CEO Outlook Survey – Australian findings on Cyber concerns

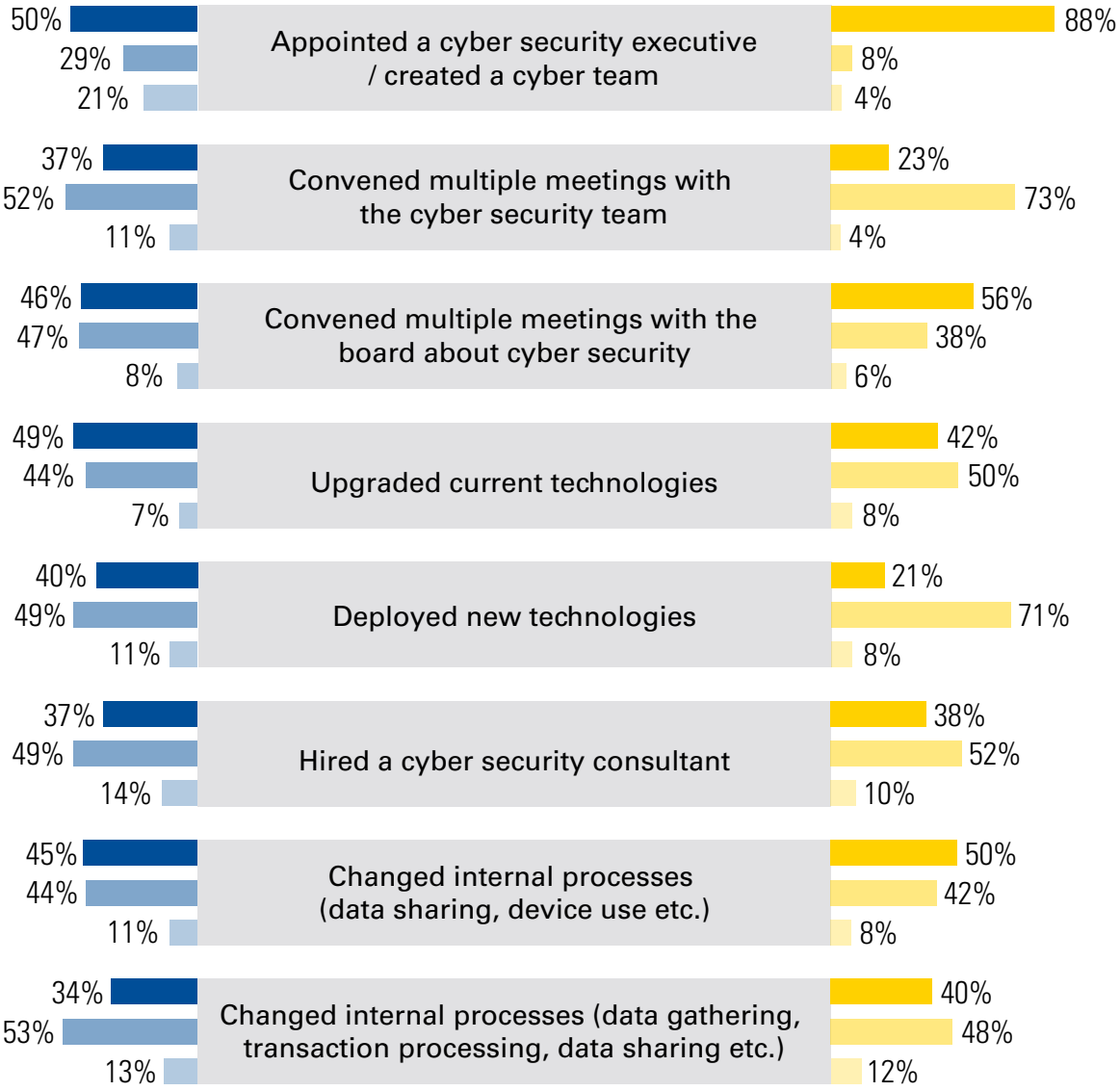
What's keeping CEOs awake at night?

Emerging Technology Risk
37%

Information Security Risk (Cyber)
29%

CEOs globally are concerned with operational and strategic risk. In Australia that concern is focused predominantly in the cyber domain.

Defence and Protection



Key

Have taken pre-emptive steps | Planning to take steps in the next 3 years | No planned action

The data published in this infographic are based on a survey of 1,276 chief executives from Australia, China, France, Germany, India, Italy, Japan, Spain, UK and the US. Fifty four Australian CEOs were surveyed. Nine key industries are represented, including automotive, banking, insurance, investment management, healthcare, technology, retail/ consumer markets and energy/ utilities. Three hundred and 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.

Resilience

Arguably any connected system that depends on information technology – no matter how many layers of protection it possesses – is vulnerable. The interconnectivity of cyber systems combined with the ever changing threat landscape creates an environment that will never be 100 percent secure.

Out of the 52 Australian respondents, only 35 percent stated they were fully prepared for a cyber-event.

Business resilience remains a key component to any cyber defence strategy.

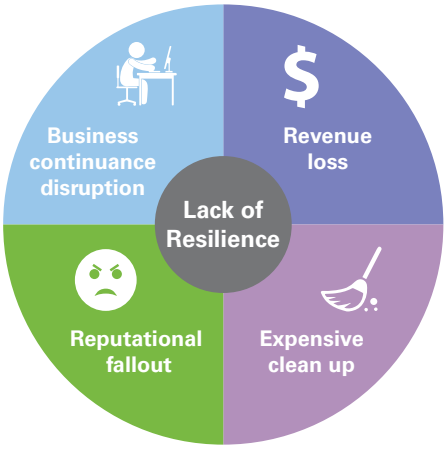
Australia is at the forefront when it comes to cyber resilience having implemented five out of eight security measures according to the global CEO survey ahead of its international counterparts. A higher intent to implement in the next 3 years was seen in the remaining three measures.

Interestingly there appears to be a disparity between the views of CEOs, who believe their organisations are reasonably prepared for a cyber-event and the operational level who disagree. Australian organisations could be operating under a false sense of security, which could have ramifications for the development of a comprehensive cyber security strategy.

Improving resilience

- Research and Development: Commitment to ongoing research into, and development of, current and emerging technologies is critical to the successful implementation of a robust cyber resilience plan.
- Internal Communication: Results indicate the majority of Australian organisations have strong channels of communication between the board and the CEO through regular cyber meetings. However, regular meetings between the CEO and the cyber security team are lacking and would create a stronger channel of communication. The Chief Security Officers (CSOs) could play a key role to address this issue.
- Awareness and Guidance: Development of collective security practices would work to create a network of prevention, awareness and assistance. Increasing governance and risk management requirements now extend externally to include supply chain management. This increased connectivity and interaction means that all organisations play an active role in sharing critical intelligence on cyber security.
- The role of cyber resilience leaders: In Australia, this could be further enhanced. A high number (88 percent) of the Australian CEOs indicate that they have taken pre-emptive steps to appoint cyber executives and implement cyber teams. Yet anecdotal evidence appears to indicate this is not translating to an operational level of comfort as all other pre-emptive steps are only marginally higher than the global average. This might be indicative of the cyber message getting lost in middle management.

Lack of Resilience



Contact us

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

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

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

kpmg.com.au