www.pwc.com.au/gsiss-2017

Discovering the potential of security: A look at threat management

The Global State of Information Security® Survey 2017: The Australian story

pwc

This year's Global State of Information Security® Survey findings explore how organisations around the world are proactively negotiating the increasingly dynamic cybersecurity and privacy landscape. More than 10,000 business and IT executives told us what they are doing – and plan to do in the future – to protect digital assets and create business advantages.

Table of contents

Organisations are adopting innovative cybersecurity and privacy safeguards to manage threats and achieve competitive advantages. To do so, they are thinking more broadly about cybersecurity and privacy as both protectors and enablers for the business, third-party partners and customers.

Threat intelligence has quickly become a talking point across industries. But have Australian companies kept up with the rest of the globe? Do they trust their competitors to collaborate and share threat intelligence? This article on 'threat management' is the first in a series of short perspectives looking at the cybersecurity trends and implications specifically for Australian organisations.

"We understand cybersecurity is not a technology issue – it is about people, it is about information and it is about coordination. In Australia, we need to increase the cybersecurity awareness in both the public and private sector with the view to establishing a layered approach for sharing information among different industries."

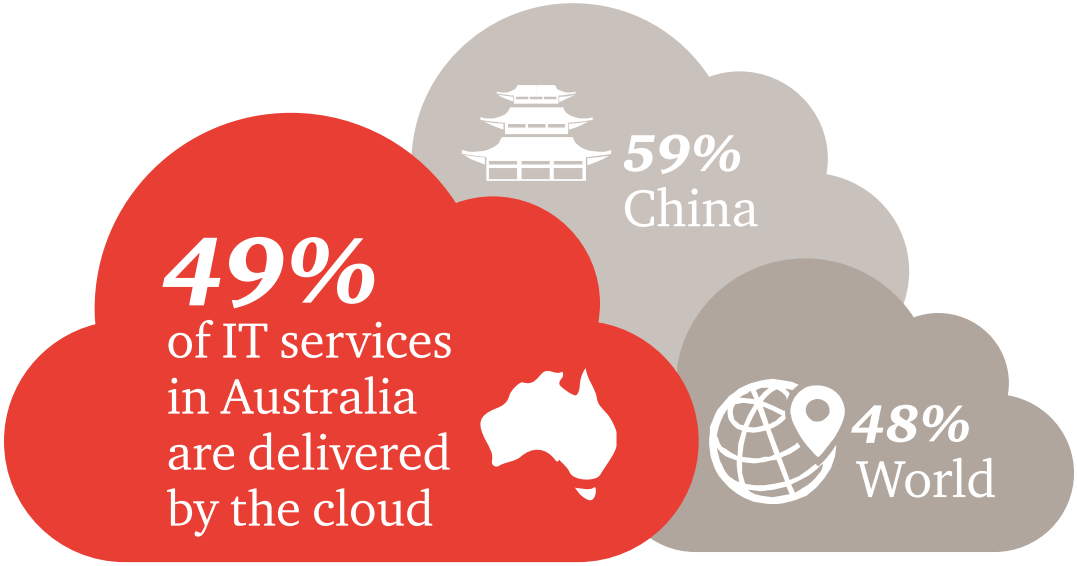
Steve Ingram
Asia-Pacific Cyber Lead

Organisations are increasingly leveraging the power within the cloud as security teams are starting to trust the cloud to host their data to benefit from the near limitless processing power as well as new technologies such as artificial intelligence (AI) and machine learning. As these new technologies provide benefits to organisations they can also increase risks meaning that cybersecurity is still a balancing act between providing the latest technologies that enable the business while protecting it from the new risks that come with these technologies.

Bold new combinations in the cloud

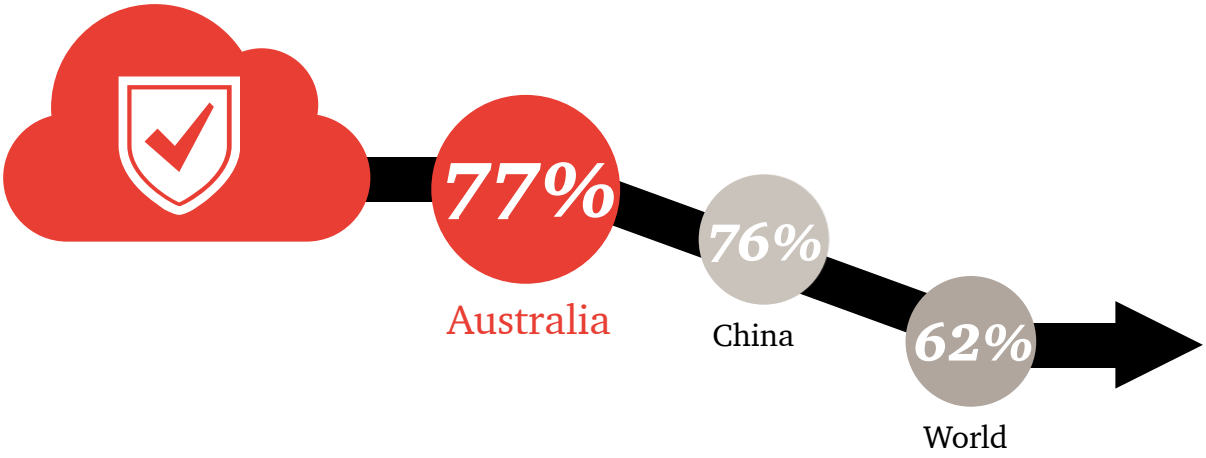
The power and interoperability of a centralised cloud platform enables organisations to synthesise a range of synergistic threat management technologies. The fusion of advanced technologies with cloud architectures can help organisations more quickly identify and respond to threats, better understand customers and the business ecosystem and, ultimately, reduce costs.

This year, 49 per cent of respondents from Australia said that they use IT services via cloud as it has flexible costs, improved mobility and less environmental impact. This was 1 per cent higher than the rest of world but 7 per cent lower than respondents from Asia.



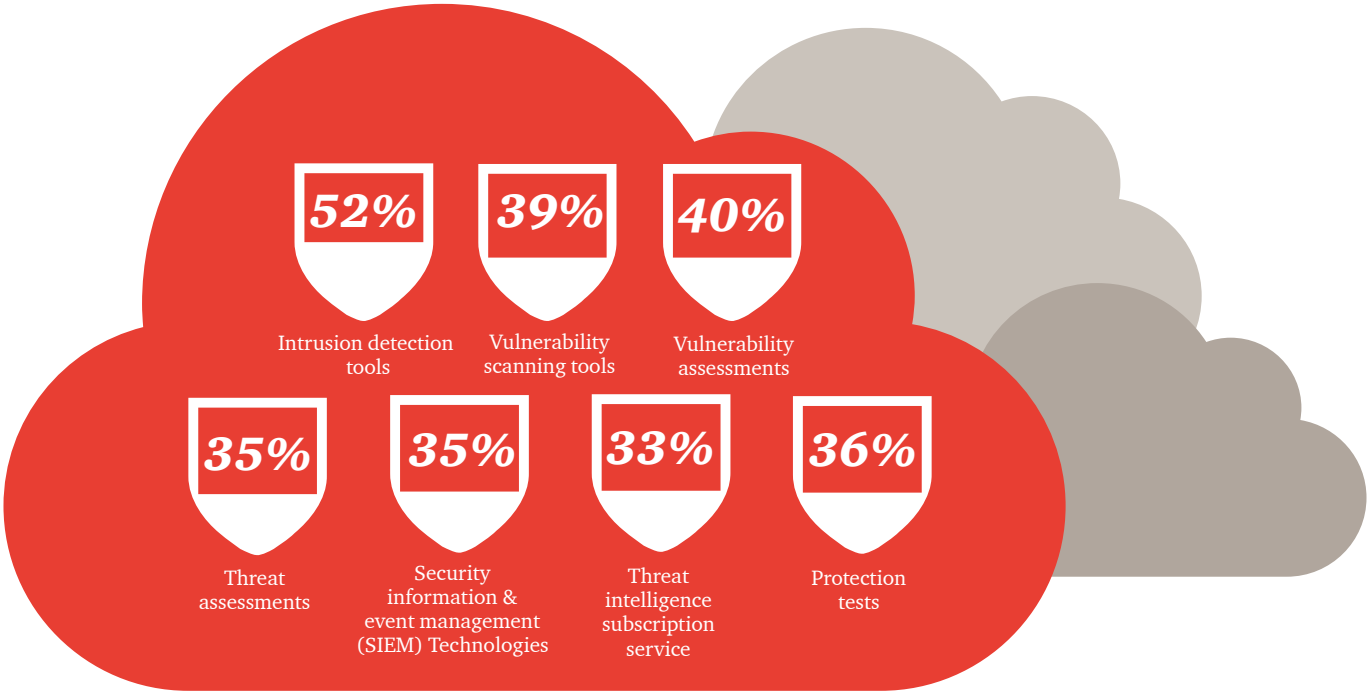
Integrating key threat management tools in the cloud

Many organisations are adopting or updating key technologies that are essential to gathering and analysing threat intelligence.



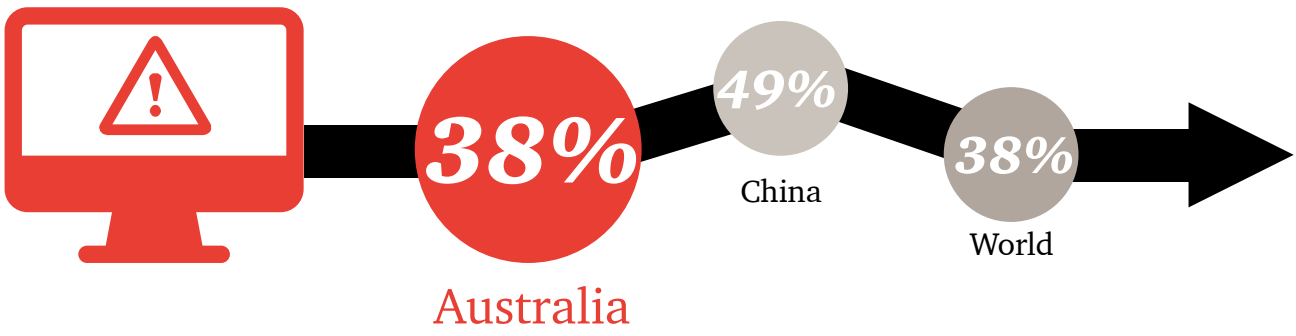
Overall, 62 per cent of respondents use managed security services for initiatives like authentication, identity and access management, real-time monitoring and analytics, and threat intelligence. In this instance, the use of managed security services in Australia (and also China) was far higher than the global average. 77 per cent of Australian respondents believe that integrating threat management services in the cloud will help them to bring all their hardware into a single platform and simplify network security architecture by reducing data centre footprints.

Threat detection tools and processes in place, 2016



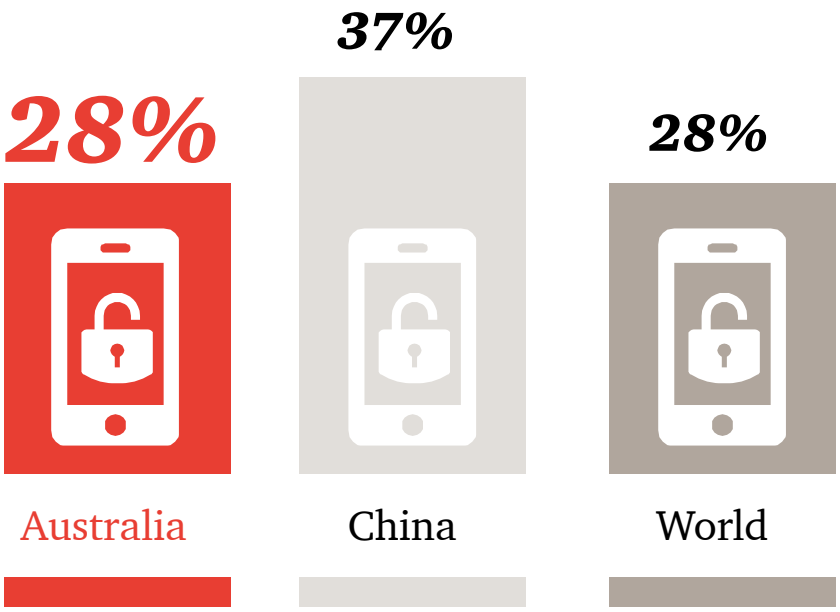
Advanced authentication to catch phishers

Over the past year, phishing has emerged as a significant risk to businesses of all sizes and across all industries. Cybercriminals have become adept at using phishing schemes to obtain user credentials and then gain access to information systems and data. This year, 38 per cent of survey respondents reported detection of phishing attacks, making it the top vector of cybersecurity incidents. Respondents from Australia aligned with the global result. However, China and Asia as a whole are reporting a higher percentage of attacks detected.



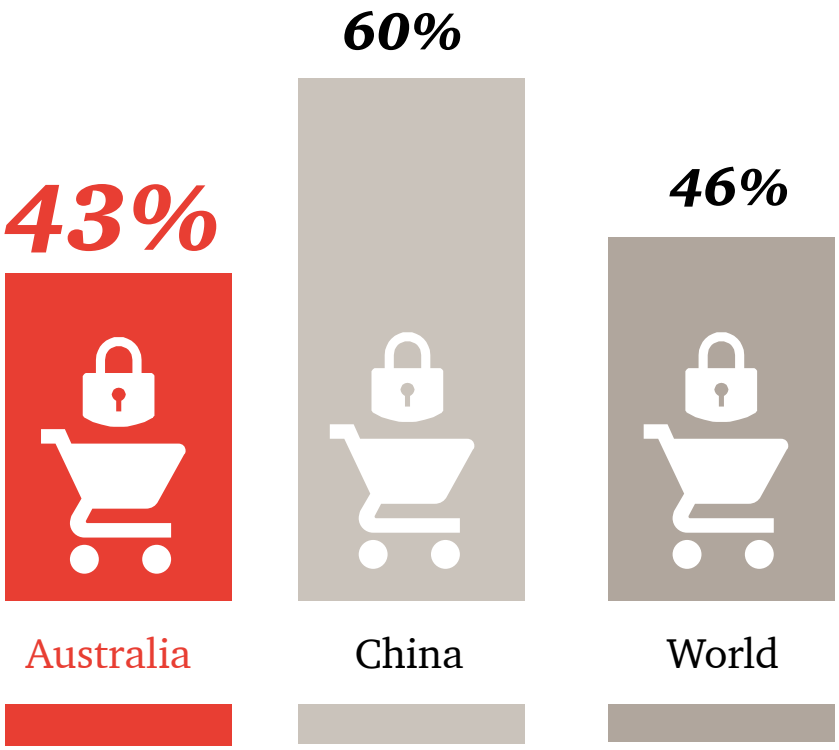
However, for the coming year, survey respondents say their number one spending priority for authentication is smartphone tokens. This year, 28 per cent of survey respondents reported security compromises of mobile devices, and securing those devices is clearly top of mind. The percentage of respondents in Australia and globally reporting mobile phone security compromises was relatively low (28%) compared to China (37%) and Asia (35%).

Percentage of respondents reporting mobile phone security compromises



Almost half (46%) of organisations that employ advanced authentication say the technology has made online transactions more secure, according to this year's survey results. Interestingly, Australian respondents reported the lowest adoption rate (43%), well below China (60%) and Asia (51%).

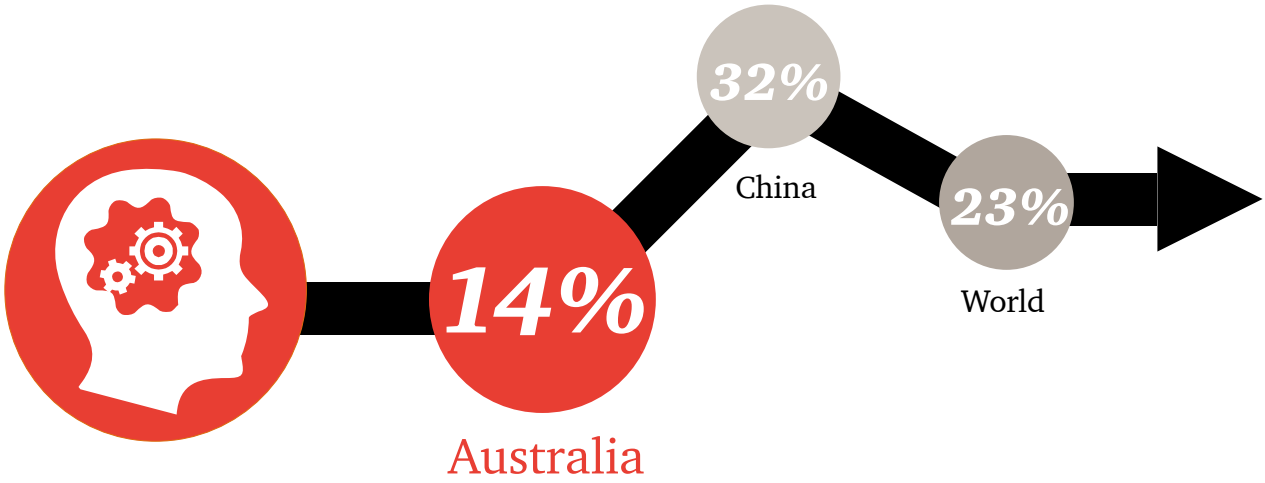
Adoption of advanced authentication for online transactions



The use of alternatives to password authentication (e.g. multifactor authentication, biometrics) will require organisations to rethink their approach to identity and access management (IAM) and calibrate the level of authentication to the security risk. Among organisations that use managed security services, 60 per cent say they have outsourced their IAM programs to service providers. In the most recent survey, Australia stands out as the lowest (42%) user of managed security services for IAM, compared to China (73%) and Asia (64%).

Truly forward-thinking businesses are beginning to combine adaptive authentication techniques with artificial intelligence (AI) and machine learning to build predictive authentication mechanisms. The use of predictive variables can make authentication a continuous event tied to the risk associated with the specific access attempts.

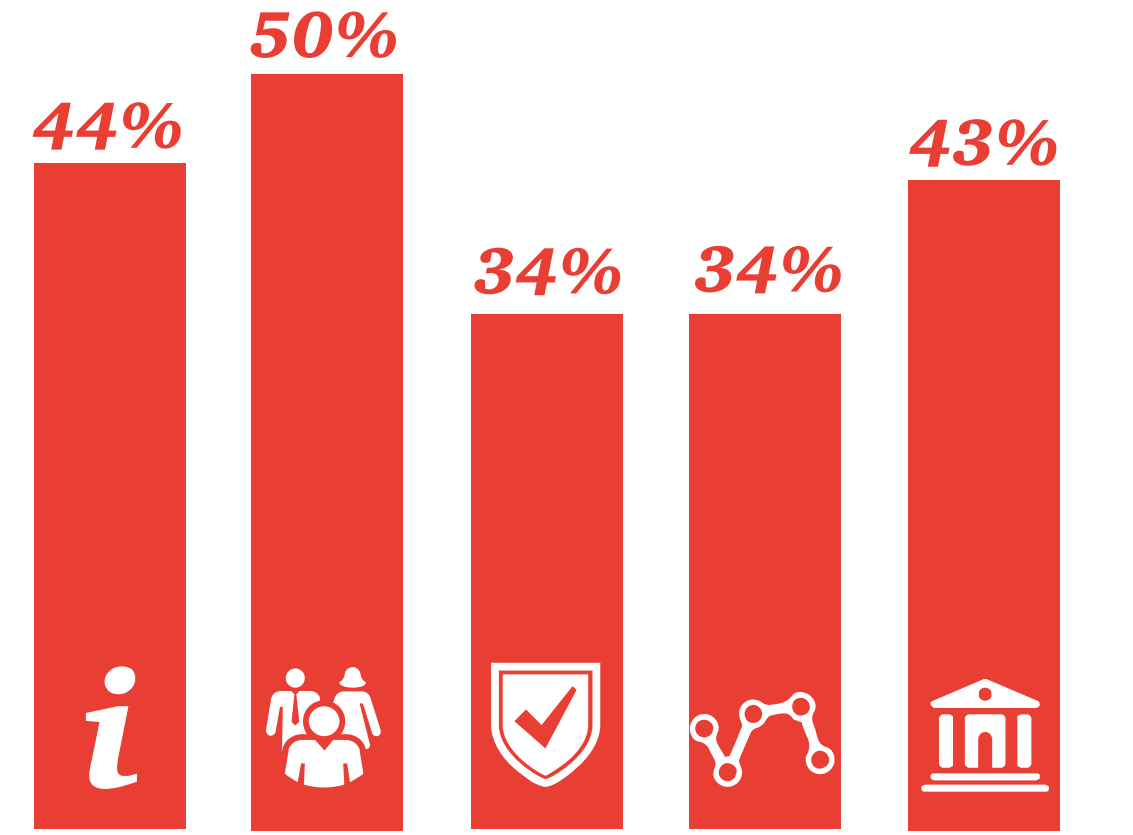
Percentage of organisations combining adaptive authentication techniques with AI



Collaboration with others

The survey results showed a slight dip for Australian companies compared to the previous year when it comes to the use of threat intelligence and sharing of information. This year's feedback confirms that Australia is behind on the use of threat intelligence and the sharing of indicators of compromise compared to Asia, China and the world average. Continuous awareness will help users to determine the benefits of sharing threat intelligence. By doing so, organisations can expand their visibility and insight into potential and active threats. Even though the use of threat intelligence and sharing of data in Australia is behind the global trend, PwC has seen that when collaboration between organisations does happen it is an effective defence against industry-wide attacks.

Australian collaboration with others



Collaboration is key to tackling cybercrime in Australia

The future growth of Australia's economy depends on consumer and business trust in our nation's digital systems and infrastructure to keep our information safe.

As our adversaries are working together to break our defences, the only effective response is a collaborative solution where both the public and private sector join forces to combat these cyber threats.

What impact has collaboration with others had on your organisation's security program?

20% detect more ***security*** incidents

27% receive more ***timely*** threat ***alerts***

13% ***improve*** regulatory compliance

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

PwC Contacts

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

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

Andrew Gordon
Partner
andrew.gordon@pwc.com
+61 3 8603 2757

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

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

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

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

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

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

Explore the Global State of Information Security® Survey 2017: The Australian Story findings at **pwc.com.au/gsiss-2017**

127047855