KPMG

Cyber security:

Are Australian CEOs sleepwalking or a step ahead?

kpmg.com.au

Cyber attack is one of the biggest threats to Australian businesses, however many Chief Executive Officers (CEOs) admit a lack of preparedness against security breaches. KPMG International's outlook study *Cyber security: A failure of imagination by CEOs* reveals the vulnerable position many Australian businesses are in as a result. Here we outline the key findings, with advice on what Australian CEOs can do to reduce risk.

The facts about Australia:

- Globally, only half of CEOs are fully prepared for a future cyber-security event, with Australia behind at 35 percent.
- 40 percent of Australian CEOs expect the Chief Information Officer (CIO) position will become more important, on par with the global average.
- 29 percent of global CEOs said cyber security is having the biggest impact on their company, just ahead of 25 percent in Australia.

"Collectively we sleepwalked into a position of vulnerability and failed to learn lessons of embedding security into products right out of the gate."

Malcolm Marshall, Global Head of Cyber Security at KPMG

For Australian CEOs and their management teams, the requirement to keep ahead of cyber security threats is vital for the safety of their business and customers. KPMG's *Cyber security: A failure of imagination by CEOs*[1], which surveyed over 1200 international CEOs, found that emerging technology risk was one of the biggest risks CEOs are concerned about – for 21 percent of CEOs globally and 37 percent of Australian CEOs.

The survey also found that 25 percent of CEOs globally are extremely concerned about keeping up with new technologies. The figure was less in Australia, at 19 percent, however 40 percent were somewhat concerned, while 40 percent were not concerned about it.

However, the real issue appears to be a lack of preparedness for a cyber attack. Of the 52 Australian CEO participants in the survey, only 35 percent said they were fully prepared for a cyber event, compared to the global result of 49 percent. A greater portion of Australian CEOs, 58 percent, were somewhat prepared, while 4 percent said they were not where they need to be, and the rest were unsure.

Security must run deep

CEOs need to realise that building cyber security into products and processes can be a competitive advantage, says Malcolm Marshall, Global Head of Cyber Security at KPMG. "Some organisations are turning security into a selling point with touch identification," he explains. Banks, for example, are starting to replace outdated security processes with touch ID.

While 40 percent of Australian CEOs expect the Chief Information Officer (CIO) position will become more important, cyber security should not be left in the domain of this role. CIOs are often not part of the C-suite inner circle, which could mean the rest of the organisation surrenders responsibility to the IT function rather than making sure security is built into behaviour, controls and processes. It's vital that the CEO and senior executives engage with the issue. There is a bottom line benefit too – Marshall says institutional investors are less likely to invest in a company that has had a major public cyber breach.

1. See survey methodology at the end of this report.

"Organisations need to understand what the 'crown jewels' are, what value they would have in the wrong hands, where they are located and how well they are protected."

Gordon Archibald, Cyber Security Leader for KPMG in Australia

Cyber security: a strategic risk

Nearly a third of the global CEOs listed cyber security as one of the issues with the biggest impact on their company (in a multiple choice answer). Australia was just short of this at 25 percent, amid the issues of economic growth at 40 percent and energy prices at 27 percent.

Globally, one out of five CEOs indicated that information security is the risk they are most concerned about, similar to Australian CEOs at 29 percent. Across the board, operational and compliance risks rated highly, but cyber risk, if uncontrolled, becomes an operational issue and a regulatory issue very fast.

Is Australia ready?

In Australia, many CEOs and boards understand the importance of cyber security, however their understanding is not yet at a level that can drive action, according to Gordon Archibald, Cyber Security Leader for KPMG in Australia. Part of this is due to lack of visibility of what needs to be done. "This falls with management who may sometimes struggle with building impetus to clearly define the problem – what am I trying to protect, what are my risks and how well protected are those assets?" he says. They are aware of the threat, but they don't always see the potential impact to the business if those assets get into the wrong hands.

What are Australian CEOs doing?

Discussions about the issue

In Australia, 60 percent of the CEOs said they had met with their executive teams or board of directors four to six times in total to discuss cyber security, up on the global rate of 40 percent, while 27 percent said they had done so one to three times, and 10 percent had done so seven to 10 times. Four percent had never done so.

Appointing the experts

In promising results, 88 percent of Australian CEOs had taken pre-emptive steps to appoint a cyber security executive or create a cyber security team, better than a result of 50 percent globally. Yet just 23 percent of Australian CEOs had taken pre-emptive steps to convene multiple meetings with their cyber security team, down from the global result of 37 percent. However 73 percent of Australian CEOs were planning to do so in the next 3 years.

Others had taken pre-emptive steps to hire a cyber security consultant – 37 percent globally and 38 percent in Australia – while in Australia 52 percent intended to do so in the next 3 years.

Upgrading technology

Compared to 49 percent globally, 42 percent of the Australian CEOs had taken pre-emptive steps to upgrade current technologies with a view to cyber protection, while 50 percent planned to take steps in the next 3 years. Eight percent had no planned action.

New technologies had been deployed by 21 percent of Australian respondents, compared to 40 percent globally, however 71 percent were planning to take steps to deploy new technologies in the next 3 years. Again, 8 percent had no planned action.

Internal and external processes

In Australia, 50 percent of respondents had taken pre-emptive steps to change internal processes with cyber security in mind – for example securing data sharing, or how employees use mobile devices containing company data. Forty-two percent were planning to do so in the next 3 years, while 8 percent had no planned action. In terms of changes to external processes, for example client data gathering or receiving invoices, 40 percent had taken pre-emptive steps to security, higher than the global result of 34 percent. Forty-eight percent of Australian CEOs were planning to do so in the next 3 years, and 12 percent had no planned action.

"The root cause is often a failure of imagination. A failure to imagine the sophistication and persistence of their attackers."

Malcolm Marshall, Global Head of Cyber Security at KPMG

How prepared is your company for a cyber threat?

Region	Global average	Australia	US	UK	China
Fully prepared	49%	35%	87%	28%	41%
Somewhat prepared/ not where we need to be	50%	62%	13%	64%	59%
Unsure	1%	4%	0%	8%	0%

Who you have is important

Organisations need to invest in the right tools and the right people to protect against cyber threats. Bringing in security intelligence can help pinpoint problems, identify anomalies and highlight unusual or suspicious activity. However one of the biggest challenges CEOs could face is skills shortage. Global estimates suggest that over 23 percent of cyber security positions take more than six months to fill, with a further 10 percent remaining unfilled.

Key lessons for Australian CEOs

1. Understand your enemy

It's vital to understand who might attack an enterprise, what they would attack and why. A cyber security framework can help organisations understand which assets are most in need of protection and which could cause damage if compromised. This framework helps focus investment and protection appropriately.

2. Share threat intelligence

Organisations can expand their security intelligence by sharing information about their own security threats with peers and competitors. While some sectors are reluctant to do, banks are leading the way with this approach.

3. Create collaborative networks

"White-hat hackers" can use their hacking powers positively rather than illegally, by helping organisations find weaknesses in their architecture. Executives are often surprised at how quickly an accomplished hacker can infiltrate their systems.

4. Be aware of fourth-party risk

Many organisations, particularly banks, have long thought about third-party cyber risk. Some have multiple suppliers so that if one fails, they have resilience. But a deeper look might reveal that the risk gets reconsolidated at the next layer because all of their diversified suppliers are reliant on a single supplier — a phenomenon known as fourth-party risk. This discovery is common in assessing liquidity risk, but the process can be equally revealing for cyber resiliency. For instance, what if all of your suppliers rely on the same cloud provider?

5. Merging or acquiring? Find out the real situation

A common risk for cyber safety is mergers and acquisitions. Buying a company that has not built security into its products can be costly, so due diligence is vital.

6. Have a response plan

One way companies can expand their expertise is by bringing in security intelligence to pinpoint problems, identify anomalies and highlight unusual or suspicious activity. Intelligence can help in two ways. First, an "early-warning-as-a-service" can reduce the vulnerability threat window: the time between the detection and the remediation of an attack. Intelligence can also provide a broader picture of global threats than any one organisation could gather on its own. Security is an ecosystem; organisations need to know what is going on externally as well as internally. Further to this is the need for a swift and effective response plan. If hackers do get in, know exactly how you will mitigate the damage and test the plan to ensure it works.

kpmg.com.au

In summary

There is no such thing as complete security coverage. CEOs must lead their organisations towards a proactive and predictive approach to cyber security, instead of relying too heavily on reactive technologies such as firewalls or intrusion prevention, or putting all the responsibility in the hands of the CIO. Understanding the threat landscape, knowing your enemy, and getting the right help with security intelligence is essential. What you can't prevent, you should try to detect. And what you can't detect, you should be prepared to respond to quickly.

Contact us

Gordon Archibald
Partner
+61 2 9346 5530
garchibald@kpmg.com.au

Gary Gill
Partner
+61 2 9335 7312
ggill@kpmg.com.au

Mark Tims
Partner
+61 2 9335 7619
mtims@kpmg.com.au

Methodology The survey data published in this report are based on a survey of 1,276 chief executives from Australia, China, France, Germany, India, Italy, Japan, Spain, UK and the US. Nine key industries are represented, including automotive, banking, insurance, investment management, healthcare, technology, retail/ consumer markets and energy/ utilities. Three hundred forty seven CEOs came from companies with revenues between US$500 million and US$999 million, 626 from companies with revenues from UD$1 billion to US$ 9.9 billion, and 303 from companies with revenues of US$10 billion or more. The survey was conducted between April 22 and May 26, 2015.