A TIGHTER HOLD ON INFRASTRUCTURE CYBER SECURITY

KPMG Board Leadership Centre

With new regulatory requirements approved, board leaders need to quickly grasp the changes and ensure that their organisations are ready for the uplift.

Click here to watch a recording of this Board Leadership Centre event

> "When you look at the day-to-day cyber incidents that are reported, one every 8 minutes, 25 percent of those relate to critical infrastructure."
>
> **HAMISH HANSFORD**
> Inaugural Head of the Australian Cyber and Infrastructure Security Centre

Key updates to the Security of Critical Infrastructure Act 2018 passed through the Senate in late 2021, meaning company directors have new responsibilities to understand and ensure are implemented. KPMG Chairman Alison Kitchen said the changes, "are designed to put more stringent frameworks around how organisations can work to protect Australia's critical infrastructure assets, particularly from cyber-related attacks."

To help board members unpack what this means for them, Kitchen hosted a KPMG Board Leadership Centre virtual panel conference along with Matt O'Keefe, ASPAC Cyber Leader, KPMG Australia. Their guests included Byron Collie, Executive Director in Technology & Cyber Operational Risk, JP Morgan Chase, Michelle Price, CEO, AustCyber, and Hamish Hansford, Inaugural Head of the Australian Cyber and Infrastructure Security Centre. Here are some of the key points raised.

Notable changes

O'Keefe outlined that the new bill expands the definition of 'critical infrastructure' to cover 11 sectors, meaning a greater mix of board leaders will need to take notice. Hansford then highlighted two obligations to watch out for.

"The first thing is, it enlivens a register of critical infrastructure assets…And that allows us to compile a sense about who owns and has beneficial ownership of critical infrastructure in Australia," he said.

He said the information is then mapped to show dependencies between critical infrastructure assets and to provide advice to Treasury on any foreign investment issues.

The second factor to note, which existed in the previous version, is the mandatory cyber incident reporting for corporations. However, once reported, the new bill allows for an Australian Signals Directorate (ASD) response in the event of a "very significant cyber security incident impacting the prosperity, security or defense of Australia, at a very high threshold where no other regulatory system is able to respond."

Increased threat landscape

O'Keefe asked why the enhanced infrastructure asset protection measures were so important, to which Hansford responded that the cyber threat landscape had significantly increased.

"…the Director-General of Security (ASIO) this year in his annual report said he's particularly worried about the pre-positioning by nation states of cyber exploits on our critical infrastructure as a key concern on our national security perspective. Equally, when you look at the day-to-day cyber incidents that are reported, one every 8 minutes, 25 percent of those relate to critical infrastructure."

> "The role of the CISO now is around being part of the strategic forward vision of the organisation, and building trust to digital business networks."
>
> **MATT O'KEEFE,**
> ASPAC Cyber Leader, KPMG Australia.

Price added that of these risks, one of the biggest that board leaders need to be aware of is ransomware – a threat that has accelerated during the global pandemic.

"…what we did learn obviously through the heat of COVID...(is) that complexity is now being aimed at the smallest businesses as well as the largest," she said.

Price said there was a growing awareness that cyber risk doesn't just sit within your own organisation, but in supply chains – particularly with ransomware perpetrators looking for a vulnerability.

"The supply chain side of this is where I think we will see enormous numbers of challenges going forward…and where we really must see partnership and collaborations coming into play with larger organisations working with each other, but also downstream within smaller organisations, to really uplift the security of the processes, and the people that we use around the technologies," she said.

Managing the regulatory uplift

O'Keefe asked Collie how boards could drive a seamless uplift to meet the new regulatory expectations. Collie said to first understand the expectations placed on your organisation by the regulations, then to look at how the regulatory agencies are going to approach those regulations, and what they will be looking for.

His second point was to look at global frameworks for cyber security risk management for guidance. He mentioned the National Institute of Standards and Technology (NIST) in the US, and in Australia the ASD and the Australian Cyber Security Centre frameworks, which can help leaders to understand what good looks like in terms of cyber risk management, and what management should be reporting to the board.

Collie said boards should be expecting management to inform them on the threat landscape, how well-managed that landscape is, the path to addressing threats, the investment required, what is needed in terms of control, and the processes if risks eventuate.

"…at what level would management actually engage the board if something were to happen in your environment? That particular escalation piece to the board is something that should be very, very clear," he said.

Cyber risk operating models

O'Keefe asked Price what she thinks the key attributes of a cyber risk operating model of the future should be. Price pointed to two things – the first being around the importance of how risk is built into the organisational structure, as well as between the board and the management team, and the organisation and supply chains.

"…does the CISO (Chief Information Security Officer) have the supported ability to approach the CEO super-fast if something is going down?" she said.

The second component is to create "trusted markets of information" which can be relied upon in the event of a risk coming to fruition, so decisions and action can be quickly taken.

"How do we make sure that we have the trust within our ecosystem of companies and regulatory agencies and partners more broadly, so that when something does happen, we can trust the information that we are receiving into the organisation?" she said.

Collie added it was essential to have detailed awareness of contract terms with software providers, particularly as organisations increasingly work in the cloud.

"It's the same as any other vendor engagement, it comes back to the fundamentals, what's in the contract and how you can enforce it," he said.

O'Keefe made the important link between cyber risk operations and building or maintaining stakeholder and customer trust in the organisation.

"...the role of the CISO now is around being part of the strategic forward vision of the organisation, and building trust to digital business networks. How are you going to interact with your customers, with your employees, with your supply chains, and what does trust mean in those systems, and how is that going to be protected?" he said.

Regulatory harmonisation

O'Keefe asked how Australian cyber security regulations were interplaying with global regulations. Price responded that both can help, so the most important thing is having 'principles' around how your cyber security is managed, as well as an internal governance committee that can stay across all of the developments of the different jurisdictions the business is involved in.

"More (Australian) organisations are choosing NIST (regulations) over ISO (regulations), but if you've got most of your customer base offshore in Europe, then you'd go for ISO," she said.

Hansford added that the government is less concerned about which standard an organisation is adhering to around cyber security, but more so if it helps the organisation to meet its regulatory obligations.

"We're looking at the outcome. And the outcome is for you to look at cyber security in your business," he said.

Security everywhere

With employees increasingly working away from the workplace, O'Keefe asked Collie how secure the 'work-from-home' environment can be. He responded that the answer lies in the implementation of the technology.

"You need to look at the totality of what work-from-home looks like to your particular business activity, how it's been technically implemented, and then the risk assessment associated with it," he said.

He added that there will be vulnerabilities, but understanding how work-from-home could increase infrastructure asset risks, and focusing on continuous improvement are essential.

A final takeaway

As board members get prepared for the new bill, O'Keefe asked each panelist for a final piece of advice to take away.

For Collie, it was to have cyber security front of mind in discussions with management.

"…do not be afraid to ask questions, do not be afraid to actually improve your learning on the subject and request management educate you as well," said Collie.

Price pointed out that board members need to understand how the practice of cyber security is built into the organisation, how it is part of the culture, and if customers trust your approach.

"…increasingly, customers are expecting more from you to be able to hold their trust in the organisation," she said.

Hansford wrapped up with a tip regarding the cyber security of the board members themselves.

"We often see the CEO, managing directors and board members subject to cyber threat, which then affects their role in business…look after your passwords and make sure that security is in check. Then, look after your business," he said.

KPMG.com.au

The information contained in this document is of a general nature and is not intended to address the objectives, financial situation or needs of any particular individual or entity. It is provided for information purposes only and does not constitute, nor should it be regarded in any manner whatsoever, as advice and is not intended to influence a person in making a decision, including, if applicable, in relation to any financial product or an interest in a financial product. Although we endeavour 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.

To the extent permissible by law, KPMG and its associated entities shall not be liable for any errors, omissions, defects or misrepresentations in the information or for any loss or damage suffered by persons who use or rely on such information (including for reasons of negligence, negligent misstatement or otherwise).

Liability limited by a scheme approved under Professional Standards Legislation.