce their liability.

If leaders cannot answer these questions with certainty, then they should immediately take, at least, the following steps:

- Evaluate existing cyber risks and risk management strategies
- Seek independent advice from experienced cyber risk advisors
- Leverage their existing trusted advisor network including legal and insurance experts

As a result of these ramifications, leadership is becoming increasingly concerned about cyber risk and working to ensure that they have are in a good position to explain their organisation's cyber risk management posture. All organisations, regardless of size or function, should be on the path to cyber risk operational maturity.

Please contact the Cyber Advisory Practice with any queries.

CAP
thecap.io

The Cyber Advisory Practice
Level 35, One International Towers
Barangaroo, NSW Australia 2000
+61 2 8046 6895 | contact@thecap.io