www.pwc.com.au/gsiss-2018

The global importance of cybersecurity awareness

A broader spectrum of Australian organisations embrace cyber capabilities

PwC's 2018 Global State of Information Security® Survey (GSISS)

pwc

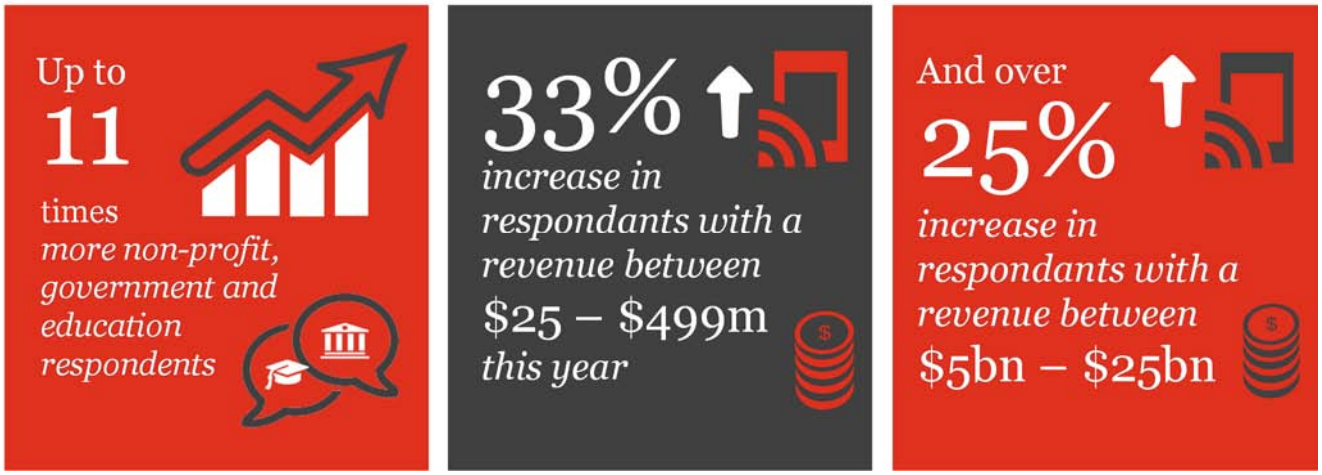
Table of contents

Introduction

This report focuses on the Australian results from PwC's 2018 Global State of Information Security® Survey (GSISS). It shows that across Australia, all organisations irrespective of size need to continue to become more involved in understanding and assessing their cyber risks, as cybersecurity breaches continue to increase in both frequency and impact.

Key findings for Australia

An increase in respondents from organisations of all sizes from the prior year:



Big business problems are becoming small business problems. Australia has experienced several high-profile data breaches recently where a large organisations' data was taken from a smaller third party business partner. In one attack in 2016, almost 30 gigabytes of commercially sensitive information related to naval vessels and warplanes was stolen from a local defence contractor. The organisation in question was defined as a "small 'mum and dad type business' – an aerospace engineering company with about 50 employees".[1]

Threat actors are now targeting business connections in order to expand their attack surfaces. Business partners of all sizes are now as much of a target as any larger scale business. Many recent breaches have been through business partner exposure, as illustrated by the Defence contractor.

Operational Technology Cyber Risk

According to the World Economic Forum (WEF), a growing trend of using cyberattacks to target critical infrastructure and strategic industrial sectors, raising fears that, in a worst case scenario, attackers could trigger a breakdown in the systems that keep societies functioning.[2]

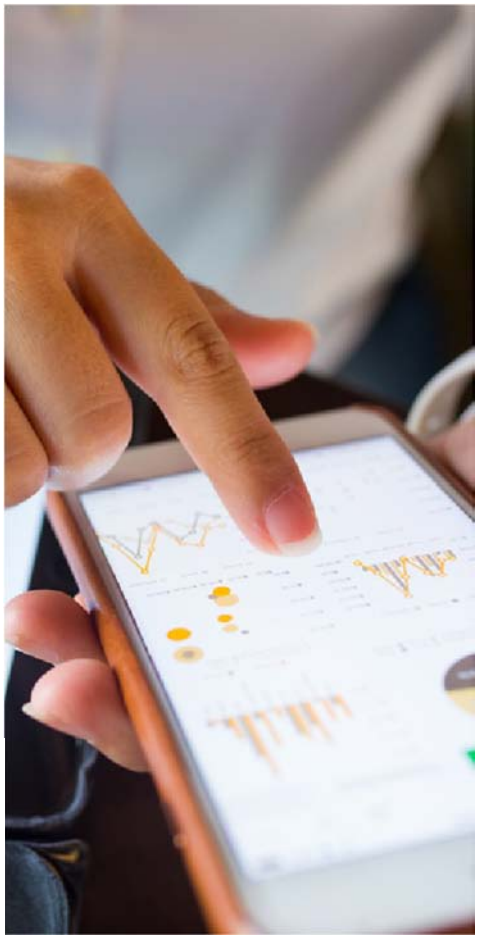
As the world's reliance on data and interconnectivity grows, all organisations are now concerned about the threat to the availability of operational technology (OT) networks and their increasing vulnerability from the Internet of Things (IoT).

---

[1] http://www.skynews.com.au/news/top-stories/2017/10/12/defence-contractor-s-cyber-security-breached.html

[2] World Economic Forum, 2018 Global Risks Report, January 2018

According to a recent ACCC Communications Sector study draft report, it is anticipated that in Australia, "by 2025 IoT will provide one to two percent uplift in GDP per year, and an impact of $45 billion to $116 billion across all key sectors of the economy."



Forty per cent of global respondents cited the disruption of operational technology as the biggest potential consequence of a cyberattack, 39% cited the compromise of sensitive data, 32% harm to product quality, 29% damage to physical property, and 22% harm to human life. According to a recent ACCC Communications Sector study draft report, it is anticipated that in Australia, "by 2025 IoT will provide one to two percent uplift in GDP per year, and an impact of $45 billion to $116 billion across all key sectors of the economy." Clearly the threat is real and can be costly to not just individual businesses, but to the nation's economy.

How does Australia compare?

This report also looks at some differences in China's approach to cybersecurity compared with Australia's, and the impacts being seen in the China environment.

As a result of prior year investments in cybersecurity, the number of incidents detected in China reduced markedly. Chinese respondents have an increased confidence in their ability to detect and respond to cyber based incidents.

Internal focus on compliance with the June 2017 implementation of China's cyber security laws (CSL), and investment in compliance with the upcoming EU GDPR requirements are preparing the country for expansion in their trade and partner environments. Australia have also increased the regulation related to cyber with the introduction of the Australian Notifiable Data Breach scheme on 22nd February 2018.

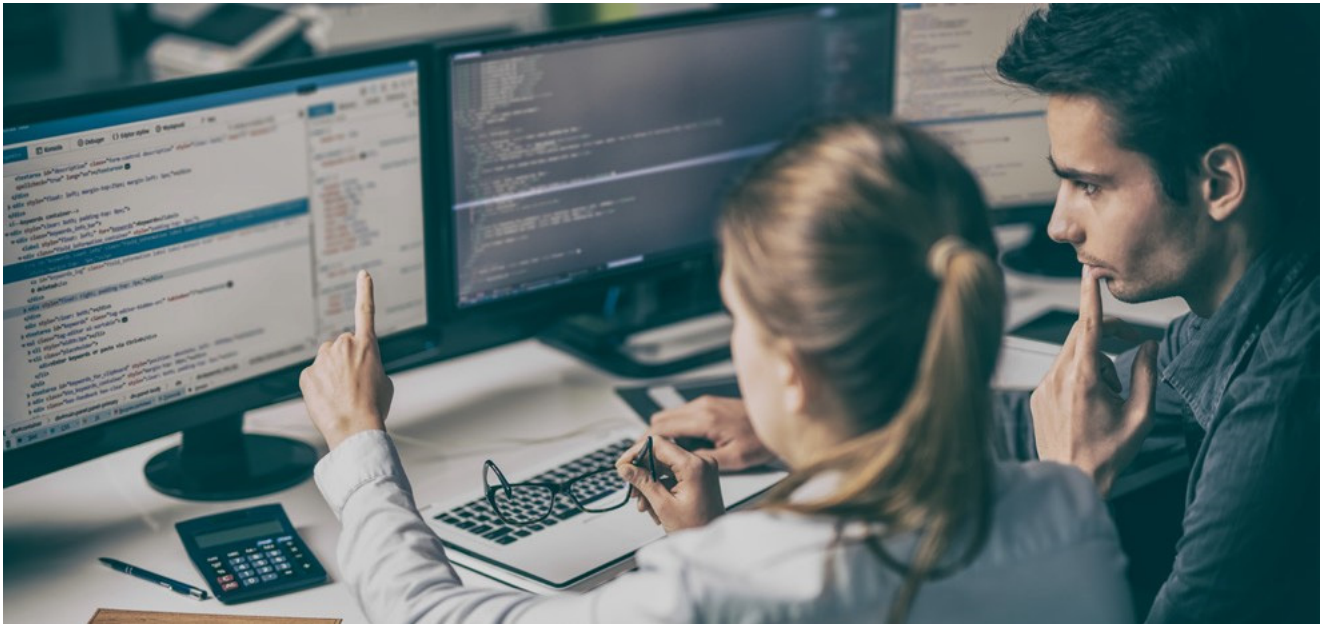
The China 'Belt and Road' initiative, will see investment in infrastructure that aims to open land and sea connectivity with national and international trade partners. The CSL will aid the management of the cyber risk associated with such an economic expansion.

The Australian response

In Australia, this year's GSISS results indicate that information security concerns are being recognised more widely, with greater responses from SMEs, the education sector, and not for profit organisations. In the current survey, Australian responses made up 13.2% of those from the Asian region.

There was greater Australian participation in this year's survey from the following sectors:

- SMEs, with the response rate of enterprises with revenue between $25m – $499m rising from 25.8% last year to 33.7% this year, an increase in respondents of 31% and
- non-profit, government and education – an increase in respondents of 11 times from last year.



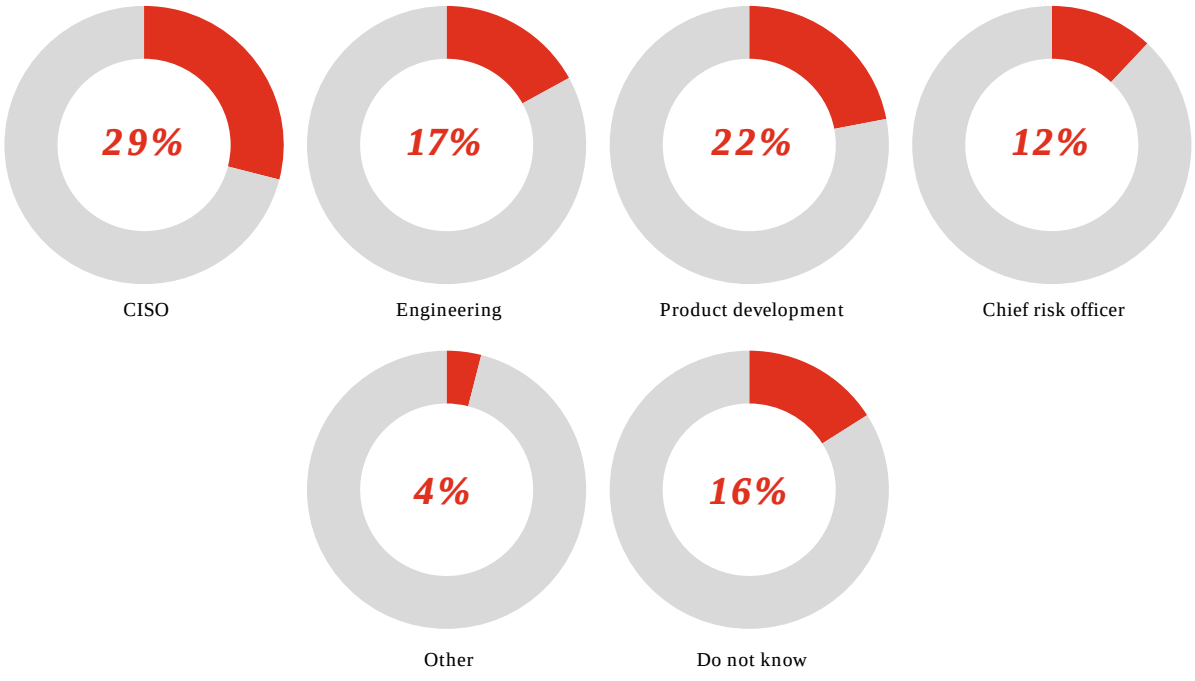
Issues for Australian respondents

Operational technology and Internet of Things

Achieving greater cyber resilience as a society and within organisations will require a more concerted effort to uncover and manage new risks inherent in emerging technologies. Organisations must have the right leadership and security processes to cope with digital advancements. Many businesses are just beginning this journey.

Based on this year's GSISS, we found that 28.6% of Australian organisations' chief information security officers (CISOs) are accountable for IoT. At the same time, 16.1 per cent of respondents are not aware who is responsible for IoT in their firms. Defining the right accountability is an issue that needs to be addressed as a priority.

Who is responsible for IoT [3]

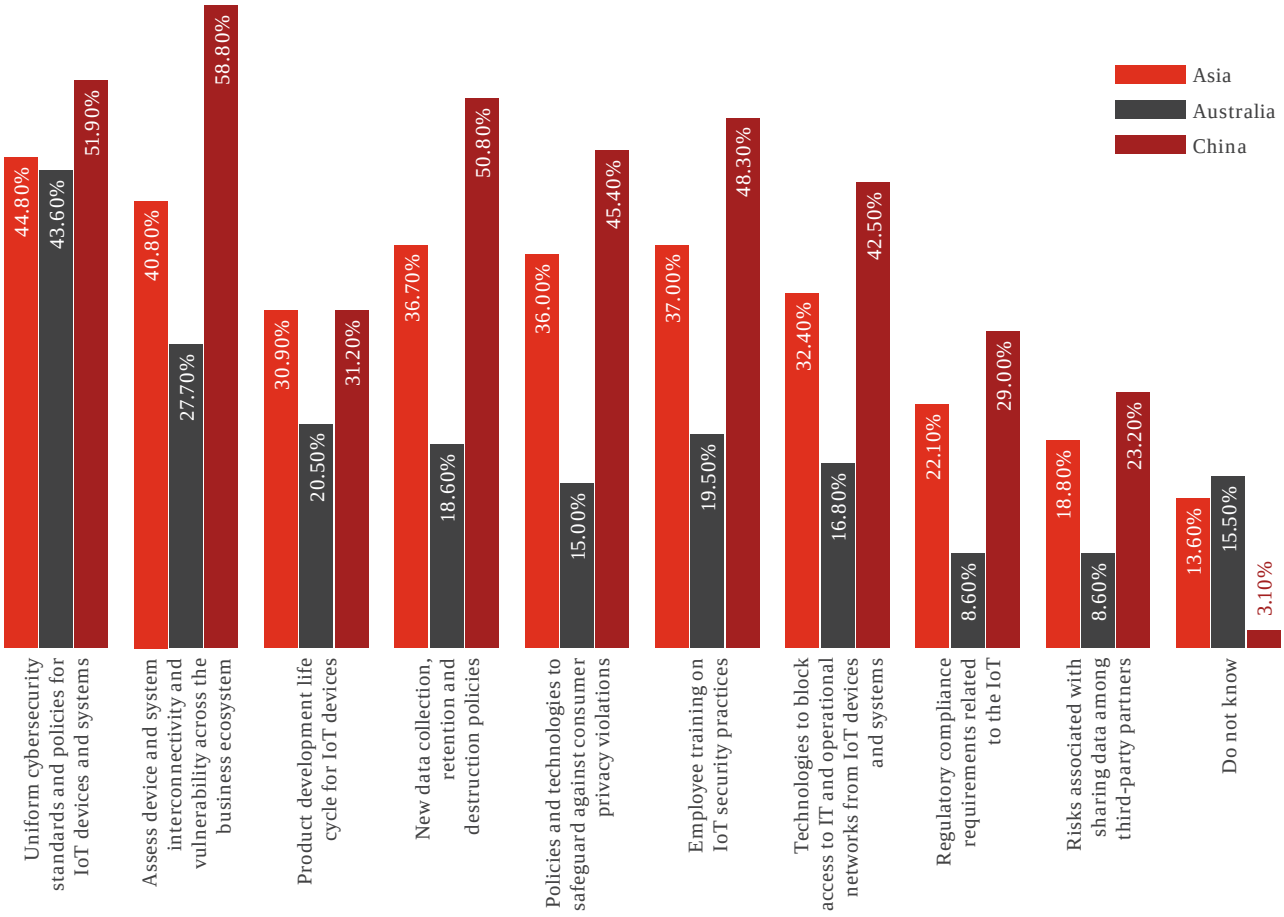


It is also interesting to note that Australian responses overall, seem to be less interested in this area of protection than both their Asian and Chinese Counterparts.

---

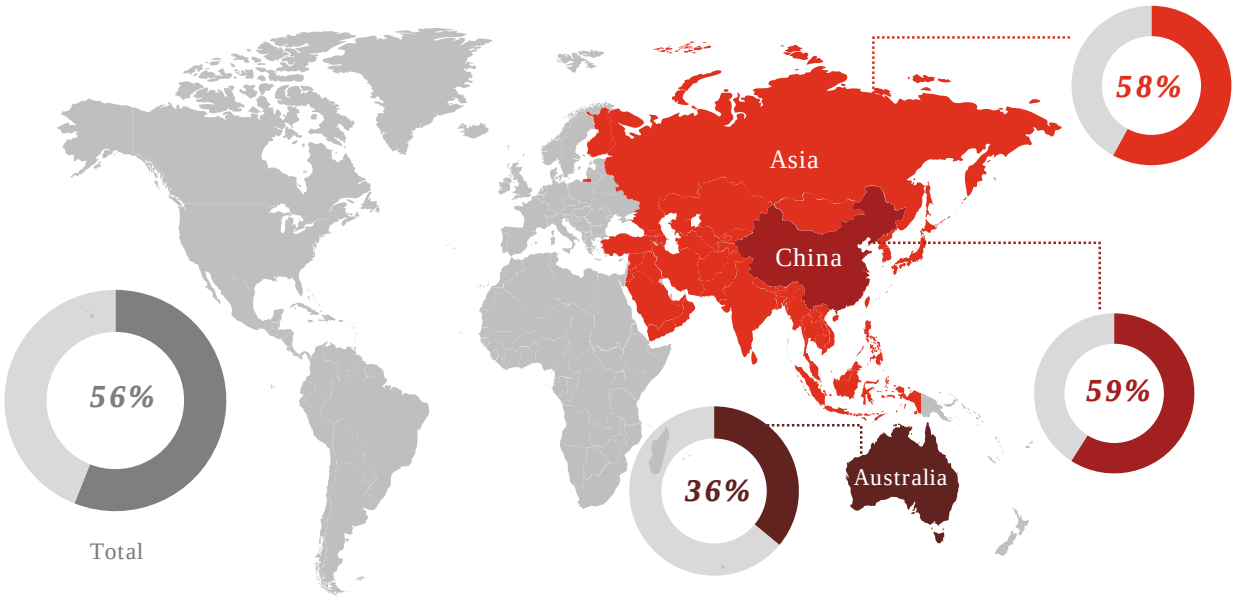
[3] Who in your organisation is responsible for the Internet of Things (IoT)?

Plans for policy, technologies and people skills to implement over the next 12 months



Australian figures indicate a lower number of respondents having an overall information security strategy in place with Australian numbers lower than both global and regional standards, and in sharp decline on prior years, which comes from the greater number of responses from smaller Australian organisations, who are less mature overall than larger Australian respondents.

Overall information security strategy



With over
33%
of respondents coming from the $25m - $499m range of business representing

a 31% *increase in responses from previous years*

Globally, the responses from businesses ranging from non-profit to $499M represents in excess of

48% *of the response total*

SMEs more aware

More Australian SMEs are embracing cyber security capabilities than in previous years, with over 33% of respondents coming from the $25M – $499M range of businesses representing a 31% increase in responses from previous years. Globally, the responses from businesses ranging from non-profit to $499M represents in excess of 48% of the response total.

The number of Australian government and educational organisations and non-profit agencies participating in the 2018 survey increased 11 times from the previous survey results.

Three factors have influenced this greater awareness amongst smaller organisations:

1 Two ransomware attacks were influential in WannaCry attack in mid-May hit 200,000 victims in 150 countries, locking computers and holding users' files for ransom.

2 Data breach disclosure laws.

3 Larger organisations assessing their smaller business partners and suppliers' security controls

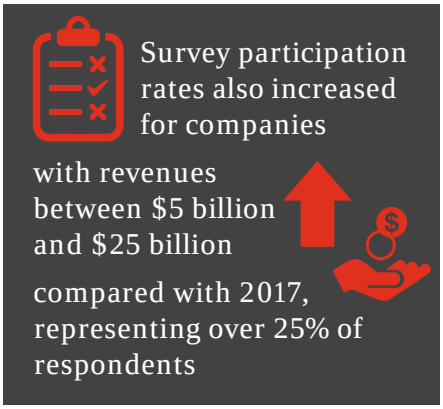
"Security concerns deter nearly half of consumers (47%) from using digital channels. It will also reduce churn and attract competitors' customers – 74% of consumers would switch their bank or insurer in the event of a data breach".[4]

Government organisations have shifted their focus to cybersecurity after recent major data breaches. This has been after a number of local breaches which highlighted potential access points through partners and also through the capture and release of potential toolsets which were originally intended as a defence and analysis tool for government agencies, but which are now in the wild, and potentially available to any threat actor for a price.

Even the bad guys are seeing commercial opportunity grow. Cybercriminals have become so successful that they have started to expand using franchise models. Ransomware, data- theft, spyware, propagation networks and other infrastructure can be purchased on the darkweb by anyone with an internet connection and crypto currencies and hidden finance make tracking transactions difficult. We are now seeing Ransomware- as-a-Service, which allows anyone with a computer and internet connection to use ransomware kits so long as they pay a fee to the original creator or seller".[5]

With recent breaches such as the estimated 143 million record Equifax breach coming to light, and their resultant loss of up to 18% of share value after the announcement of the breach,[6] people are recognising that there can be significant impacts to exposure and they need to remain up to date.

The recent Petya attacks even had major global organisations having to release sales forecast revision announcements due to breach impacts.[7]



With some estimates that up to 74% of clients are ready to switch vendor in the event of a breach, and the fact that the breach may be in a partner or service provider, means there is a higher level of scrutiny than ever before on third party cyber capability.

It is becoming harder for smaller organisations to engage with big business without having a deeper understanding of their cyber risk posture.

---

4 https://www.capgemini.com/consulting/resources/data-privacy-and-cybersecurity-in-banking-and-insurance/

5 ACSC 2017 Annual Report

6 http://fortune.com/2017/09/11/equifax-stock-cybersecurity-breach/

7 https://www.ft.com/content/ef641e2e-6214-11e7-8814-0ac7eb84e5f1

The China response

Some of the key findings of the Asia analysis from GSISS 2018 showed the following:

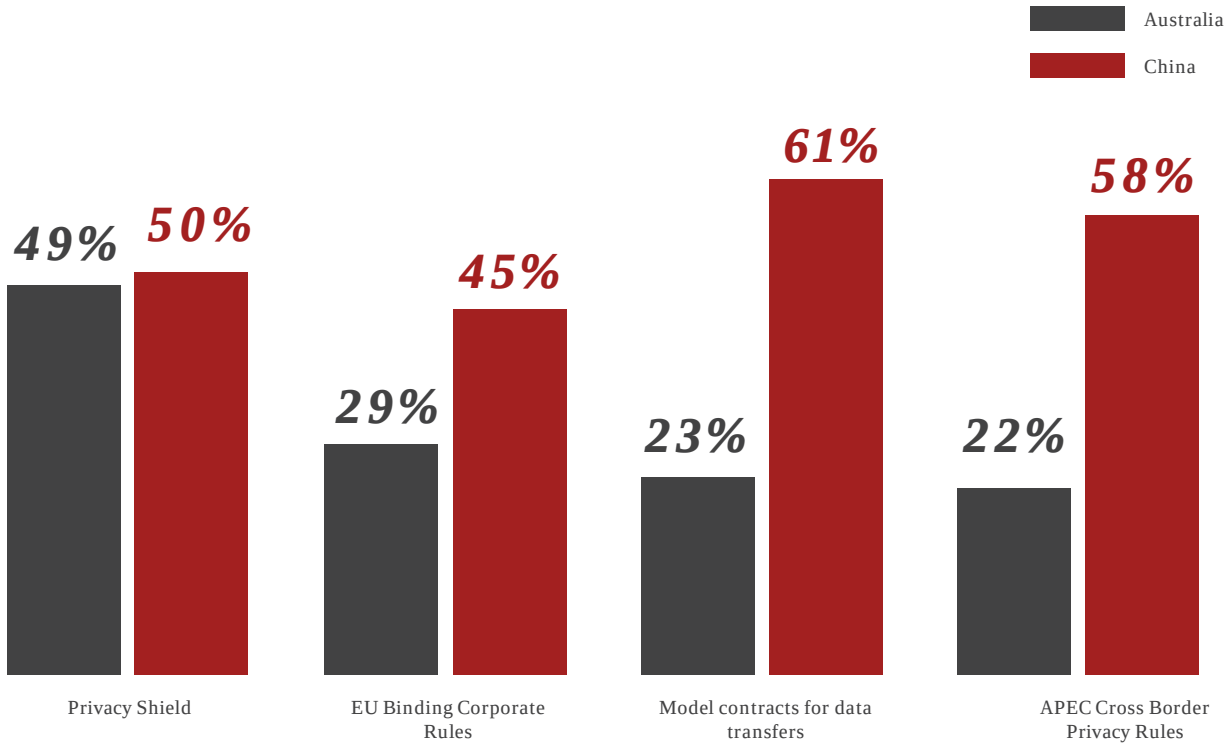
Many Chinese companies are generally outpacing their Australian counterparts in cybersecurity spending but are now starting to see the benefit of multi-year investments.

Chinese companies are spending more than their Australian equivalents to comply with new cybersecurity compliance law. This is not limited to just local Chinese cybersecurity laws (introduced in June 2017), but we also see a greater effort within China than Australia to comply with new international requirements such as the EU based General Data Protection Regulation (GDPR) which comes into effect on 25 May 2018 and the APEC Cross-border Privacy Enforcement Arrangement (CPEA).

President Xi Jinping said accelerated development of China's cybersecurity systems was needed to protect key information infrastructure and to "strengthen cyber defence and deterrence capabilities". China's new five-year plan, passed in March, devotes much attention to the development of the internet sector and cybersecurity, including cyber defences.[8]

As the GSISS findings reflect, The WEF 2017 Global Risks Report similarly found that "cyberattacks, software glitches, and other factors could spark systemic failures that cascade across networks and affect society in unanticipated ways".[9]

Approaches to Cross Border Data Flow



---

[8] South China Morning Post, www.scmp.com/news/china/policies-politics/article/1937224/china-will-boost-cyber-deterrence-powers-vows-president.

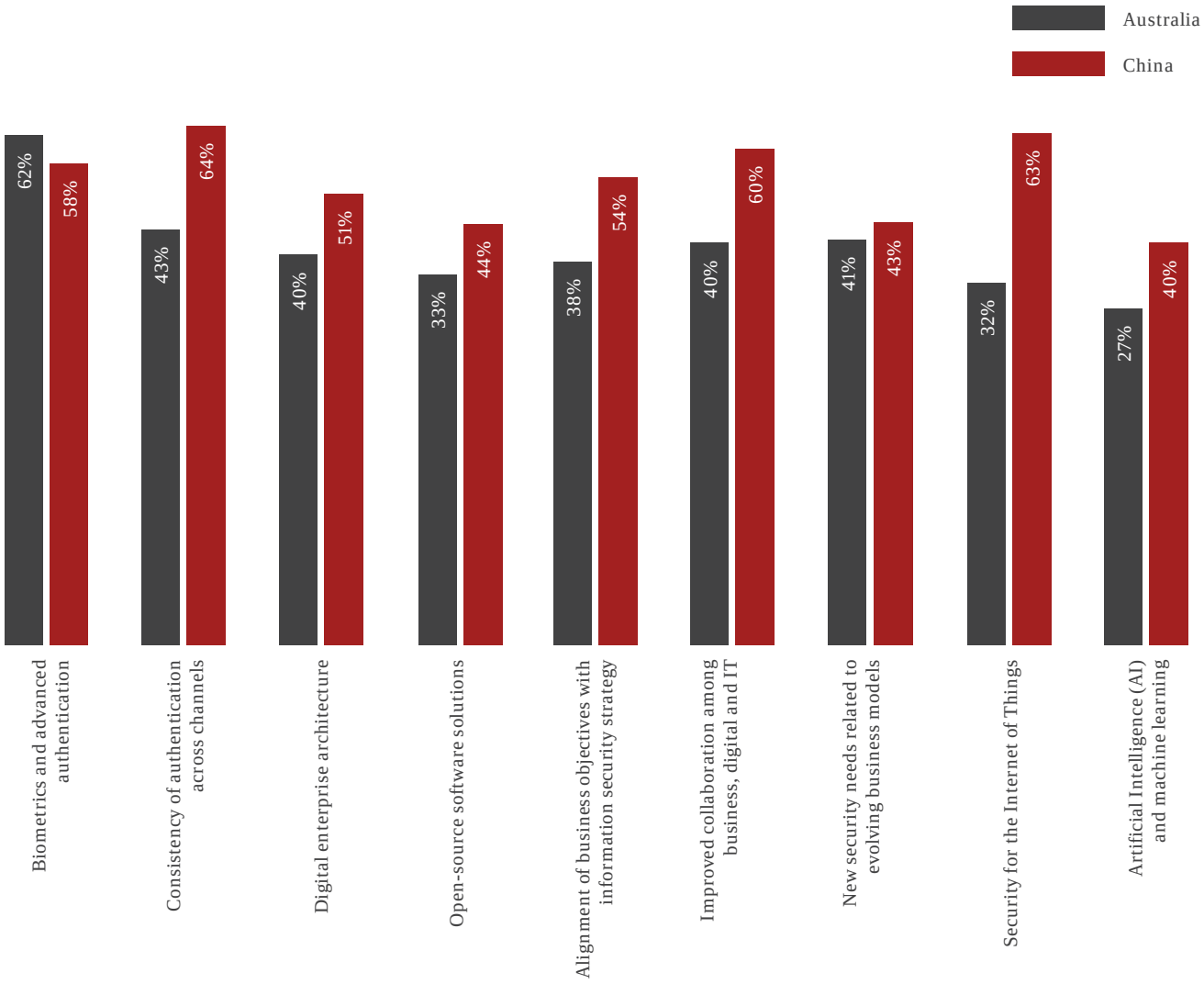
[9] World Economic Forum, 2017 Global Risks Report, January 2017

China's new cybersecurity law covers topics ranging from privacy of personal information to security standards. The laws focus on protecting personal information and individual privacy, and streamlines the collection and usage of personal information. All local companies will now be required to manage data protection measures, with a law defining how to manage sensitive data. It also defines that information on Chinese citizens or data relating to national security must be stored within China.

In Australia, the Notifiable Data Breaches scheme came into effect on 22 February 2018. A notifiable data breach is one that is likely to result in serious harm to any of the individuals to whom the information relates. A data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure. This will clearly affect Australian businesses and also foreign organisations with a local presence.[10]

To date China has been less inclined to invest in Cloud based infrastructure but does have more Operations and IT services cloud based than their Australian counterparts. Many China based responses saw an increase in plans to invest here, with significant investments in Marketing and Sales and HR information being cloud based.

Investment plans in current year



10 https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

The NDB scheme applies to agencies and organisations that the Privacy Act requires to take steps to secure certain categories of personal information. This includes Australian Government agencies, businesses and not-for-profit organisations with an annual turnover of $3 million or more, credit reporting bodies, health service providers, and TFN recipients, among others.

Conclusion

In summary, we are seeing a local alignment with the global findings of the The Global State of Information Security Survey 2018;

- The growth in digital devices is driving risk management
- Business leaders see new risks tied to emerging technologies
- Cyber threats to the integrity of data are a rising concern
- Current employees remain the top source of security incidents

As expected with varying levels of maturity and complexity within the region, there are some differences seen in the manner that these traits are identified within each market.

Particularly within Australia we are seeing;

Increased growth in technology and technology reliance, especially where these are deployed in the 'The Cloud' or under a managed service means that a greater level of understanding of risk and exposure is needed across all businesses.

More mobile devices are taking access points and vulnerability outside business control, so again risk needs to be understood and managed.

The benefits of emerging OT and IoT needs to be balanced against the return and the associated risk. Similarly, there are now areas of concern with connectivity that make things from fridges to pacemakers and even planes, trains and automobiles now being seen as cyber targets. New ways of managing and securing these environments is critical to the safety of individuals and societies.

Cyber threats are still being taken seriously and are of major concern at all levels of the business. We are seeing more attacks, and some are delivering greater impact, so the focus on awareness, detection, resolution and protection remains high.

Changes to Global regulations and compliance mean that to remain competitive, and to retain partnerships and foster growth, alignment across domains is critical, and knowing where and what data organisations have is becoming more critical.

All the while, there is still the human element of risk that threatens all security, both internal within an organisation as well as external, as it is generally human error that has lead to some of the most recent high-profile breaches.

PwC Contacts

Steve Ingram
Partner, Asia-Pacific
Cyber Lead
steve.ingram@pwc.com
+61 3 8603 3676

Rob Martin
Partner
robert.w.martin@pwc.com
+61 2 8266 5261

Andrew Gordon
Partner
andrew.n.gordon@pwc.com
+61 3 8603 2a757

Michael Cerny
Partner
michael.cerny@pwc.com
+61 3 8603 6866

Richard Bergman
Partner
richard.bergman@pwc.com
+61 2 8266 0053

Thomas Sonderegger
Partner
thomas.sonderegger@pwc.com
+61 3 8603 2548

Megan Haas
Partner
megan.haas@pwc.com
+61 3 8603 6522

Jason Knott
Partner
jason.knott@pwc.com
+61 8 9238 3418

Robert Di Pietro
Partner
robert.di.pietro@pwc.com
+61 3 8603 2391

Rob Parker
Partner
rob.parker@pwc.com
+61 2 6271 3484

Join the conversation around 'Building Transparent Businesses' at **www.pwc.com.au/btbnetwork**