TELSTRA CYBER SECURITY REPORT 2016

Managing risk in a digital ecosystem

IT'S HOW WE CONNECT

EXECUTIVE SUMMARY

Managing Risk In A Connected World

Connectivity and technology provide great benefits to our society and the economy today, and the full potential to touch and benefit us all is yet to be fully realised. However with this benefit comes some risk – and as more of the world embraces technology and connectivity the risk increases and organisations need to be able to manage this risk.

Successful businesses already manage complex risks today. Understanding the cyber security risk and what it actually means for the business and customers can be a challenge. In the intangible world of cyber space, where neither the assets we value, nor the threats, are visible, it can be difficult to understand how to go about minimising these risks. This challenge is compounded by a barrage of cyber security technical jargon.

The increase in connectivity and the rapid uptake in new technologies means that crime, espionage, protest and even mistakes can happen on this platform at a pace, scale and reach that is unprecedented. This makes cyber security a significant issue, one of global importance that no organisation can handle alone.

Companies need to be equally concerned with their own actions and those within their supply chain. A member of staff, a partner's staff, a partner or business unit making a mistake, or in rare cases malicious acts by an individual, can result in the loss of valuable customer or corporate information or cause disruption to networks and services.

Now more than ever, C-level executives and Boards need assurance that their organisation has taken the right steps to manage this cyber security risk, including having the right response capabilities and plan in place when needed.

This report aims to share our knowledge and insights about the cyber security risk identified by businesses in Australia and the Asia Pacific region. Some of our findings highlighted the extent of the threats, and equally the increased awareness of this important issue:

- We learned that 23.7% of Australian organisations surveyed detected a business interrupting security breach during an average month. This is more than twice as often as 2014 (10%).
- The Asia Pacific region experienced an even higher level of security incidents with 45.5%of surveyed organisations impacted by a security incident in an average month.
- We also found that organisations that attribute responsibility to C-level or business line managers and conduct frequent cyber security briefings are better positioned to handle security incidents.
- Ransomware continues to rise in Australia together with phishing emails which increased by 29% in 2015, that reinforces the need for staff training to help mitigate these threats.
- Technology adoption, in particular cloud services, continues to be a security challenge. Nearly half of Australian organisations do not track and monitor Shadow IT, leaving organisations potentially exposed to valuable data loss.
- More than half of Australian organisations also see data theft as a risk in adopting cloud services, and many reported they are not yet ready to handle this exposure.

Businesses who approach cyber security as an IT risk rather than a business risk will struggle and in many cases fail to appropriately manage the risk. Addressing this as a business risk with the right mix of people, processes and technology will mean businesses are well placed to reap the benefits of the digital world.

It is our hope that this information will improve awareness about the nature of the cyber threat and help your organisation make vital cyber security decisions that minimise the risk to your business.

Mike Burgess
Chief Information Security Officer
Telstra Corporation Limited

Craig Joyce
Director Security Practice
Telstra Corporation Limited

METHODOLOGY

Telstra's Cyber Security Report 2016 aims to assist organisations in the Asia Pacific region to better manage and mitigate their business risks by sharing our knowledge of the evolving security landscape.

The report draws on analysis of security event data gathered from Telstra managed infrastructure and trusted third party security partners. In addition, Telstra engaged a research firm to interview professionals responsible for making IT security decisions within their organisations.

The research firm's online surveys harvested more than 305 responses. 75% of these responses were from Australian businesses and the remaining 25% were from businesses in the Asia Pacific (APAC) region. All the businesses who were interviewed in the Asia Pacific region have an Australian branch office and more than 500 employees located in APAC. 71% were multi-national organisations and the remainder only have offices in Australia (29%). C-level executives including Chief Executive Officers, Chief Financial Officers, Chief Information Security Officers and Chief Security Officers accounted for 32% of respondents across Australia (33.3%) and Asia (28.6%). The remainder were in IT security managerial roles.

Just over 55.7% of respondents worked for organisations employing more than 500 Australian-based employees across Australia (53.5%) and Asia (62.4%). 80% worked for organisations with 200 or more Australian based employees across Australia (87.4%) and Asia (75.6%).

HEAD OFFICE LOCATION FOR ASIAN RESPONDENTS

20.8% – INDONESIA

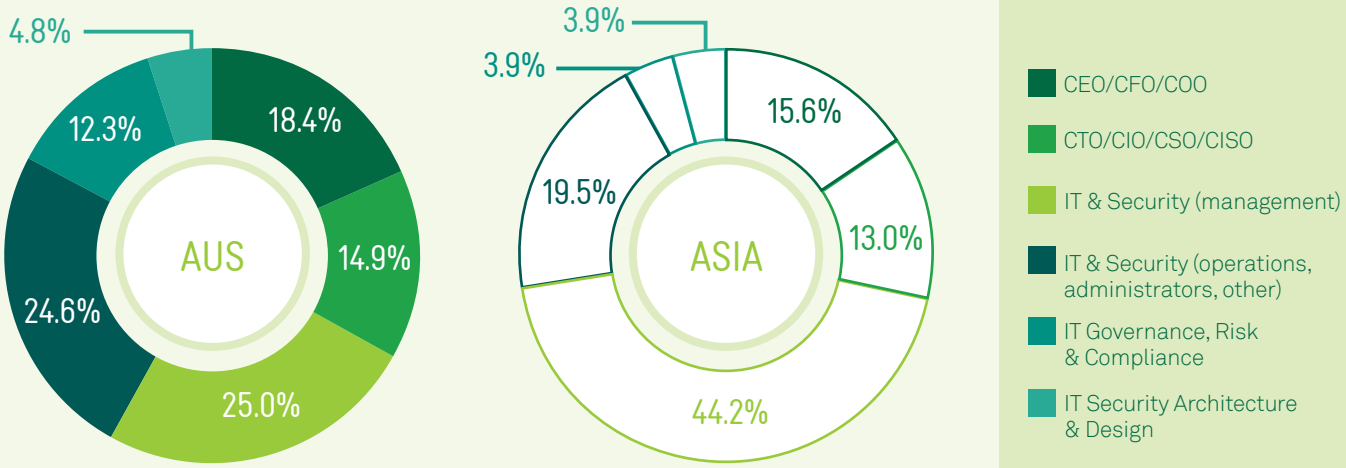
20.8% – PHILIPPINES

19.5% – SINGAPORE

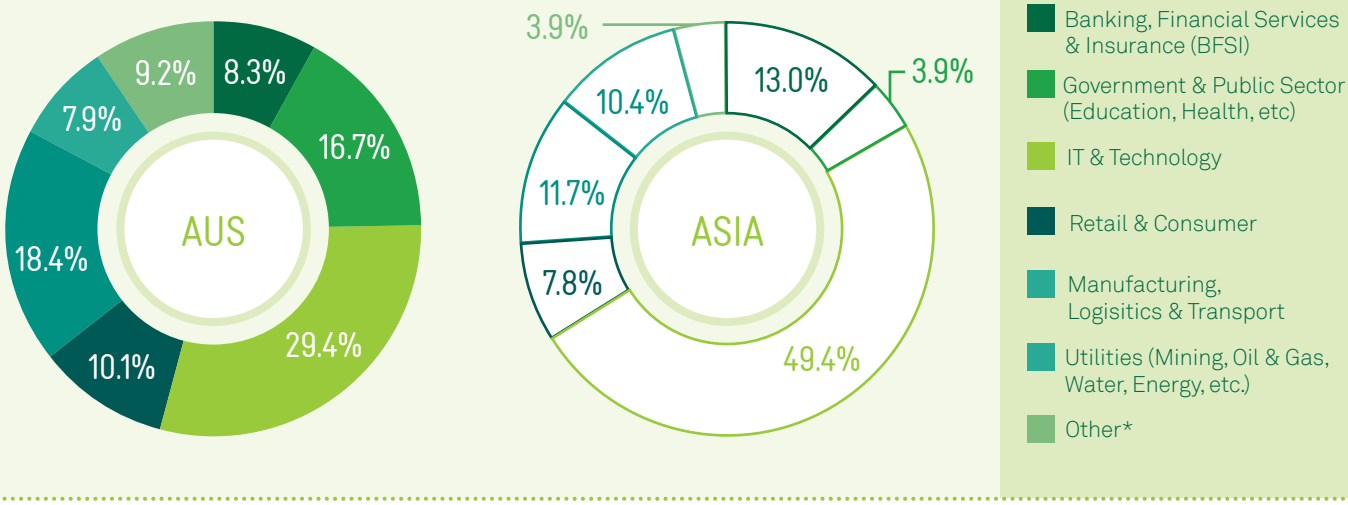
19.5% – MALAYSIA

19.5% – HONG KONG

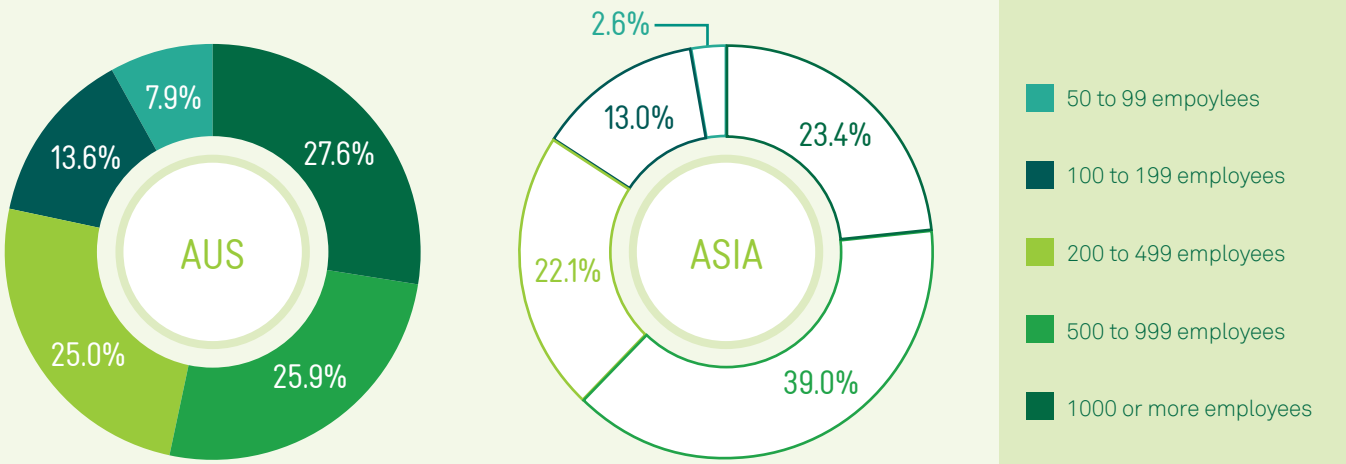
ORGANISATIONAL ROLE IN AUSTRALIAN AND ASIAN RESPONDENTS



RESPONDENTS IN AUSTRALIA AND ASIA BY INDUSTRY



SIZE OF SURVEYED ORGANISATIONS IN AUSTRALIA AND ASIA



*Others include training, construction, wholesale, professional services, media, security, construction, legal, distribution, pharmaceutical, charity, education, travel , agriculture, hospitality, non-government healthcare, engineering, energy storage.

CONTENTS

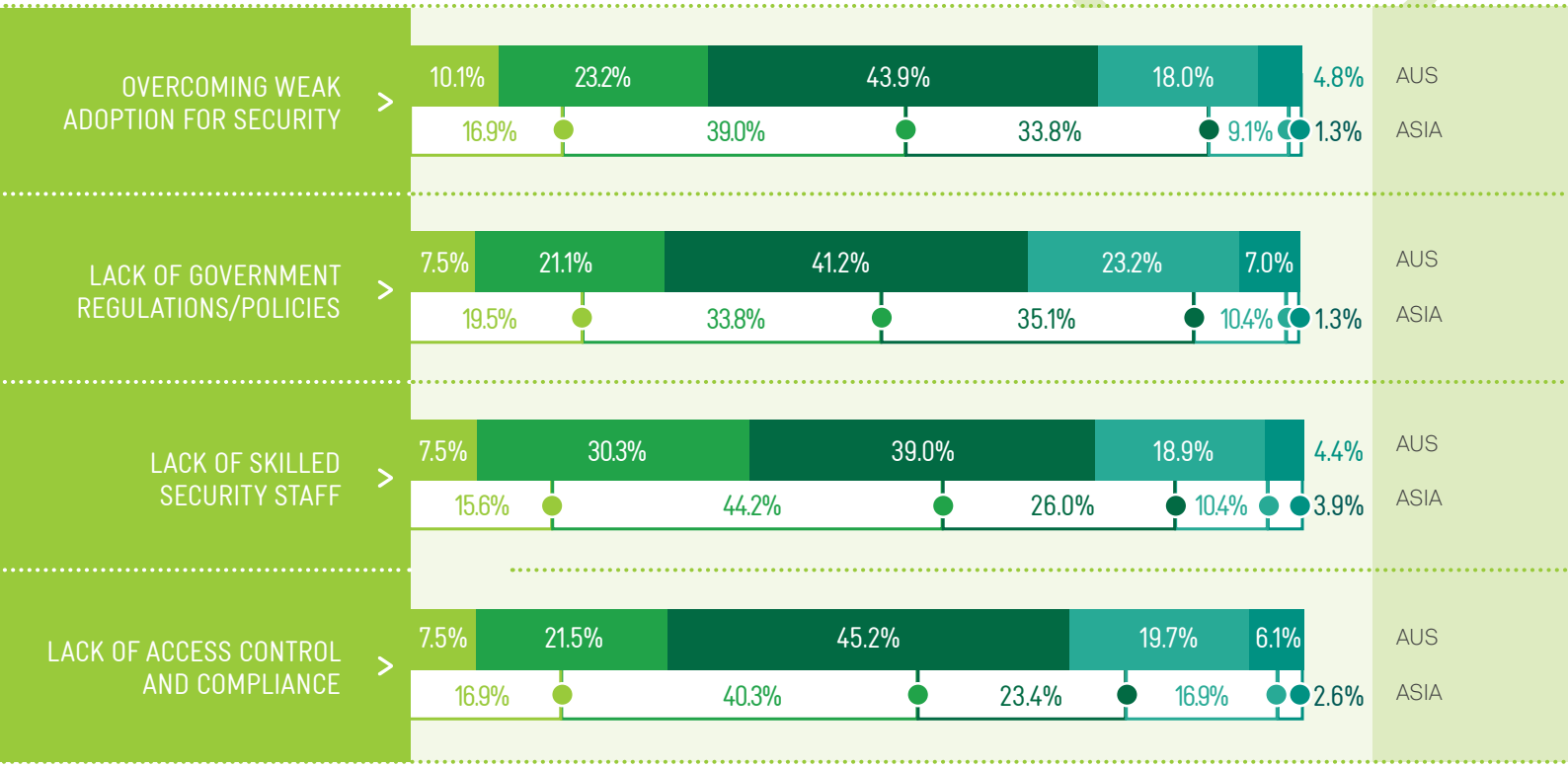
Executive Summary	03
Methodology	04
1.0 : Cyber security readiness and maturity	08
1.1 Security challenges for organisations	09
1.2 Cyber security must be a Board-level priority	10
1.3 Tackling data privacy	13
2.0 : Security threats and trends	14
2.1 Malware attacks reign	14
2.2 Defending against the APT insurgence	16
2.3 Ransomware	17
2.4 Email and phishing attacks	18
2.5 Web and application vulnerabilities	20
2.6 Network security threats	22
2.7 Denial of Service attacks	24
2.8 Cloud adoption	26
2.9 Cloud security and shadow IT	28
2.10 Mobility threats	32
3.0 : Security incidents and business impacts	35
3.1 Organisational readiness and maturity to handle security incidents	36
3.2 Frequency of security incidents	38
3.3 Business impacts	41
4.0 : Security drivers and investment decisions	42
4.1 Cyber security drivers	42
4.2 Investment decisions	44
4.3 Security technology investments	45
4.4 Cyber security insurance	46
5.0 : Global security challenges and approaches	48
5.1 Global security challenges for Asia-Pacific multinationals	48
5.2 Global security methodologies	50
5.3 Increasing third-party threats	52
6.0 : Summary	54
Acknowledgements	57

1.0 CYBER SECURITY READINESS AND MATURITY

Businesses that embrace digital transformation and the opportunities that come with this should also consider mitigating their potential security risks by incorporating security into all aspects of their people, processes and technology solutions. Incidents of malicious hacking, ransomware, data leaks, theft, and electronic fraud regularly make headlines because today's connected technologies make everyone a target. Governments are introducing legislation including data sovereignty provisions in some jurisdictions to regain control of their citizens' private information.

It is perhaps not surprising then that Australian organisations are starting to conduct their affairs in a manner more cognisant of data security. For instance, our security research revealed that the majority of CEO, CFOs and COOs are now briefed at least quarterly on cyber risks and mitigation strategies. As a further indication of the growing concern over data security, the majority of Australian and Asia Pacific organisations are becoming more effective at defining their security strategies and executing their security plans. Despite this, we found organisations are still being challenged in a number of areas that limits their effectiveness in executing their security plans. Notably these challenges include a shortage of skilled security resources and a lack of staff training and security awareness within their organisation.

AUSTRALIA & ASIA RATING SECURITY CHALLENGES IN THE ORGANISATION



1.1
SECURITY CHALLENGES FOR ORGANISATIONS

THE SECURITY SKILL GAP WIDENS AS SCARCITY OF SECURITY RESOURCES CONTINUES TO GROW DESPITE RECRUITMENT BUDGETS INCREASING

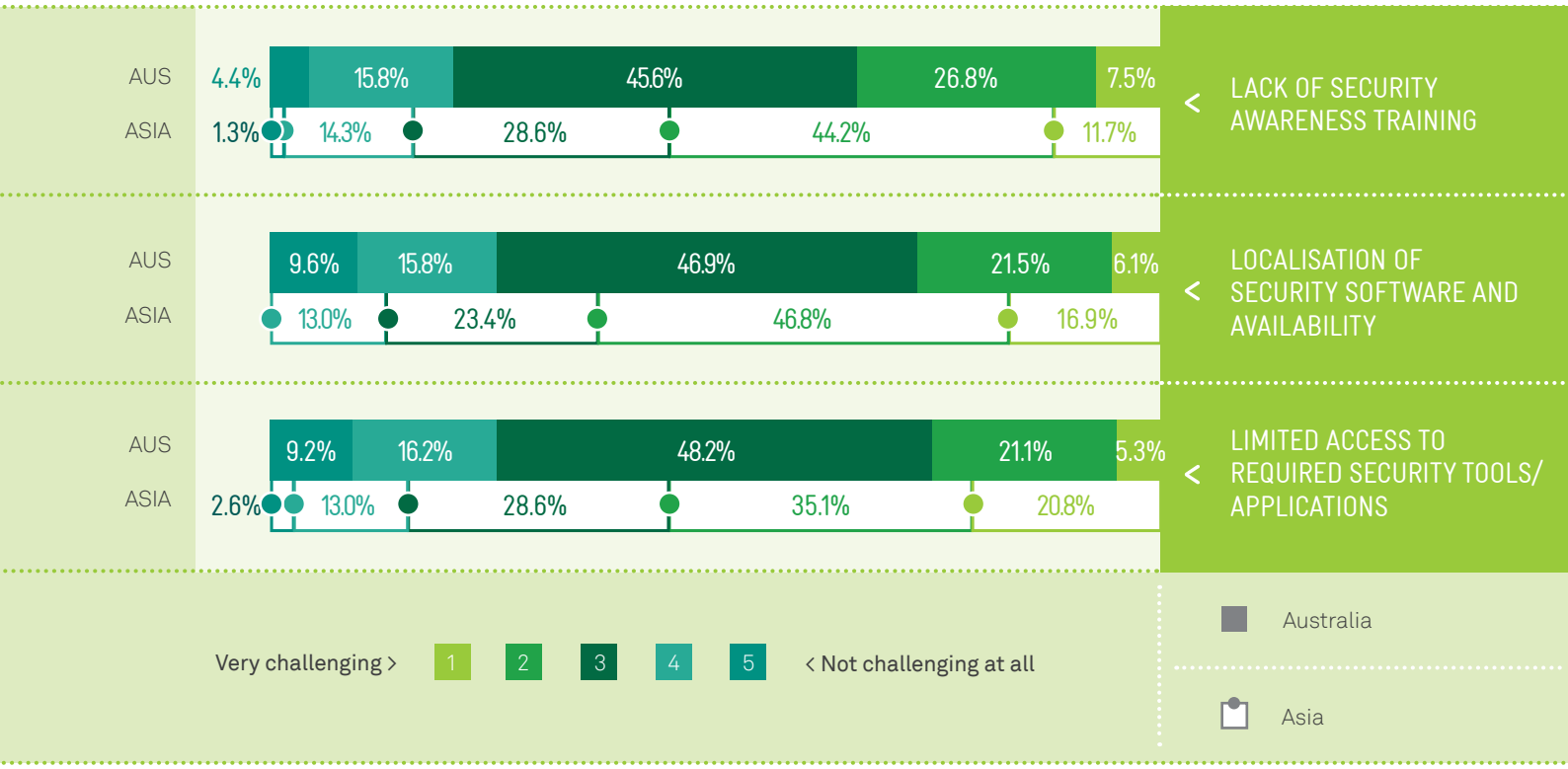
There are a host of cyber security issues that challenge most organisations. Unlike last year where the lack of budgets or funding was a major concern, this year organisations focused on issues that were further progressed within the company. The main challenges for Australian organisations concerned staffing issues such as lack of skilled staff, lack of security awareness training and weak adoption of security policies. Asian organisations tended to be more concerned with the lack of access to security tools and the lack of government regulations and policies.

This year's survey highlighted the growing shortage of skilled security staff required to perform increasingly complex security tasks as one of the major challenges for organisations. 62% of organisations stated that they have too few information security professionals to implement security activities within their organisations. Skills that entailed security risk assessments and conducting forensic investigations were among the most lacking across all verticals with an average of 54.3% organisations indicating a shortage of skills in these areas. Asian organisations lacked more than their Australian counterparts across all areas on average.

Our research reveals that the reasons for the hiring shortfall are less about funding than an insufficient pool of suitable candidates. While the sophistication of cyber-threats and a broadening landscape that requires security oversight (e.g. mobile devices, cloud-based services, and the Internet of Things) and the skills to identify, analyse, manage and prevent cyber-related attacks are becoming more demanding. Despite increased industry demand for specific ICT skills, the take-up of ICT-related tertiary courses in Australia over the last decade has halved. A 2014 analysis by the Australian Financial Review[1] of university course take-up by domestic undergraduate students since 2001 shows a 36% decline in students. While the mismatch between the needs of industry and tertiary graduate qualifications is a general one impacting the whole of the ICT industry, it particularly affects dynamic and rapidly changing areas of technologies which is specifically relevant for cyber security.

More broadly, building the pipeline of ICT graduates, in fact Science, Technology, Engineering and Mathematics (STEM) graduates generally, to meet the future demand for security professionals is going to be essential. A number of bodies have recently taken action to address these security resource demands, including the Australian Department of Defence in conjunction with the University of NSW[2] and the University of Oxford's first international expansion of their Cyber Security Centre in Melbourne[3].

The skills shortage has seen organisations move towards outsourcing security resources to security providers, predominantly driven by the staffing and skills overheads of the in-house approach (recruitment and training costs).



[1]The Financial Review, Shortage of IT graduates a critical threat, 7 Feb 2014, http://www.afr.com/news/policy/industrialrelations/shortage-of-it-graduates-a-critical-threat-20140206-iy4lx
[2]http://www.governmentnews.com.au/2014/06/defence-opens-new-cyber-security-school-unsw-canberra/
[3]http://www.computerworld.com.au/article/590804/vic-govt-lures-oxford-university-security-centre-melbourne/

1.2
CYBER SECURITY MUST BE A BOARD-LEVEL PRIORITY

CYBER SECURITY IS A BUSINESS IMPERATIVE THAT REQUIRES EXECUTIVE AND BOARD LEVEL ONGOING INVOLVEMENT

Executives across every business sector are increasingly concerned about cyber security and new governmental laws and regulations are placing even more focus on organisations having the right cyber security controls in place. Not only do customers expect that their personal and financial information will be protected from unauthorised disclosure and use, so are shareholders and potential investors increasing their demands that effective controls are put in place to protect sensitive information to avoid liabilities and litigation.

Recent high-profile cyber attacks and media coverage of data breaches and security incidents have raised the awareness of executives. Executives are increasingly aware of the importance of their customer data and corporate information and the reasons for them to be protected. These continue to be the top two data types that are most likely to be compromised in a breach.

While many Australian organisations have indicated greater engagement with senior executives, only 36% of respondents had an effective information security strategy in place. The figure was much higher for Asian organisations at 60%.

Cyber security is as much about technology as it is about managing risk, and we have seen this with roles and responsibilities of cyber security executives expanding in recent years. Today's Chief Information Security Officers (CISOs) take on a multidisciplinary approach – they not only need to have expertise in security but also in corporate governance and in risk management while trying to maintain overall business objectives.

Our research has also found that board members have also become more involved in a wide range of activities. This year we saw an increase in board participation in most aspects of information security and who took part in the responsibility for the organisation's cyber security program. However, at below 20%, this is still below global average numbers at around 35%. The survey suggested that the BFSI industry had the most even spread of responsibility across their respective organisations. In Asia, business line managers and the traditional IT department still have the majority share of responsibility for cyber security within their organisations, which is an area for improvement.

One area for improvement we found was that many senior executives express frustration in understanding cyber security and integrating it into their management processes. Many cyber security measures rely on complex technical controls and many senior executives feel uncomfortable in understanding the security technology that supports the business. It is apparent that language gaps create barriers that sometimes produce organisational friction, lack of communication, and poor decision-making.

> CONSIDERATIONS

Implement regular briefing sessions with Board members and senior management on the potential security risks and ensure that you articulate the business impacts of these risks

Ensure that your IT department learns to speak the right language when communicating security issues to C-level executives and Board members

Ensure that you have a comprehensive security strategy and plan in place to mitigate these risks which is endorsed by Board members and senior management

Your security strategy and plan must include people and process aspects for potential risks as well as the technology and network changes that may be required.

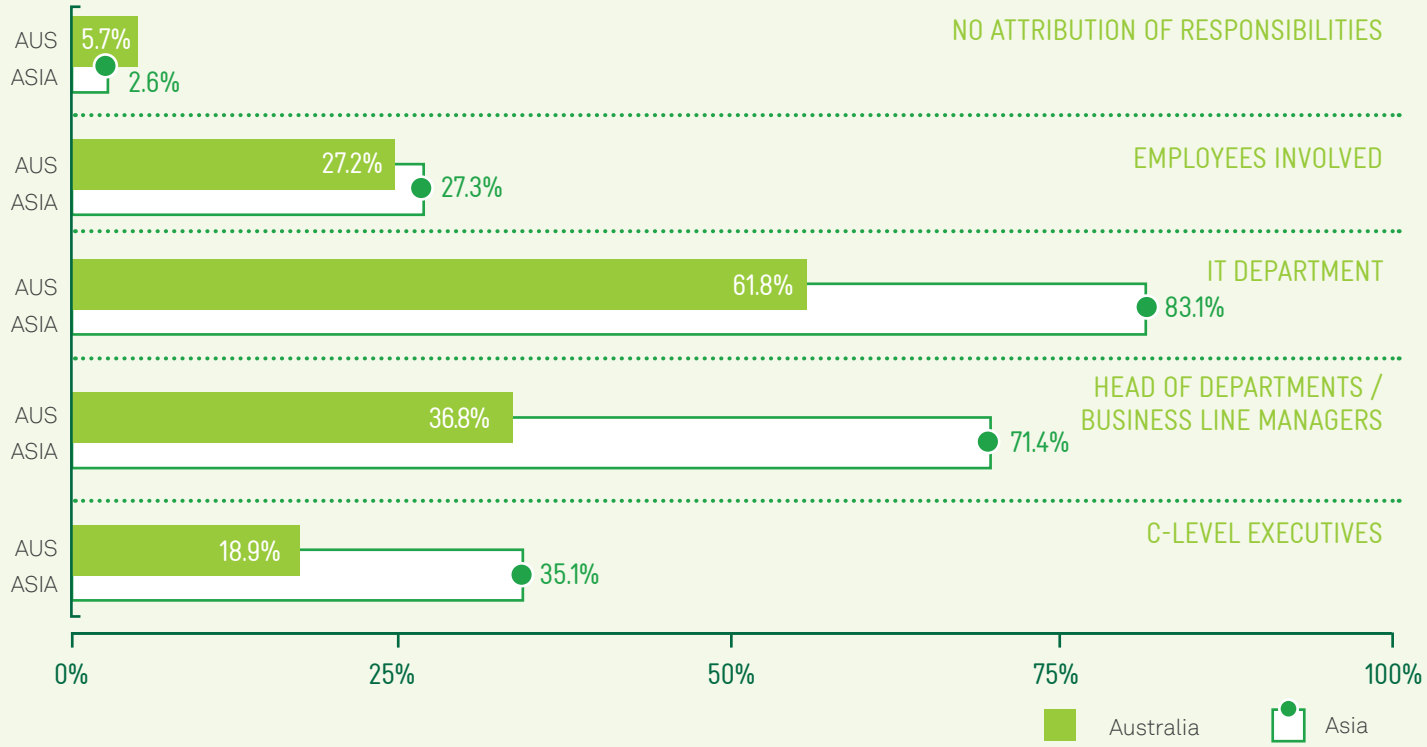
Establish a cyber security program if you haven't got one in place already and ensure the Board and management know that it's a full-time activity, not a single initiative

Ensure you position cyber security initiatives reflective of the business function it supports or enables

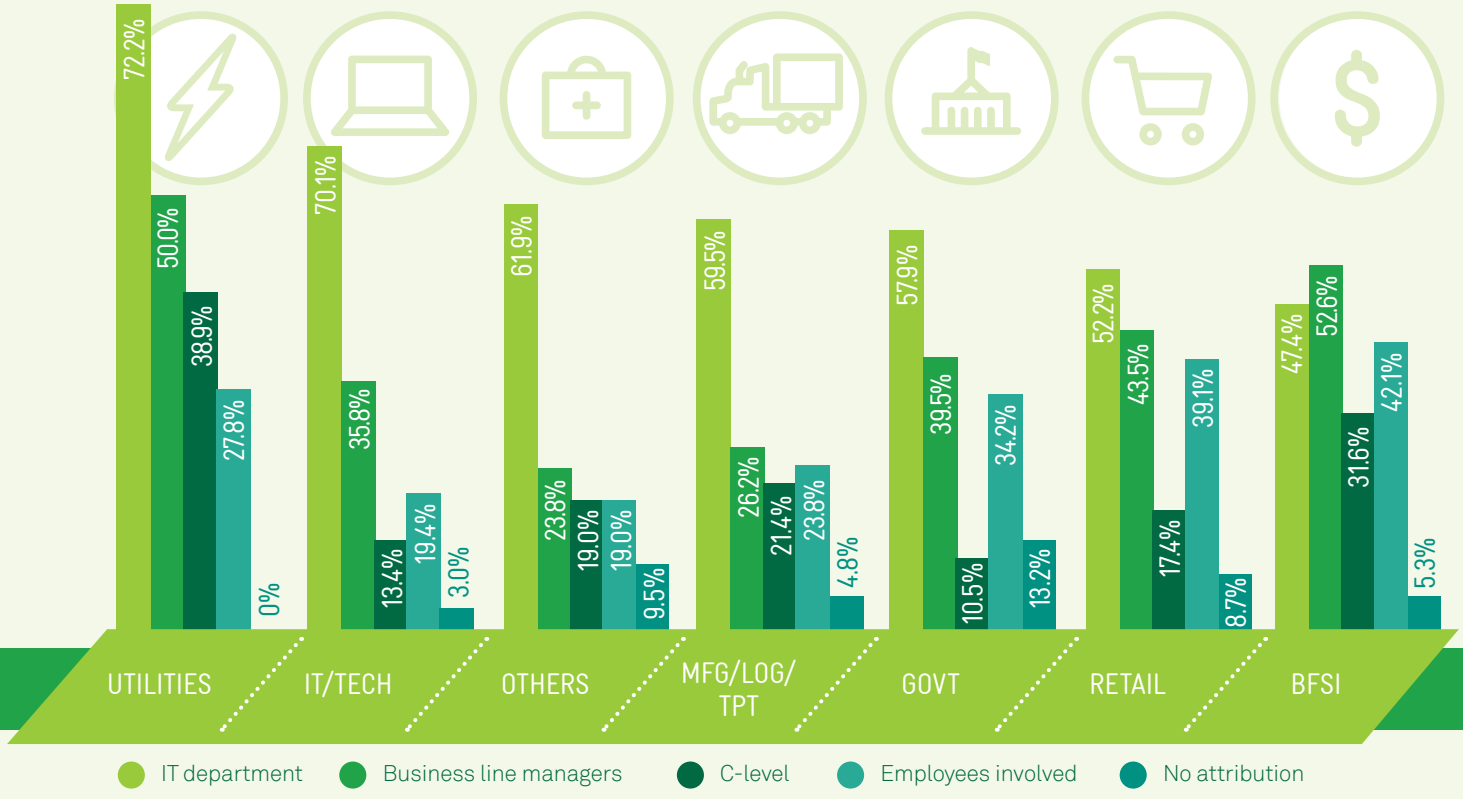
Put in place metrics that executive members can easily track how well the organisation is performing

Identify the gaps and investment required with reference to organisational risk, so that management can decide on the level of risk warranted for the business

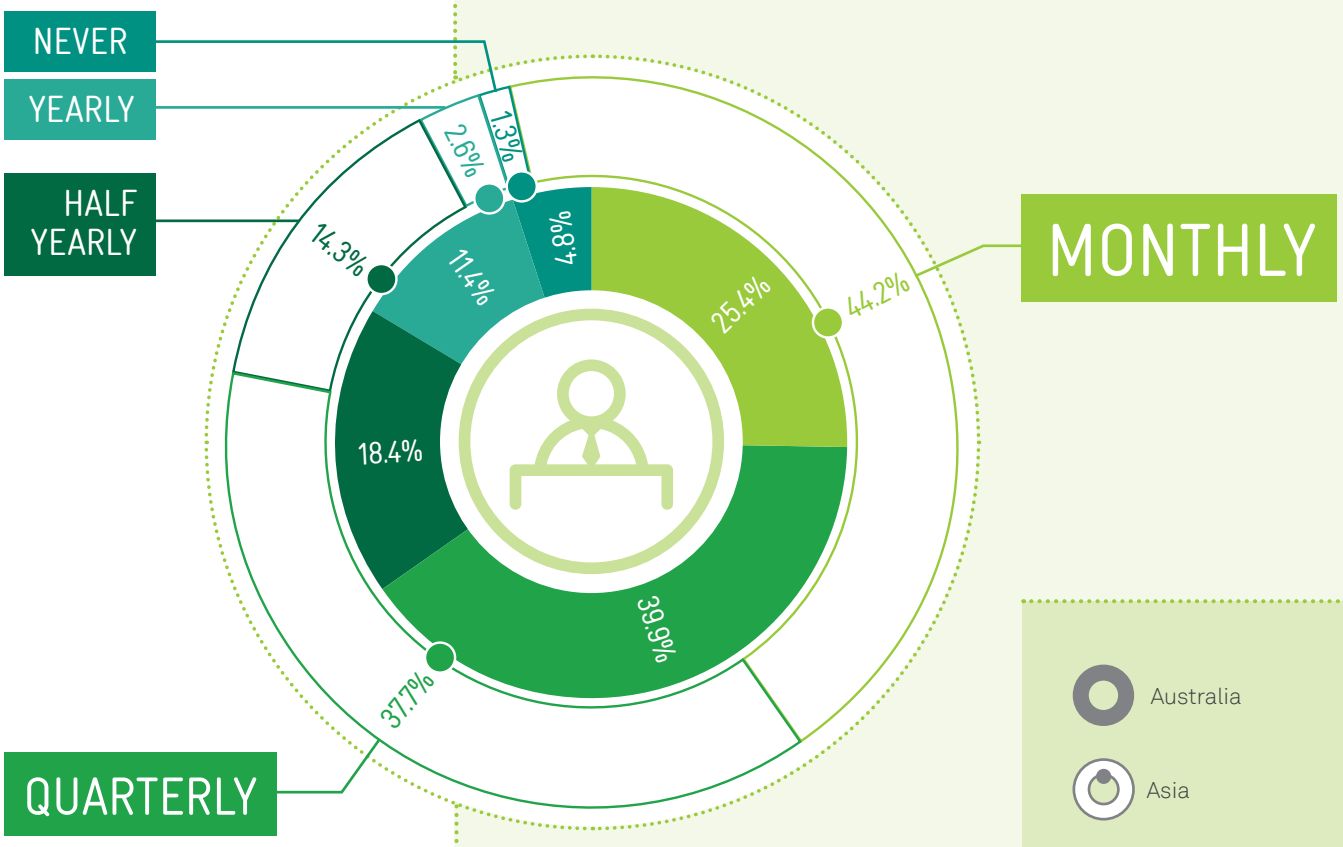
AUSTRALIA & ASIA
WHO IS RESPONSIBLE FOR YOUR CYBER SECURITY PROGRAM WITHIN THE ORGANISATION?



AUSTRALIA
WHO IS RESPONSIBLE FOR SECURITY MANAGEMENT WITHIN THE ORGANISATION



AUSTRALIA & ASIA
FREQUENCY OF CYBER RISK, MITIGATION AND STRATEGY BRIEFINGS TO BOARDS



> ADDITIONAL FINDINGS

Asian enterprises conduct more frequent security briefings to senior management compared with Australian enterprises

44.2% of Asian enterprises conduct security briefings on a monthly basis compared with only 25.4% for Australian enterprises

75% of Indonesian enterprises, followed by 53% of Malaysian and Philippines enterprises run monthly briefings

Most Singapore and Hong Kong enterprises hold briefings quarterly

The frequency of briefings is highest in the Government and BFSI verticals in Australia

The biggest concern is that nearly 5% of Australian organisations and over 1% of Asian organisations never hold regular security briefing sessions with senior management

19% of the Others industry vertical never hold security briefing sessions

1.3
TACKLING DATA PRIVACY

The pace of innovation has caused consumers, consumer watchdog groups and legislators to be increasingly concerned about the type and amount of data being collected and particularly whether organisations have the right security safeguards in place to protect the privacy of consumers. The Australian Government commissioned a review into the state of Australia's privacy laws in 2008 and produced a report titled 'For Your Information: Australian Privacy Law and Practice'[4], where it recommended significant changes be made to the Privacy Act, as well as the introduction of a statutory cause of action for breach of privacy.

On 12 March 2014, new legislation was introduced by the Australian Commonwealth regulation under the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) which requires an organisation dealing with an individual's personal information to ensure appropriate security measures are taken to protect their data. Penalties of up to $1.8 million may be imposed on an organisation that seriously or repeatedly interferes with an individual's privacy.

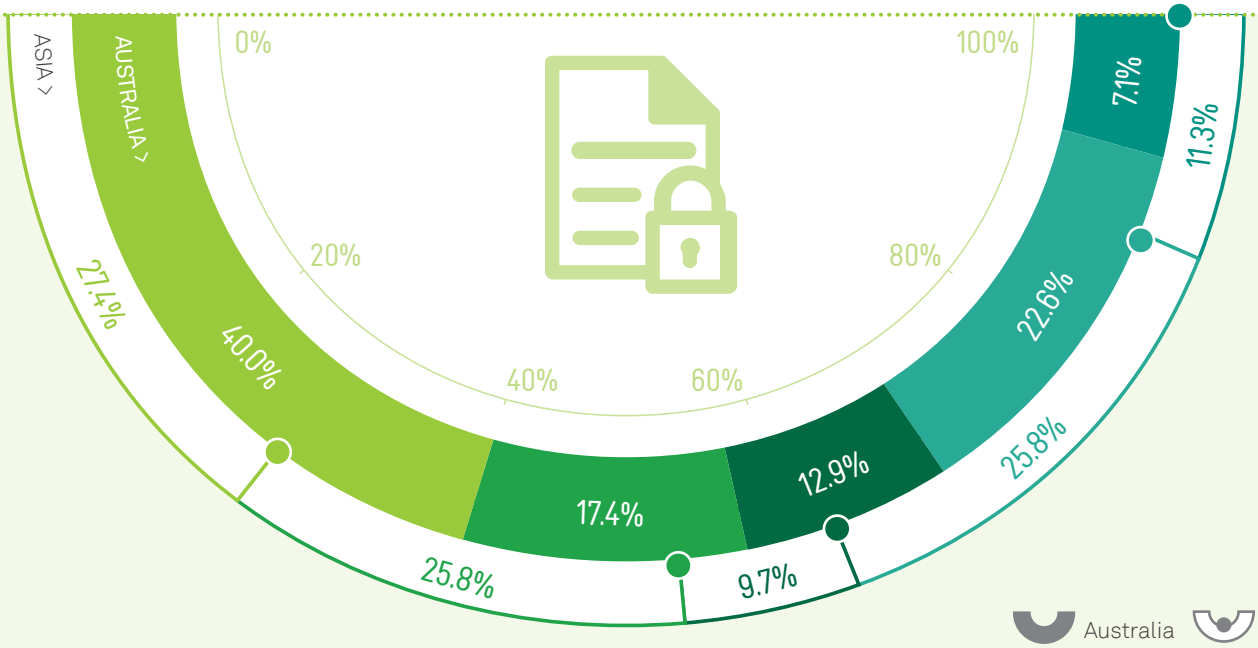
Our survey found that 68% of Australian businesses were collecting or managing personal information, while over 80% of Asian businesses were doing the same. However, even with the heavy penalties associated with the recent amendment to the Privacy Act in Australia, only 40% of respondents in Australia were aware of the amendments and already had security measures in place to protect personal information, where as, less than 28% of respondents from Asia were in a similar position.

Clearly privacy responsibility within many organisations needs to be improved. To improve the security of information protected under the Privacy Act, we have seen larger organisations moving towards hiring dedicated personnel in the form of a privacy officer (or Corporate Risk Offer). Smaller-sized organisations were more likely to pass on privacy responsibility to their IT group as the first step.

Ensuring privacy requires a combination of technology, policy, culture, and collaboration between many business units from security to legal to HR to employees.

If your organisation is collecting or managing personal information it is essential to audit and track the flow of personal information from both a systems and process perspective. If you are collecting personal information via an online system, ensure that you have appropriate security measures in place to protect the data and clearly identify the end user accessing the data. Conduct regular audits and vulnerability scans to ensure that you have appropriate safeguards in place and that they are effective. Regularly review your company's privacy policies and procedures to ensure that staff access to this information is appropriate and that they are trained to ensure the secure and proper handling of important corporate and customer data.

AUSTRALIA & ASIA
CURRENT RESPONSE TOWARDS PRIVACY AMENDMENT ACT IN AUSTRALIA



The organisation is aware and already has security measures in place to protect personal information	The organisation is aware of this and considering taking action	The organisation is aware of this but not taking any action yet	The organisation was not aware of this before, but may now consider taking action	The organisation is not aware of this regulation and not doing anything in response to this

[4]http://www.alrc.gov.au/news-media/privacy/australia-must-rewrite-privacy-laws-information-age

2.0 SECURITY THREATS AND TRENDS

2.1 MALWARE ATTACKS REIGN

HOSTED MALWARE IN AUSTRALIA IS ON THE RISE WITH NO SIGNS OF SLOWING DOWN

The increased use of technologies for business processes in an outsourced world has created an environment where malware threats are thriving to the extent that a cottage industry for creation of malware has been established.

Exploit kits have made it even easier to create new malware variants which don't require special programming skills for criminals to generate a profit or make a statement. Most kits have a user-friendly web interface which operates in a similar way to commercial software with licensed users, software updates and support. The exploit kit author ensures that they are able to exploit the latest vulnerabilities and sometimes zero-day vulnerabilities so that they can increase demand and continue to profit from their monthly licensing fees.

Exploit kits have made a significant contribution to the thousands of new domain names and URLs which host malicious content and Australia has its fair share. In 2012, there were approximately 120,000 Australian-hosted web domains carrying malware. By mid-2015, 167,000 suspicious domains and 500,000 suspicious web addresses were hosted in Australia. Of the malicious URLs discovered in 2015, 88% of these were classified as "maximum risk"[1]. According to Cisco, Australia is second only to the US as a source of malware for Australian based destinations.

One of the biggest threats to the Asia Pacific region in 2015 is the Angler Exploit Kit. Angler is known to use zero-day vulnerabilities in Java, Flash, and Silverlight in order to compromise victims, posing a wider threat due to the increasing availability of mobile applications that now play these files. There is now evidence linking malware growth to that of smartphones and tablets, which is not surprising when the number of mobile devices in the Asia Pacific region is forecast to grow from approximately 6 billion devices in 2014 to approximately 10 billion in 2019[2].

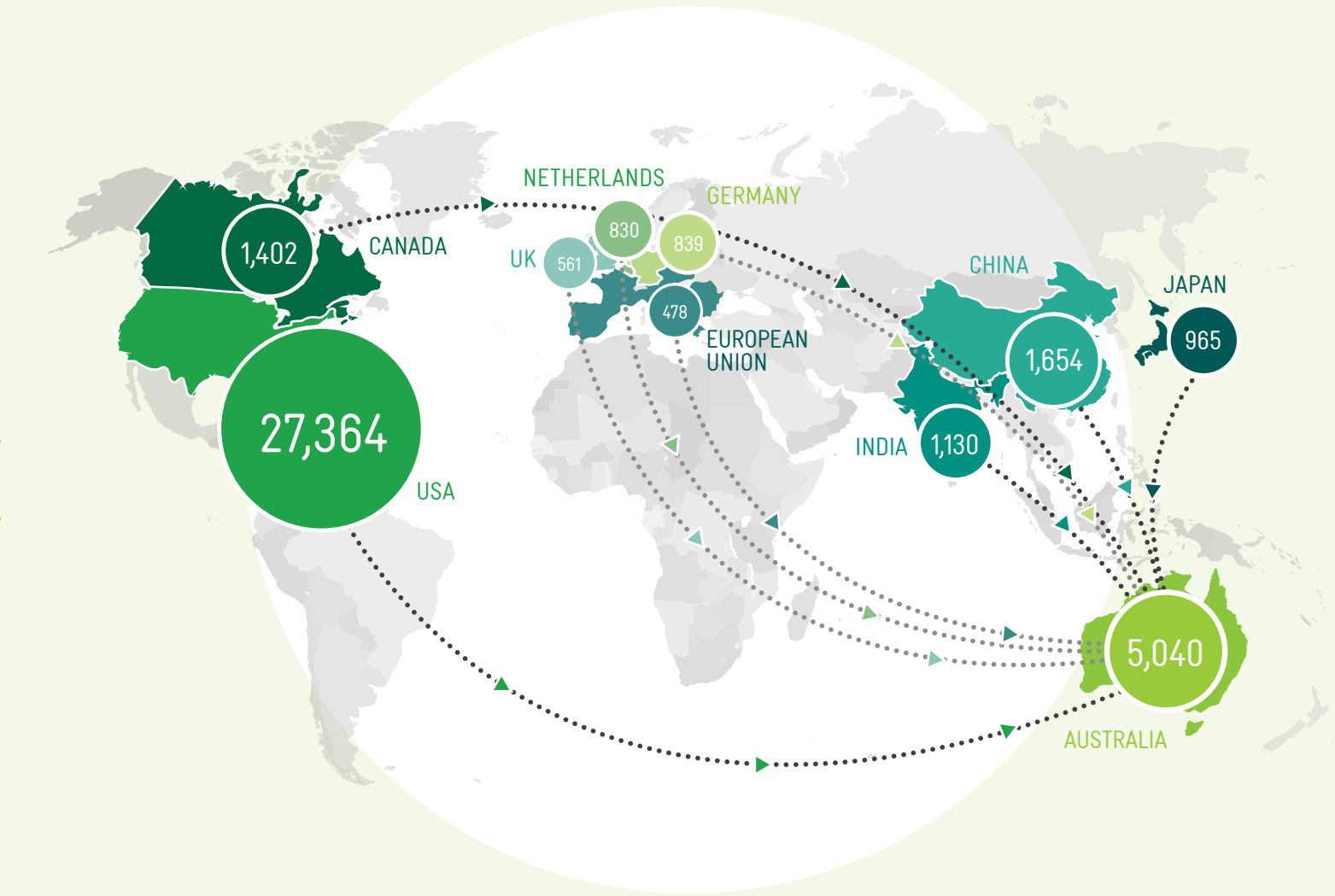
TOP EXPLOIT KITS IN AUSTRALIA

EXPLOIT KIT	DESCRIPTION
PC Utility Kit	Website which offers to run free Anti-virus (AV) scan and then to download fake AV software
FakeAV/Blackhole	Drive by download website uses Blackhole exploit to deliver the Fake AV malicious payload
Neutrino	Malicious code present on fraudulent websites or illegally injected on legitimate but hacked websites without the knowledge of the administrator
Nuclear	Attempts to detect an exploit called nuclearsploit which download malicious files that may further compromise the target host
DotKachef/Ramayana/Dotcache	Website exploit kit which infects legitimate advertising sites via OpenX
Angler	A hacking tool that is produced to search for Java and Flash Player vulnerabilities on the attacked PC and use them with the aim to distribute malware infections

Source: Telstra - Top Exploit kits (March 2015- June 2015)

[1] McAfee labs Threats Report, 2015
[2] www.cisco.com/web/solutions/sp/vni/vni_forecast_highlights/index.html

TOP SOURCE COUNTRIES TARGETING AUSTRALIA FOR MALWARE – 6 MONTHS OF DATA (MAY 2015)



Source: Cisco Systems

2.2 DEFENDING AGAINST THE APT INSURGENCE

THE FIGHT AGAINST MALWARE ATTACKS IS CHALLENGING AS ORGANISATIONS STRUGGLE TO COPE WITH THE EVER GROWING NUMBERS

The new generation of cyber-attacks are coordinated efforts that are highly sophisticated in scale. The rise in the number of breaches caused by advanced malware attacks aimed at enterprises and organisations with highly sensitive data has highlighted the need for protection against these types of threats.

These threats are collectively known as Advanced Persistent Threats (APTs), which is a term that generally means a coordinated and targeted attack or vulnerability using sophisticated intrusion techniques that are unable to be detected by conventional signature and/or reputation-based malware detection tools. An APT essentially consists of an advanced malware typically built on zero-day vulnerabilities and some form of botnets. The targeted nature of an APT attack often means that it will involve some form of social engineering reconnaissance before the attacker establishes a target or puts a foothold in the network. The persistent nature of an attack means it is often designed to remain undetected and may reside in the network for some period of time. The use of social engineering techniques remain a mainstream approach in the distribution of APT attacks, and email phishing will remain one of the most popular attacking methods of APTs.

Despite the disruption APTs can create, the adoption of APT solutions remains relatively low and this is mainly due to the cost of the solutions along with low levels of awareness of APTs across most industries, with the exception of government agencies and the Financial Services sector.

In recent years, government agencies have become the primary targets of these attacks, especially as many of the APT attacks have been politically motivated. Governments across the region have been forced to adopt measures protecting themselves from these targeted attacks as one of their highest priorities. The governments which had experienced geopolitical attention during the year were found to be greater targets.

With the growth of financially motivated actors, financial institutions and insurance organisations have also been the target of these attacks. Other industries such as the Energy, Oil & Gas and Mining with industrial control systems (ICS) are also becoming likely targets – particularly those companies with high-value information.

2.3 RANSOMWARE

AUSTRALIAN ORGANISATIONS ARE A POPULAR TARGET FOR RANSOMWARE ATTACKS

2015 saw a substantial increase in the amount of ransomware infections and this is largely due to the practice becoming a profitable business for cyber criminals. Ransomware is a type of malware that encrypts files and gives a number of days to pay a ransom to remove the restriction - either by supplying a program or by sending an unlock code that decrypts the files. A key element in making ransomware work for the attacker is using a convenient, anonymous payment system, like Bitcoin.

Ransomware typically propagates via phishing emails (Spear Phishing techniques in particular) to initiate an infection. Phishing emails appear to come from trusted organisations and are used to infect the host with the ransomware which is delivered via an infected attachment or a redirection to an infected website.

Key targets of ransomware appear to be wealthier countries whose victims are more likely able to pay ransom demands by hackers. CTB-Locker, CryptoWall 3.0, CryptoLocker and TorrentLocker were the most prevalent ransomware in Australia[3]. The main offender was Cryptolocker which uses a bug in a Windows API to encrypt all images, documents and other files which the infected machine can access. So it is no surprise that when the Websense ThreatSeeker network detected 1.05 million instances globally of ransomware CryptoLocker attacks, 60% of these attacks were detected in Australia[4]. The total amount of money reported lost in 2014 due to ransomware and malware incidents in Australia was estimated at $1,228,282[5].

The impact of a ransomware attack can vary depending on the organisation's size and level of readiness to deal with such incidents. Some organisations suffer operational disruptions or the loss of key company data, while for less fortunate organisations, mostly among small to mid-sized businesses, ransomware attacks can be devastating and cause a complete shutdown of the business and the recovery of data unlikely. User education is key to preventing this type of infection.

In the event that you become infected with ransomware and receive a ransom request, you should be aware that even if you pay, there is no guarantee that you will get your files back.

Some simple first-line defences for ransomware include:

- Make sure you have a current backup of all your data, and that this is kept up-to-date
- Remove administrative privileges where they are not needed, including local admin
- Make sure your IT systems and applications are updated and patched regularly
- Ensure your anti-virus and anti-malware software is up to date and active
- Educate users to take care with attachments coming from people not known to your organisation
- Backup your data – create a backup which is not connected to the local network as in most cases encrypted data is unrecoverable. Note: if you are using a cloud-based backup system there is a chance that the encrypted files may have been backed up to the cloud and some cloud providers only restore the most recent versions which may also be encrypted
- Block unwanted applications originating from your network. E.g. Users using Tor may unwilling download encrypted malware that may not be visible to some security gateways
- Upgrade OS and patch maintenance for operating systems (e.g. Java, Adobe Reader, Flash and applications) and enable automatic operating system updates where possible
- Deploy end-point protection
- Deploy anti-spam on email gateways and block unnecessary file formats like .scr which are used in some ransomware
- Conduct Phishing user awareness training to prevent the infection occurring in the first place

[3] McAfee labs Threats Report, May 2015 & Trendlabs 2Q 2015 Security Roundup
[4] http://www.computerworld.com.au/article/575096/australia-popular-target-ransomware-attacks/
[5] http://www.canberra.edu.au/cis/storage/Scams%20report__FINAL.pdf

2.4
EMAIL AND PHISHING ATTACKS

Threat actors are increasingly targeting end users as they are considered one of the weakest links in the security chain. It only takes one user to click on a malicious link or attachment in an email to infect and control your machine and then move laterally through the organisation to target IT infrastructure. Telstra security partner Firstwave blocked 613 million malicious emails on behalf of its clients' networks in 2015. By the end of year, they expected that the proportion of emails detected carrying malicious content will reach 68% .This is one of the reasons why phishing campaigns are becoming increasingly popular to gain a foothold into organisations.

Phishing campaigns have evolved in recent years to incorporate installation of malware as the second stage of the attack. Phishing emails with "drive-by download" compromised websites continue to be a common way for malware to gain a foothold in your network. The total amount reported lost in 2014 in Australia, due to information obtained from phishing scams and other sources to hack into email, banking or social media accounts, was $1,906,007[6].

Phishing attacks are by far the most common form of attack method used to compromise individuals and organisations. Phishing attacks increased by 29% in 2015 with the key increase due to Snowshoe-type spam sent in 2015, according to Firstwave. Snowshoe spam is difficult for traditional anti-spam gateways to block because it typically uses multiple IP addresses with very low spam volumes per IP address.

Insider threats play a major part in email security. In 2015, Firstwave detected 17,000 attempts to send credit card information over email in breach of finance industry security standards. This figure was 45% lower than 2014 which may be due to an increasing staff awareness and using more secure ways of transferring PCI data and not sending this type of information via email.

Firstwave blocked over 987,000 inbound and outbound emails that contained compromising content such as profanities and offensive images. Offensive content being distributed by employees can lead to businesses experiencing significant reputational and financial losses due to sexual harassment, discrimination and bullying claims. Fortunately, there has been a significant drop in the distribution of inappropriate outbound emails in 2015, with a drop of 16% across the total client emails sent.

Some simple considerations:

- Use dedicated email security tools that protect against malware and repel phishing emails
- Educate your staff through an awareness program about phishing and malware and test their knowledge periodically
- Implement social media and email policies to address inappropriate use and privacy issues for sensitive and personal information
- Implement data loss prevention and other tools that prevent unauthorised data leaving your business
- Deploy end-point protection on all devices within your organisation

[6] http://www.canberra.edu.au/cis/storage/Scams%20report__FINAL.pdf

MOST COMMON ADVANCED FORMS OF PHISHING MALWARE IN 2015

EXPLOIT KIT	DESCRIPTION	THREAT
Troj/Agent-AKWY	TR-Agent.AKWY.7.trojan is a Trojan horse developed by cyber criminals in order to mess up your computer and steal your personal information. Most computers get infected with this Trojan because the user downloads something from the internet. They are either bundled with useful applications or users are tricked into downloading them. Trojans are most likely to be installed alongside freeware applications, which is why it's so important to be careful whenever installing anything. Once this virus is downloaded, it will create a secret backdoor into your computer. This allows hackers to easily access your computer. It also gives the hackers a great way to put additional viruses or software onto your computer.	**HIGH**
Troj/VBAgent-W	Trojan/Agent.w has been classified as a really hazardous Trojan horse that has the ability to damage the system files of the infected systems in a very short time. The virus uses a network loophole to invade many systems.	**HIGH**
Troj/Invo_Zip	The Troj/Invo-Zip is a Trojan horse that is activated when a user downloads an attachment from a spam email and then is used to steal identity information. The Troj/Invo-Zip has been named as one of the worst computer malware threats.	**HIGH**
Mal/BredoZp_b	Package delivery email with either an infected attachment or URL to an infected site to distribute malware. Mal/BredoZp-B is a malicious infection that points to all the Windows systems. It can enter your computer through the shortcomings of Adobe Flash. The infection presents itself to users as an Adobe PDF file on spam email attachments. Mal/BredoZp-B is a type of Trojan horse that spreads over the network. It often lurks into the targeted system via sharing files on peer-to-peer networks, unsolicited emails, hacked websites, infected removable storage devices and more. This Trojan horse has the ability to hide deep in the infected system and perform various harmful activities according to the commands set by its creators. It modifies the registry entries so as to make sure that it can run automatically whenever Windows launches. It disables the antivirus program installed in the computer to evade detection and removal.	Medium
Troj/Agent-AKYO	This Trojan may often install itself by copying an executable to the Windows system folders, and then modifying the registry to run this file at each system start. This Trojan may perform different malicious functions like redirecting web traffic, installing additional malicious programs or manipulating certain Windows settings.	Low

Source: Phishing Malware Telstra

2.5 WEB AND APPLICATION VULNERABILITIES

There have been many attention-grabbing zero-day vulnerabilities that have provided the opportunity for hackers to gain unauthorised access to computer systems. Two recent high-profile vulnerabilities, Heartbleed and Shellshock, have brought a new perspective on the impact that these types of vulnerabilities can have on organisations. What makes these vulnerabilities so unique is the prevalence of the software impacted and that they were found in many systems and devices. While many vulnerabilities can affect millions of systems, experts estimated around half a billion web servers (almost 51% of all web servers)[7] and devices could potentially be affected by Shellshock, which makes it the largest known risk of its kind in terms of devices it could compromise.

Shellshock was exploited within hours of the initial disclosure by attackers creating botnets of compromised computers to perform Distributed Denial-of-Service (DDoS) attacks. Cloud security provider Incapsula noted that there were 17,400 attacks on more than 1,800 web domains within one 24 hour period; of which 55% of the botnet attacks originated from China and the United States[8].

The scale and rapid nature of attackers using these vulnerabilities to exploit systems within a short period of time after public disclosure was remarkable. Although remedies, workarounds or patches were made available for the majority of reported vulnerabilities typically within days or hours, there is always the potential for attackers to quickly exploit wide-reaching vulnerabilities to cause a major disruption for an organisation.

An exploit is a software tool designed to take advantage of a flaw/vulnerability in a computer system, typically used for malicious purposes which may include things like gaining control of a computer system, allowing privilege escalation, installing malware or a Denial-of-Service (DoS) attack. Many hackers won't utilise the latest exploits for new vulnerabilities if an old one exists. Exploits against zero-day vulnerabilities are not highly sought after by the attackers, especially when there is a known vulnerability already present that they can use existing tools and known techniques to exploit.

> RECOMMENDATIONS

Have a regular program that focuses on patching and maintaining software upgrades of operating systems and web applications for all IT infrastructure (not just internet-facing applications)

Adopt secure protocols offered by web applications like SSL or TLS to encrypt data when it is being accessed

Where possible, use two-factor authentication methods rather than just using username/password to access web applications or IT infrastructure. Ensure that password lockout after a fixed number of failed login attempts is active

Ensure input validation is implemented in applications when capturing data from an end user to safeguard against poor data quality and to stop injection of malicious code on your website (XSS & SQL injection)

Deploy website error masking to prevent hackers from discovering software versions and other reconnaissance information

Ensure that sensitive files/folders are not accessible/visible externally

Make sure security is a key consideration of web application project phases right from development to ongoing lifecycle management

[7] http://www.smh.com.au/digital-life/consumer-security/shellshock-the-latest-security-superbug-explained-20140926-10mcfx.html
[8] http://bits.blogs.nytimes.com/2014/09/26/companies-rush-to-fix-shellshock-software-bug-as-hackers-launch-thousands-of-attacks

AUSTRALIA TOP DOZEN INTERNET FACING VULNERABILITIES LAST 12 MONTHS (2014)

27%	Web server uses plain-text form based authentication
13%	Syntax error in web application indicates attack vector
10%	Apache mod_rewrite off-by-one buffer overflow vulnerability
10%	SSL server has SSLv2 enabled vulnerability
6%	SSL server supports weak encryption vulnerability
5%	Mail server accepts plain-text credentials
5%	SSL server allows anonymous authentication vulnerability
4%	X.509 certificate MD5 signature collision vulnerability
3%	TCP source port pass firewall
3%	Reflected cross-site scripting (XSS) vulnerabilities
2%	Web server predictable session ID vulnerability
2%	UDP source port pass firewall
11%	Other

Source: Qualys

2.6 NETWORK SECURITY THREATS

Palo Alto Networks has provided their top threats vs application reports in Australia and the Asia Pacific region. The highest volume application threats were DDoS attacks using DNS (Domain Name System) and NTP (Network Time Protocol) applications and Brute force login attempts using remote desktop protocols.

Brute force login attempts include remote desktop protocols which is why it is important to use strong two-factor authentication and strong encryption for remote access to your corporate ICT. DDoS and Brute force login attempts need to be considered as part of your security plans to ensure that your business is not overwhelmed by unwarranted malicious traffic.

THREAT	APP	SEVERITY	NO. OF IP PACKETS	
		1= high 4 = low	AUS	APAC
DNS ANY Request	dns	1	122487628	2618896078
DNS ANY Queries Brute-force DoS Attack	dns	3	86788494	2684078572
SSH2 Login Attempt	ssh	1	43977058	311406395
Microsoft remote desktop connect initial attempt	ms-rdp	1	43300825	258460109
MS-RDP Brute-force Attempt	ms-rdp	4	41997852	1099504052
HTTP NTLM Authentication Brute-force Attack	icloud-base	4	32963809	167612615
DGA NXDOMAIN response	dns	1	31262018	247541537
DGA NXDOMAIN response Found	dns	1	29613837	140738921
Microsoft SQL Server User Authentication Brute-force Attempt	mssql-db	4	14917855	72581771
Morto RDP Request Traffic	ms-rdp	2	14252243	754027204
Microsoft Windows SMB Negotiate Request	ms-ds-smb	1	12664078	1630130702
NTP Denial-Of-Service Attack	ntp	2	491490	1004406079
Microsoft Windows SMB NTLM Authentication Lack of Entropy Vulnerability	ms-ds-smb	3	2939238	915198336
NTP REQ_MON_GETLIST Request Found	ntp	1	491270	689764505
SMB: User Password Brute-force Attempt	ms-ds-smb	4	3547456	655420986
SSH User Authentication Brute-force Attempt	ssh	4	4400822	602131494

Source: Palo Alto Networks

2.7
DENIAL OF SERVICE ATTACKS

PERPETRATORS FOCUS FIRE ON APAC AND U.S

A Denial-of-Service attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the internet. Criminal perpetrators of DoS attacks often target sites or services hosted on high-profile web servers such as credit card payment gateways. Attackers vary greatly in terms of motives, capabilities, and resources. Attacker profiles include cyber criminals that are opportunistic and profit-driven, activists that are less sophisticated but highly motivated, and nation-states that have tremendous resources.

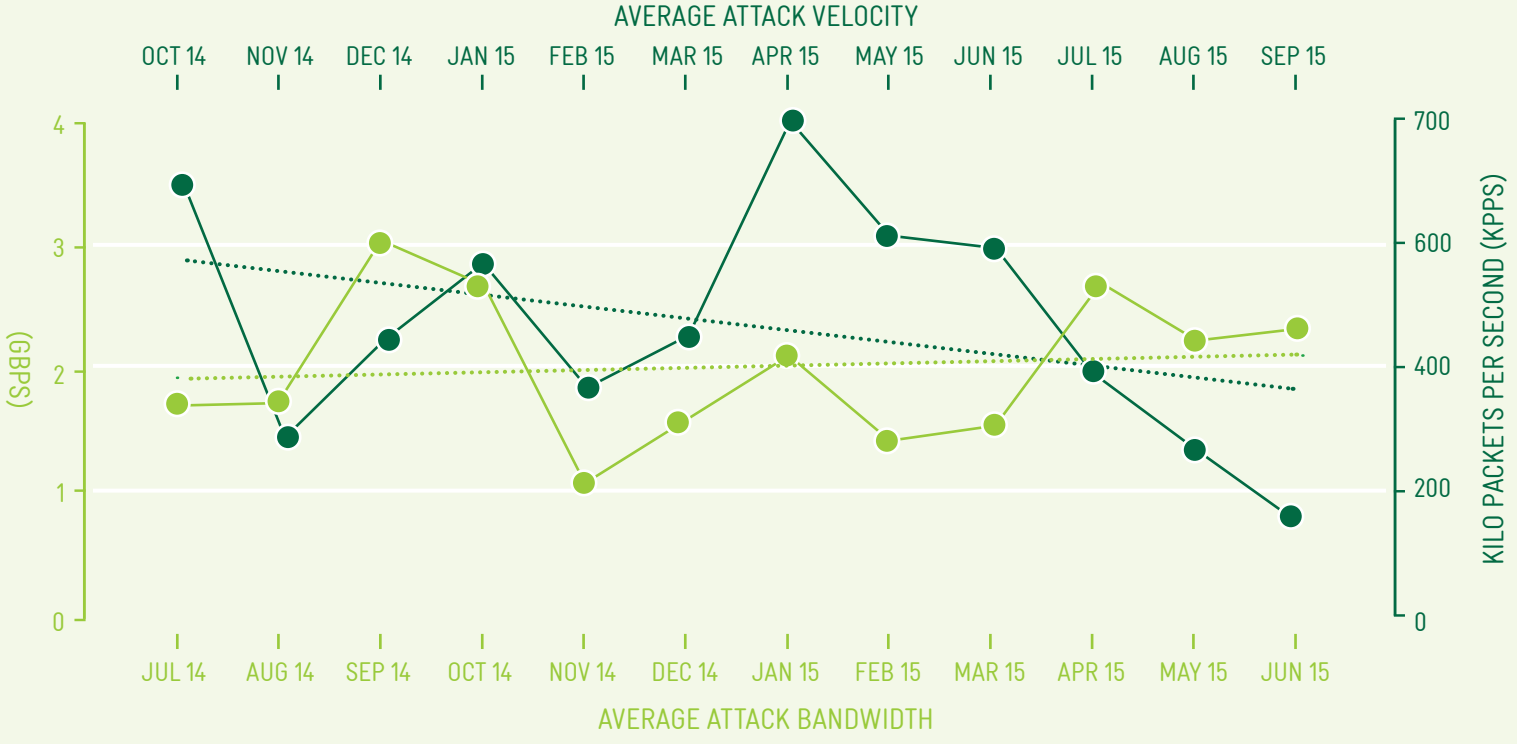
The Australian average attack bandwidth identified by Telstra was trending upwards at around 2-3Gbps with an attack velocity in the range of 200-800kpps (kilo packets per second). Such high-volume assaults have the ability to cause network saturation by utilising much of the available bandwidth resources. Australia's average fixed broadband speed has grown at approximately 5Mbps per year from 18Mbps in 2014, projected to reach 44Mbps in 2019[9]. As a result, we expect the attack bandwidth to rise.

There are two DDoS event types: network layer and application layer attacks.

Network layer attacks target the network and transport layers (OSI layers 3 and 4) and are typically measured in Gbps (gigabits per second).

Application layer attacks, on the other hand, target OSI layer 7 and are measured in RPS (requests per second), for the amount of processing tasks initiated per second. Unlike their network layer counterparts, these can bring down a server by overwhelming its processing resource (e.g. CPU) with a high number of application layer requests. Application DDoS attacks are typically executed by bots – compromised machines that are able to establish thousands of requests with a targeted application.

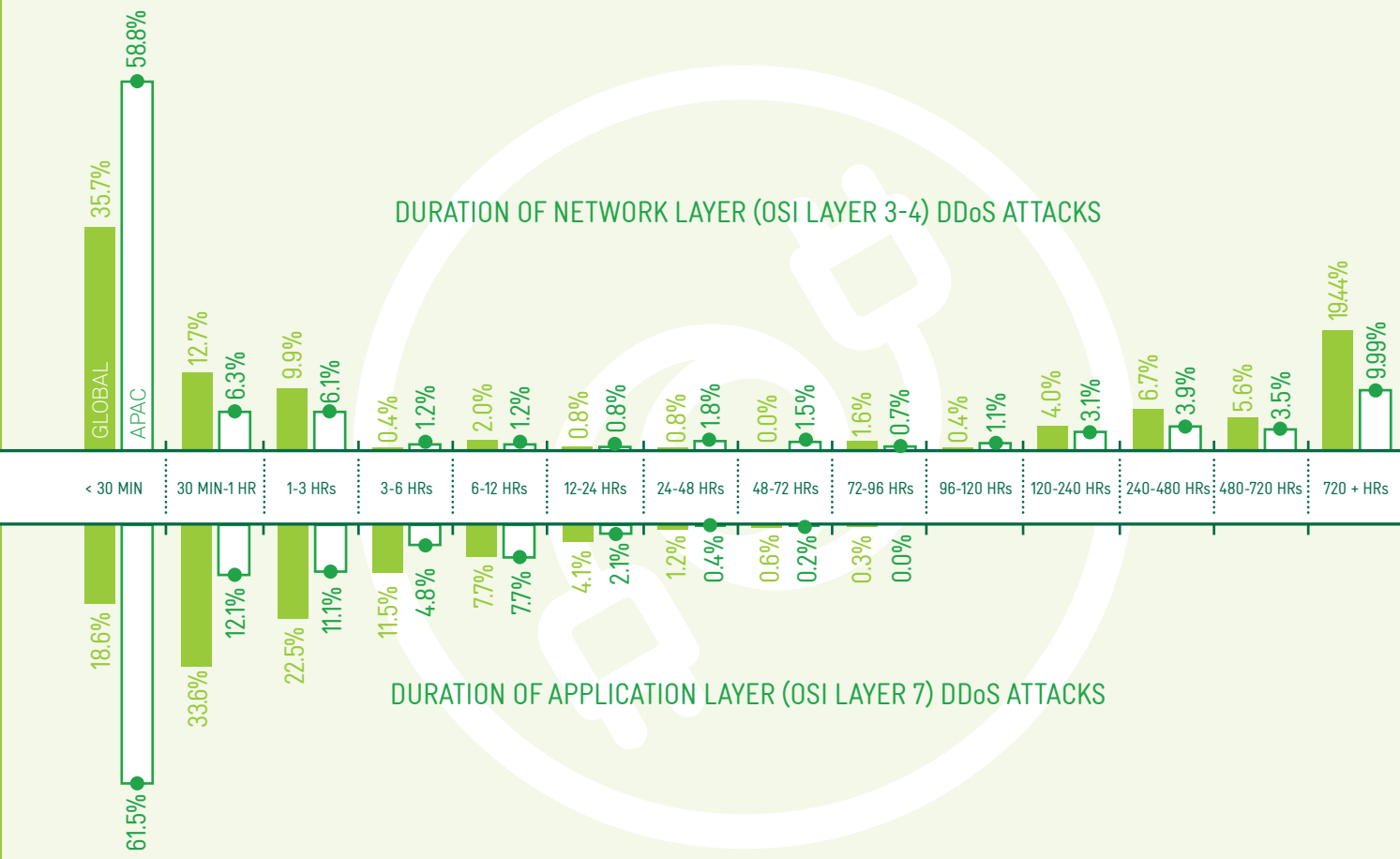
AUSTRALIAN NETWORK AND APPLICATION LAYER DDoS ATTACKS



Source: Telstra

[9] http://www.cisco.com/web/solutions/sp/vni/vni_forecast_highlights

DDoS ATTACKS AGAINST GLOBAL AND APAC BASED CUSTOMERS (MARCH – MAY 2015)



> LEGENDS

Global

APAC

Source: Imperva

AVERAGE ATTACK BANDWIDTH (GBPS)

LINEAR AVERAGE ATTACK BANDWIDTH (GBPS)

AVERAGE ATTACK VELOCITY (KPPS)

LINEAR AVERAGE ATTACK VELOCITY (KPPS)

Australia rated number 8 on the Top 10 Source countries for DDoS attacks in 2015 with 5% of the source DDoS traffic. The UK was the highest producer of DDoS traffic with 26%, with China at 21% and the US at 17% respectively[10].In the APAC region, we see the work of professional DDoS attackers that display a higher-than-usual degree of sophistication as opposed to "hobby" attackers using DDoS-for-hire services or simple DIY tools. DDoS Attacks against Asia Pacific targets are significantly more complex, with 62.3% being multi-vector threats with some exceeding up to 9 vector assaults[11]. Even though multi-vector attacks are low in overall percentages, they highlight the fact that advanced botnet capabilities are being used by attackers. DDoS botnets can display advanced capabilities like being able to dynamically change different packet types, as well as easily shift between symmetrical and asymmetrical attack methods, and even mimic browser-like features used for bypassing common security safeguards.

Durations for both Application and Network DDoS attacks are typically shorter in the APAC region compared with the global trends with more than half of the DDoS attacks under 30 minutes duration. The hit-and-run nature of these attacks suggests an ongoing trend in which attackers prefer to launch multiple assaults against a number of targets, as opposed to a single prolonged attack. This is consistent with the use of DDoS-for-hire, which offer attackers access to botnet resources—enough to launch a few short duration, mid-sized attacks.

[10] Akamai – The state of the Internet Q3 2015 Report
[11] Incapsula Global DDoS Threat Landscape Q3 2015

2.8
CLOUD ADOPTION

Cloud computing is a service which is in high demand due to the advantages of computing power, cheaper service costs, high performance, scalability, as well as availability and ubiquitous access. Adoption of cloud services has been strong for both Australian and Asian organisations with 64% and 95% respectively using cloud services, however organisations are still concerned about the security implications these services may bring. Data theft and network outages were amongst the biggest concerns raised by organisations and the least prepared for in the adoption of cloud services

Our research found that organisations who adopt cloud services are also concerned about transferring control of their data to their cloud service provider as their data may be stored in multiple countries. Organisations are worried that they may not be aware of the regulations within each country and the impact of government jurisdictions who can request access or intercept data with a warrant or for national security purposes. In Asia, data sovereignty was noted as the highest cloud services risk with the exception of Indonesian organisations who indicated that they were more prepared to handle data located outside their country. Indonesia does not have regulated restrictions for data movement overseas but they have requirements to locate data processing facilities within the country[12].

Adopting cloud services brings a number of benefits to your organisation including potential cost savings and quicker deployment timeframes but it is worth considering a number of things before you adopt cloud services.

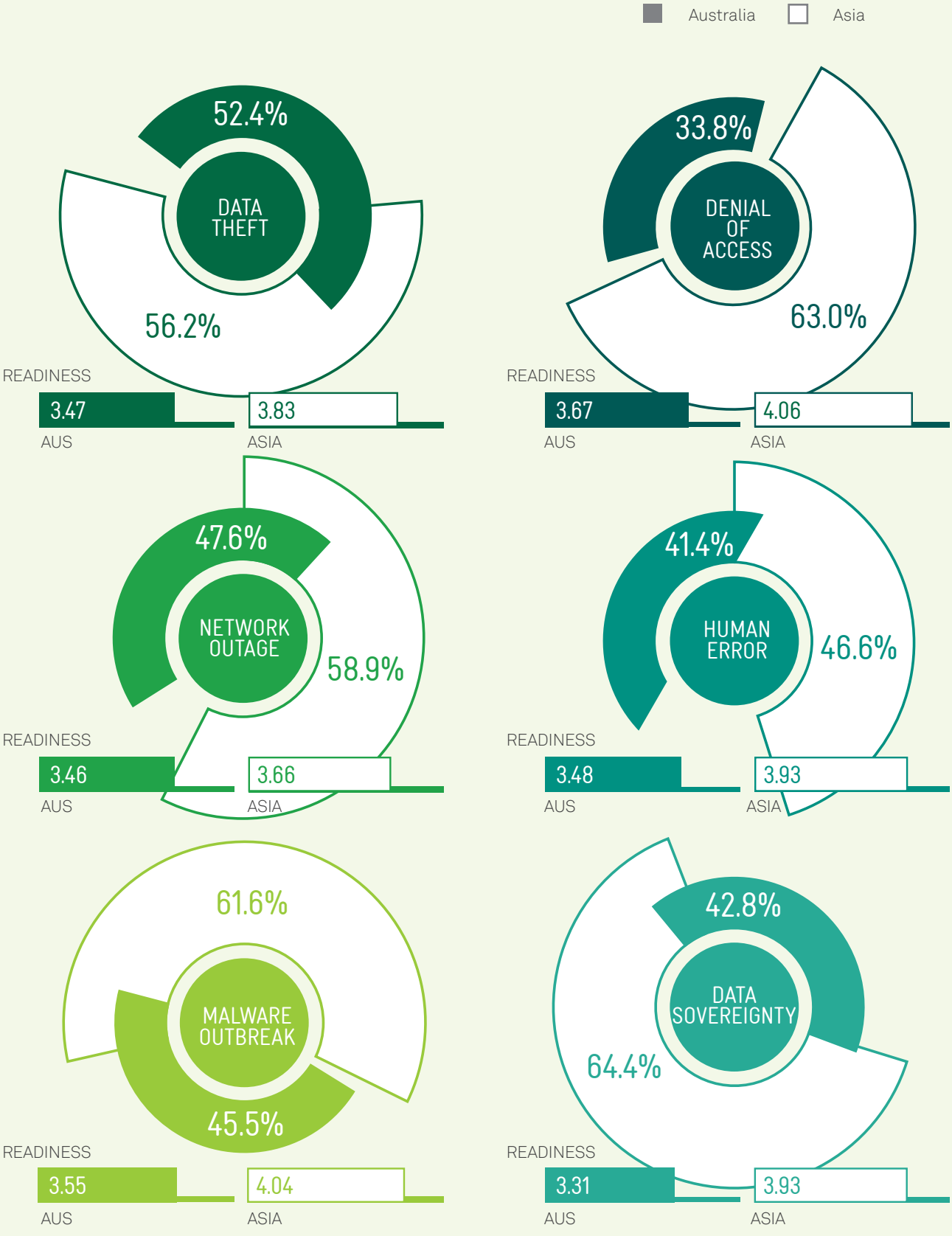
- Identify business risks associated with adopting cloud infrastructure and the types of data that is being collected, stored or shared in cloud environments.
- Ensure that you have an established security action plan in place with appropriate control mechanisms to mitigate cloud risks and disaster recovery plans to handle outages in conjunction with your cloud provider.
- Assess whether this function can be performed in house or whether external service providers would need to be engaged to perform these tasks.

[12] http://www.asiacloudcomputing.org/images/research/DataSovereigntyReport2013_ExecutiveSummary.v2.pdf

PERCEIVED RISKS VS READINESS IN HANDLING RISKS OF CLOUD SERVICES

Which of the following do you see as potential risks within your organisation as a result of adopting cloud services?
■ =YES

How would you rate your level of readiness in terms of handling exposure to any of the following risks as a result of adopting cloud?
0= NOT READY AT ALL 5=READY



2.9
CLOUD AND SHADOW IT

MOST COMPANIES ARE UNAWARE OF HOW LARGE THE SHADOW IT PROBLEM IS WITHIN THEIR ORGANISATION

With the ever-growing number of cloud-based services and changes in utility pricing models, it becomes considerably easier and quicker to buy and access software than ever before. However, these benefits come at a price; the traditional "office" no longer exists and it has presented a raft of new problems for IT staff to try and solve. The phenomenon of Shadow IT is one problem that is intensifying across the globe – a significant reason behind Shadow IT is the popularity of cloud-computing and SaaS.

Employees aren't always willing to wait for an approved solution from IT to arrive and many take matters into their own hands by utilising any solution that will fit their needs, often without the IT department's knowledge. As a result, many IT departments have knowledge gaps or "shadows" in their understanding of cloud app usage and data exposure risks in their environment.

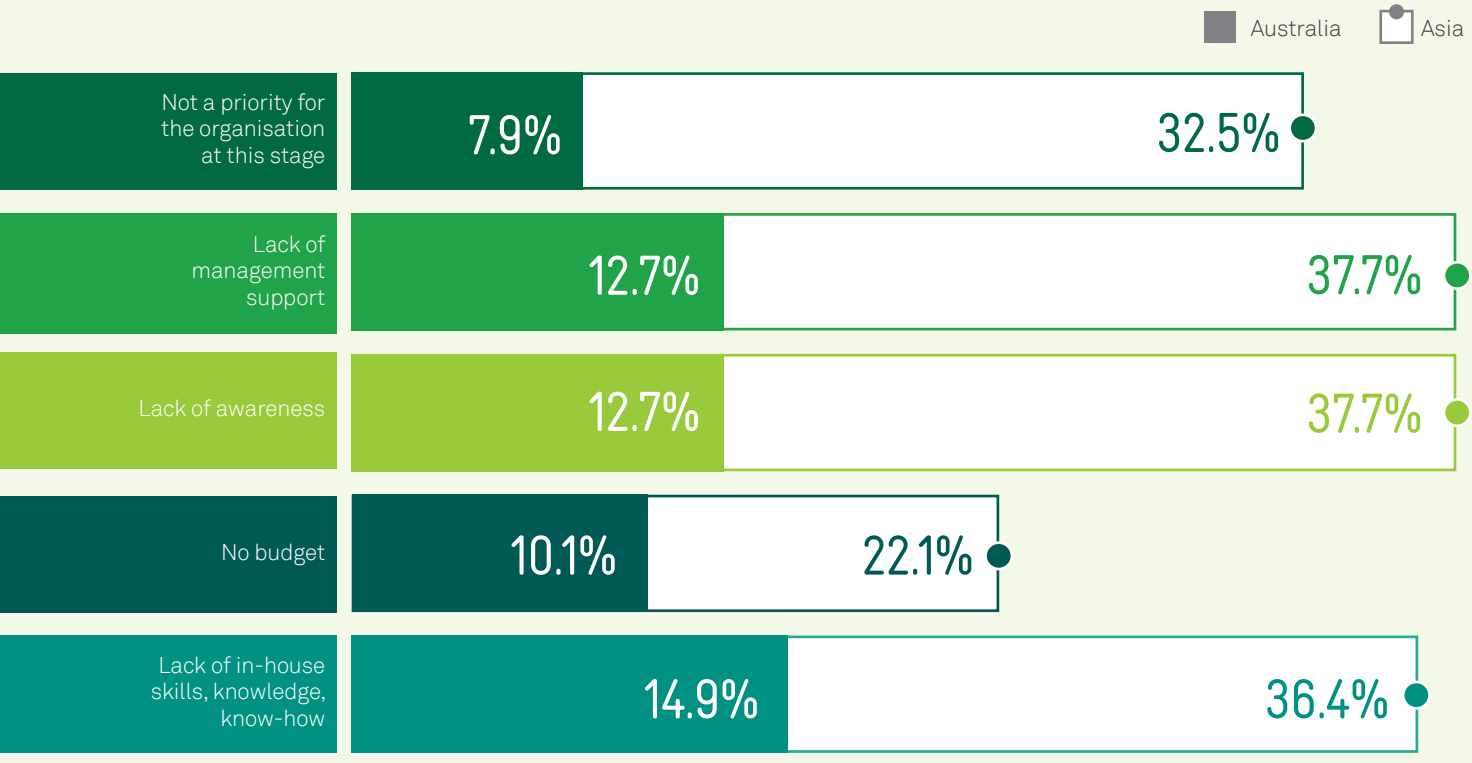
Our research suggests that this gap between the business and the traditional IT department will continue to widen. Through our engagements with clients in Australia and Asia, as many as 60% of respondents reported that Shadow IT is an issue within their organisation. Of concern was that nearly half of Australian organisations had not yet put in place the tools to track and monitor Shadow IT leaving them potentially exposed to valuable data loss. In addition, organisations generally found the lack of awareness and in-house skills as major challenges in dealing with the problem.

Two lesser but related challenges within organisations were the lack of management support and priority for the organisation to enable IT departments to secure funding and tackle the problem. The potential risks from sensitive data being uploaded into cloud apps, due to a lack of knowledge of the type of data being uploaded and shared, is a significant risk for businesses both from a privacy and compliance perspective.

Elastica[13] estimates that the risk per business of cloud data exposures from SaaS Storage providers (such as Box, Google Drive, etc.) was $13.85M per business (globally). Elastica has calculated that 25% of files per typical user are shared in 2015 (compared with 9% in 2014) and this percentage will increase in coming years. It found 2.1% of these files were shared externally (known parties outside a company) and contained Personally Identifiable Information(PII), Protected Health Information (PHI) or Payment Card Industry (PCI) data, with 1.2% of these files shared publically (available to anyone on the internet via a link to content) and contained PII, PHI or PCI data. These percentages might appear low in comparison with other cyber-threat data, but it only takes a single employee to share, for example, a spreadsheet containing sensitive customer information with the wrong person, that could have a devastating – not to mention costly – impact on the organisation.

[13] Elastica 2015 Shadow Data Report

MAIN CHALLENGES IN IMPLEMENTING A SHADOW IT STRATEGY – AUSTRALIA & ASIA



THE HIDDEN COSTS OF SHADOW IT

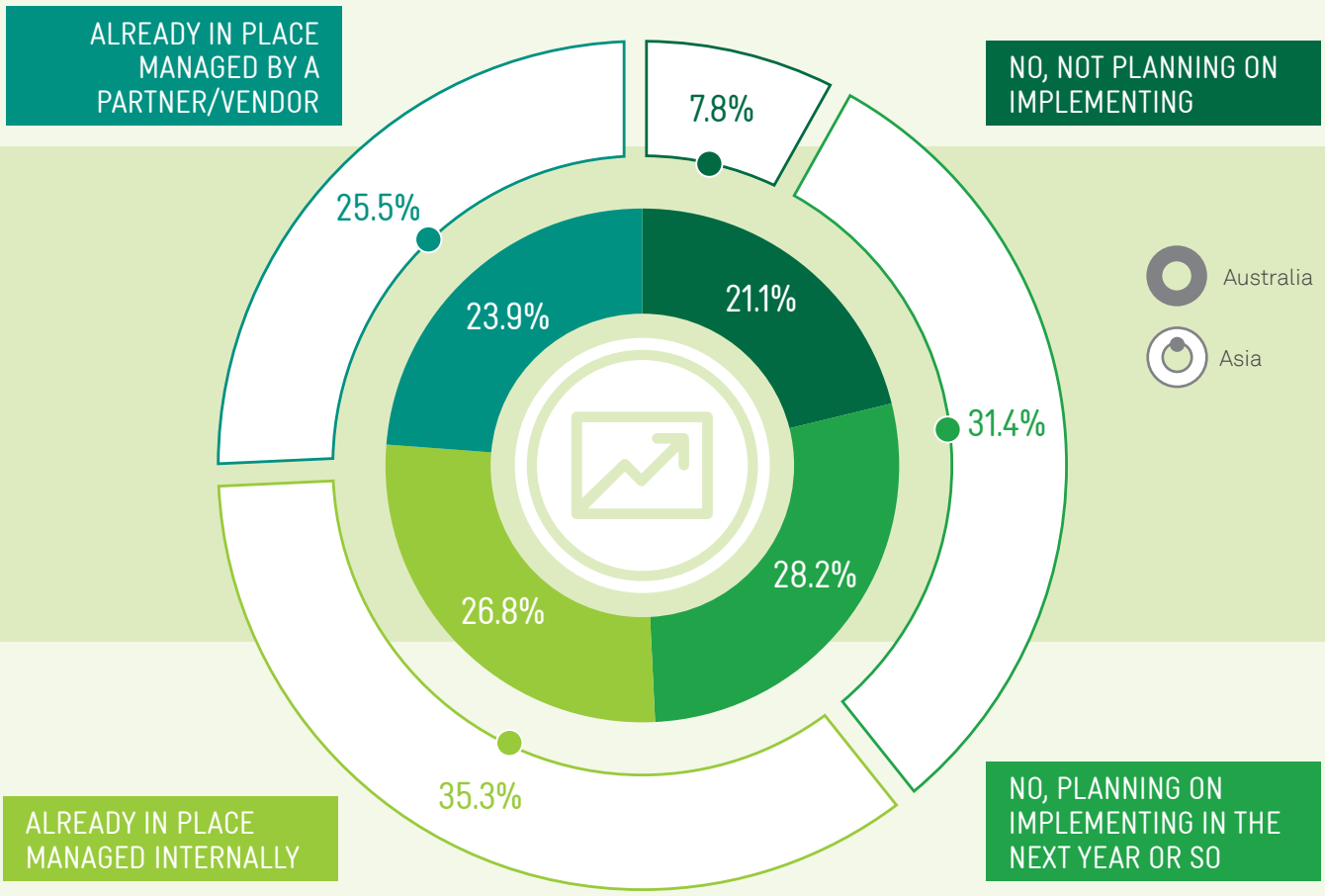
Despite the many benefits of cloud services used in Shadow IT, they can bring with them drawbacks and add hidden costs to organisations. One notable risk from a security point of view is the increased exposure it brings to data loss or data leakages with employees that may maliciously or unintentionally misuse corporate information the wrong way.

Our research shows that many unsanctioned cloud services incur additional costs that the business doesn't always see directly. Costs that can be attributed to applications not being integrated into the standard IT operational model and procedures of the corporation. This results in some activities being duplicated or inefficient at best, for instance, manual compliance checking, maintaining separate corporate identity stores, procurement and vendor management inefficiencies, or control over the use or backup of data.

CIOs generally realise that unauthorised cloud services are being used by employees within their organisation, but not many CIOs realise the number of unsanctioned cloud services being accessed and the full extent of their use within their company. More than 80% of employees admit to using SaaS applications in their jobs without IT approval and nearly 35% of all SaaS applications used in business are not approved, contributing to Shadow IT.[14] Nearly half (49%) of Australian organisations had not yet put in place the tools to track and monitor Shadow IT. 40% of these organisations came from the Manufacturing, Logistics, Transport and Retail industries. The risks associated with not deploying these tools is evident in that on average 15% of employees have experienced a security, access, or liability event while using SaaS applications[14]. However, employees will continue to use unsanctioned applications as 18% of IT users say IT restrictions on applications make it difficult to do their job and 24% of all users say non-approved software meets their needs better than the IT-approved equivalent.[14]

According to Elastica, the average number of applications found in an organisation is 774 – with many of these not known by the IT department[15]. Given the exponential growth of cloud applications, we can only assume that this number will increase.

AUSTRALIA & ASIA - USE OF TOOLS TO TRACK AND MONITOR SHADOW IT



[14] The hidden truth behind shadow IT - Stratecast | Frost & Sullivan research, McAfee, Inc sponsored
[15] Elastica 2015 Shadow Data Report

SO HOW DO CIOS ADDRESS THIS ISSUE?

A simple approach to tackling the problem is to follow the "three As" – Audit, Assess and Action.

AUDIT

Since you can't control what you can't see, the first step is to obtain a comprehensive audit of what is being used within your organisation. Most Cloud Application Security Brokering (CASB) solutions can help you achieve this, identifying the SaaS applications in use and an associated rating of the potential risks associated with each of these.

ASSESS

Once you have determined an acceptable risk of a SaaS application, determine whether it can be easily incorporated into your corporate security policies to offer a good outcome for employees and the organisation. For those applications that are deemed to be too risky, suggest alternatives that better fit your organisational risk profile.

ACTION

Given the critical nature of organisation compliance, ensure that you implement security controls that facilitate the use of approved SaaS applications. At the same time, provide control to prevent sensitive data leaving the organisation or being misused.

Things you can do to curb the Shadow IT problem within your own organisation:

- Ensure that you have clear guidelines in place in your corporate Acceptable Use Policy for the procurement and use of cloud applications within your organisation
- Implement tools to provide real-time auditing of use of unauthorised cloud applications and potential shadow data exposures
- Work with employees to understand their requirements and agree on a suitable application fit-for-purpose that allows you to monitor and block sensitive shadow data leaving the organisation
- Get ahead of the curve by providing access to a broad range of approved cloud based apps, giving employees the freedom to select what best meets their needs

2.10
MOBILITY THREATS

ORGANISATIONS MUST LOOK TO DEFEND AGAINST A NEW FIELD OF EMERGING THREATS

The traditional boundaries of an organisation have expanded as smartphones and tablets become ubiquitous within organisations. Bring your own device (BYOD) corporate policies are permitting employees to bring personally owned mobile devices to their workplace and to use to access privileged company information and applications outside the corporate boundaries. Furthermore corporate data is no longer stored safely within the confines of a company-owned data centre, but increasingly in the cloud and even on mobile devices. These technologies have become an attractive target for cyber criminals, particularly for financial gain and identity theft.

Mobile devices are collecting and storing an increasing amount of sensitive corporate information and criminals are exploiting weaknesses in a number of communication protocols like SMS, Wi-Fi networks and Bluetooth. There are also attacks that exploit software vulnerabilities from both the web browser and operating system on the device.

Organisations need to ensure that the security and integrity of their network data is maintained and that sensitive data is not lost, destroyed or held to ransom when staff connect using these mobile devices. Mobile malware infection rates were over 5% in Australia and over 9% in Asia. Globally, the number of new mobile malware instances has increased by 49% from Q4 2014 to Q1 2015[16]. The majority of the malware seen in Australia and Asia was Trojan-based malware aimed at gaining control of the device via remote access tools (RAT). The two Android malware threats which appear in the top 12 malware in Australia were specific variants of the Fakeinstaller application which can be used to send premium SMS services without the user's knowledge[17]. The spread of ransomware to mobile is likely to increase over the coming year.

> TYPES OF MOBILE-BASED MALWARE

RANSOMWARE

Early android ransomware performed a basic screen lock function which could be unlocked when a money voucher code was entered. New ransomware for Androids is able to encrypt data on the phone's memory card and uses Tor, SMS or HTTP to connect to the attackers.

BANKING TROJANS

This android malware intercepts SMS banking authorisation codes and forwards them onto the hacker, enabling them to conduct fraudulent transactions from the user's account.

SMS MALWARE

This malware sends SMS messages to premium services to extract payments without the user knowing.

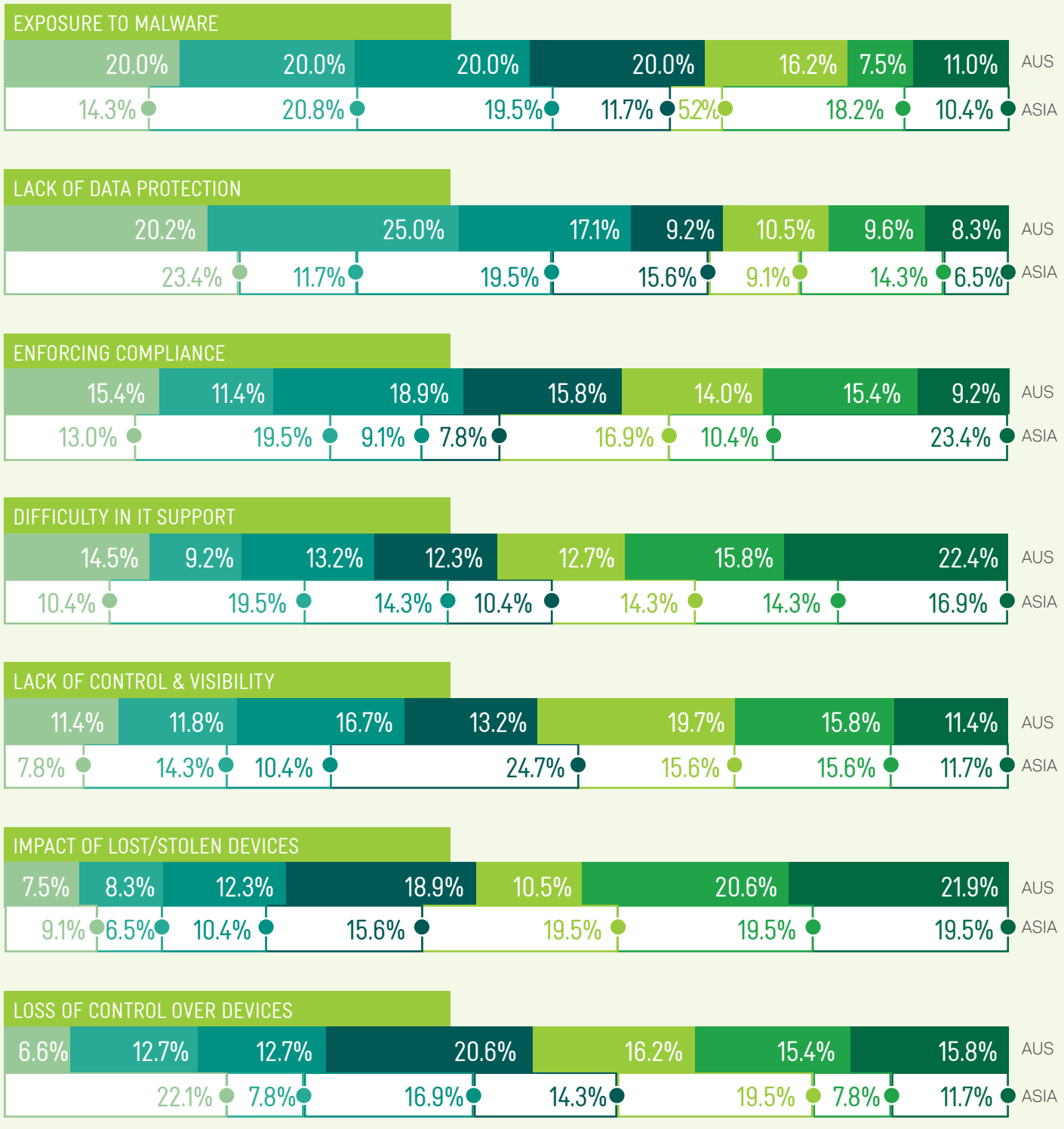
[16] McAfee Labs Threats Report, May 2015.
[17] blogs.mcafee.com/mcafee-labs/fakeinstaller-leads-the-attack-on-android-phones

AUSTRALIA & ASIA - CONCERNS WITH EMPLOYEES USING THEIR OWN DEVICES AT WORK (BYOD)

This year we surveyed Australian and Asian organisations on their main concerns with BYOD devices in the workplace. 20% of Australian organisations highlighted malware exposure and a lack of data protection as their number one concern in a BYOD environment. Whereas Asian organisations were more concerned about insider threats from leakage of data and the loss of control from loss/theft of mobile devices.

Australia Asia

Rank your top concerns with employees using their own devices at work, with 1 being the most concerned, and 7 being the least concerned.



Most organisations believed they had inadequate security safeguards to mitigate mobile threats. In particular, Australia appears to be lagging behind their Asian counterparts by as much as 20% in some cases.

While data encryption and anti-malware remained the main security technologies adopted for mobile devices in both Australia and Asia, mobile device management (MDM) and mobile application management (MAM) solutions, essential to administrating device and application policies remotely, was low and remains an opportunity for improvement.

Basic security measures like strong authentication and in particular two-factor authentication are powerful aids that provide a high level of data theft protection. There is a variety of two-factor authentication mechanisms, notably the use of a token that the user uses in conjunction with a password. More modern approaches to this uses a dynamic passcode consisting of digits that can be sent to their mobile device by SMS or via an application. The advantage of this method is that there is no need for an additional, dedicated token, as users tend to carry their mobile devices around at all times anyway.

As expected, advances in the implementation of corporate mobile security policies are more prominent among larger organisations. Financial services, government, and large retail organisations have made the most progress in advancing their mobile security policies, which tend to have more mature cyber security programs in place.

> BYOD GUIDELINES FOR A SECURE WORK ENVIRONMENT

Ensure that you have a BYOD Acceptable Use Policy implemented that also covers employees who leave your organisation but take their mobile device with them

Corporate data should be encrypted both when it is stored on the device and when it is being accessed. Ensure you use VPN encryption for connectivity back to your corporate network

Ensure you have end-point protection on all devices within your organisation including mobiles, tablets, laptops, PC and server-based infrastructure

Ensure devices are regularly updated with the latest OS and patches

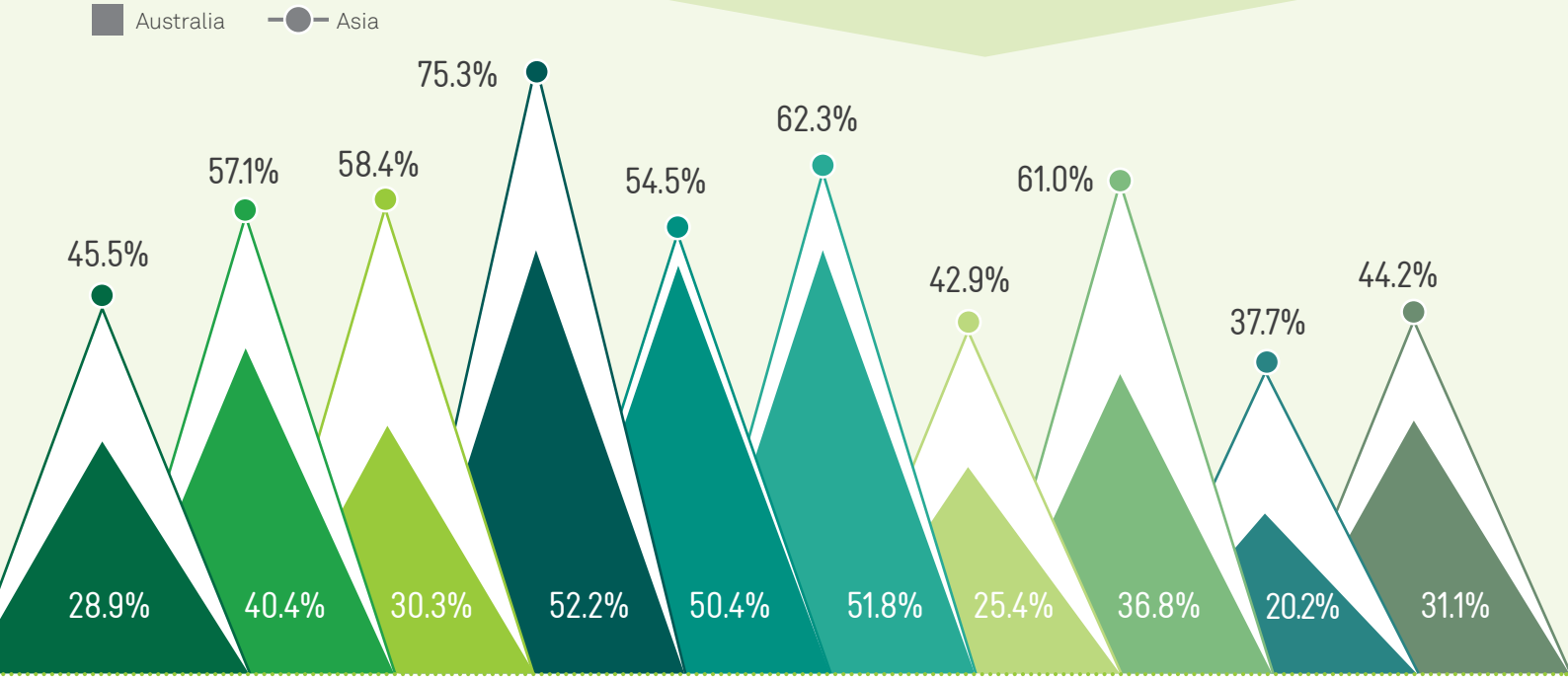
Never allow jailbroken and rooted devices onto your network

Ensure you have remote policy management of devices using technologies that include Mobile Device Management (MDM), Mobile Application Management (MAM), or Mobile Content Management (MCM) to help with keeping business data separate from personal data

Enforce using strong passwords on devices and, where possible, use two-factor authentication for access to sensitive applications or data

AUSTRALIA & ASIA ADOPTION OF TECHNOLOGIES TO MITIGATE BYOD THREATS

- Remote application/policy configuration
- Remote lock/wipe for lost/stolen mobiles
- GPS location tracking
- Data encryption
- VPN
- Anti-malware
- Segmentation of company and personal applications and data
- Cloud-based email and web security
- Containerised security
- Two-factor authentication



3.0 SECURITY INCIDENTS AND BUSINESS IMPACTS

Cyber criminals typically target financial information like credit/debit cards, with high profile examples like Target (US) and Home Depot in 2014[1]. However, there is a growing trend among cyber criminals towards stealing full personal details, healthcare information and identity theft which has a higher impact than simply reissuing credit cards. Full identity records, including healthcare records, are a more attractive target as this sells for 10x price of credit card details on the black market and there are multiple opportunities to fraudulently claim for benefits in a user's name (e.g. tax refunds or health insurance refunds) or build up debts on new loans/credit cards.

In the US, there have been a number of security breaches announced by government departments in 2015 where significant amounts of sensitive and personal identity information has been stolen.

The Office of Personnel Management (OPM) announced two separate security breaches in April and May 2015. The earlier breach exposed basic job application data for 4.2 million people. All these people were notified and offered to enrol in an identity protection program. The much larger breach – which was discovered in May – involved more sensitive personal information which is gathered for security clearance investigations for current, former and prospective federal employees and contractors. The breach included 19.7 million contractor and employee security clearance information and 1.8 million "non-applicant" information whose personal data was included as part of the security clearance e.g. spouses.
A total of 21.5 million Americans have been compromised as there is some data overlap between the two breaches[2].

The IRS announced security breaches in May and August 2015 where a total of 334,000 taxpayers' information has been lost. The thieves accessed the information by entering personal data, which included social security number, date of birth, tax filing status and address, which was previously stolen from other sources to get even more information about taxpayers. This would allow the thieves to claim fraudulent tax refunds in the future.
The IRS has been notifying all potential victims and offering free credit monitoring services and enrolling the potential victims in a program that assigns them a special ID number to use to file their tax returns. This is not the first time the IRS has been targeted by identity thieves.
The IRS estimates it paid out $5.8 billion in fraudulent refunds to identity thieves in 2013[3].

[1] http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/#11e044013a48
[2] http://www.msn.com/en-us/news/us/us-has-yet-to-notify-215-million-data-breach-victims-officials/ar-AAcZ4kO?srcref=rss&ocid=iehrs
[3] http://www.msn.com/en-us/news/us/irs-says-thieves-stole-tax-info-from-additional-220000/ar-BBlOJ7e?srcref=rss&ocid=iehrs

3.1
ORGANISATIONAL READINESS AND MATURITY TO HANDLE SECURITY INCIDENTS

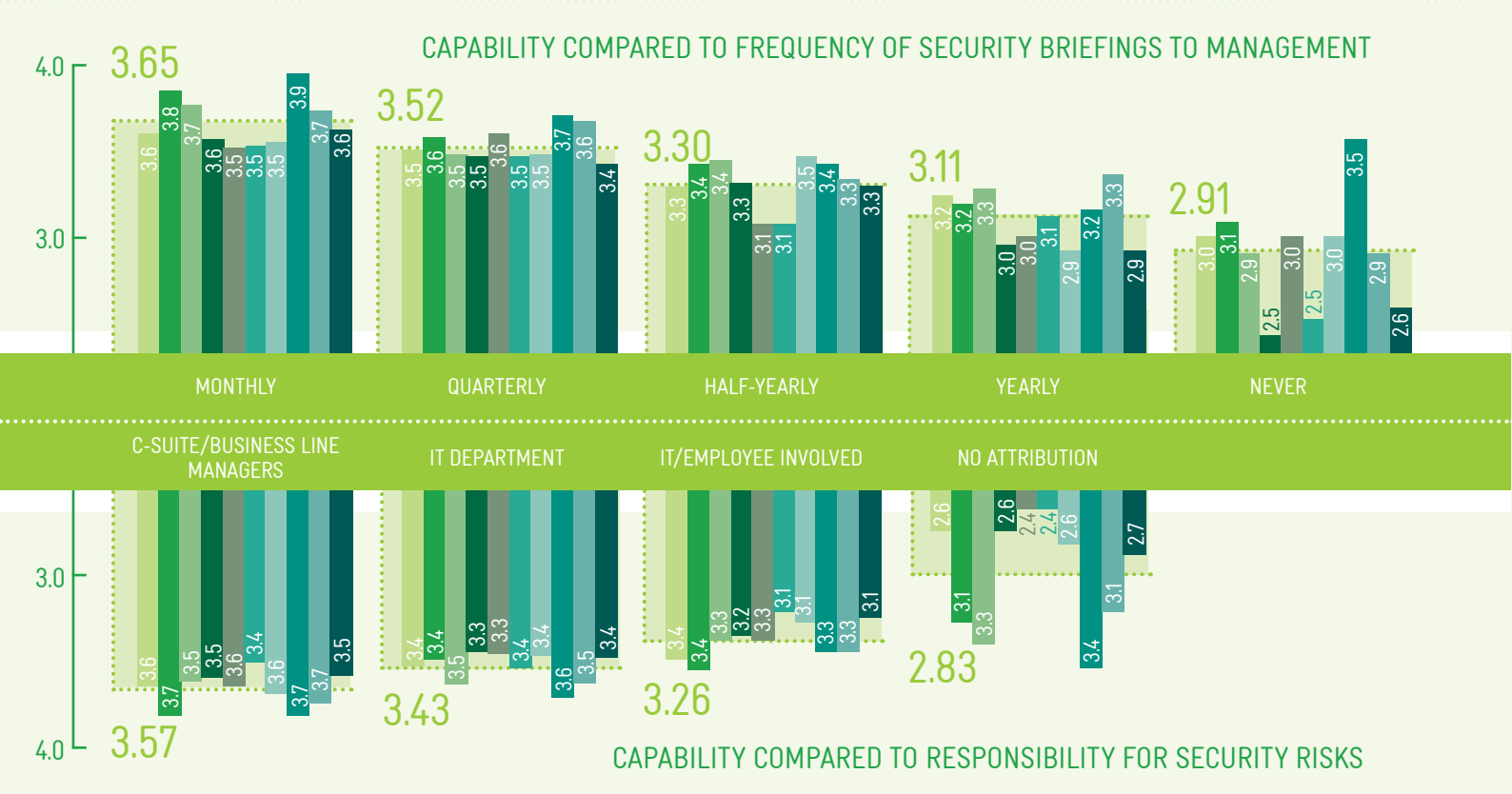
While our survey research indicates that the number and impact of cyber incidents continues to rise, many organisations in Australia still operate under the assumption that they won't be breached. We believe the reason for this is the lack of stringent regulations in Australia for data protection of corporate and customer data and the legislation of mandatory disclosure in the event of a data breach.

C-suite and Board members are shifting their focus to cyber security, but there is still room for improvement. Ideally, every organisation should have a cyber response plan to deal with cyber security incidents. While Australian organisations feel they have sufficient capability to address a range of security incidents that include malware and phishing related incidents, less than 20% of the overall respondents indicated that they were confident in addressing security incidents.

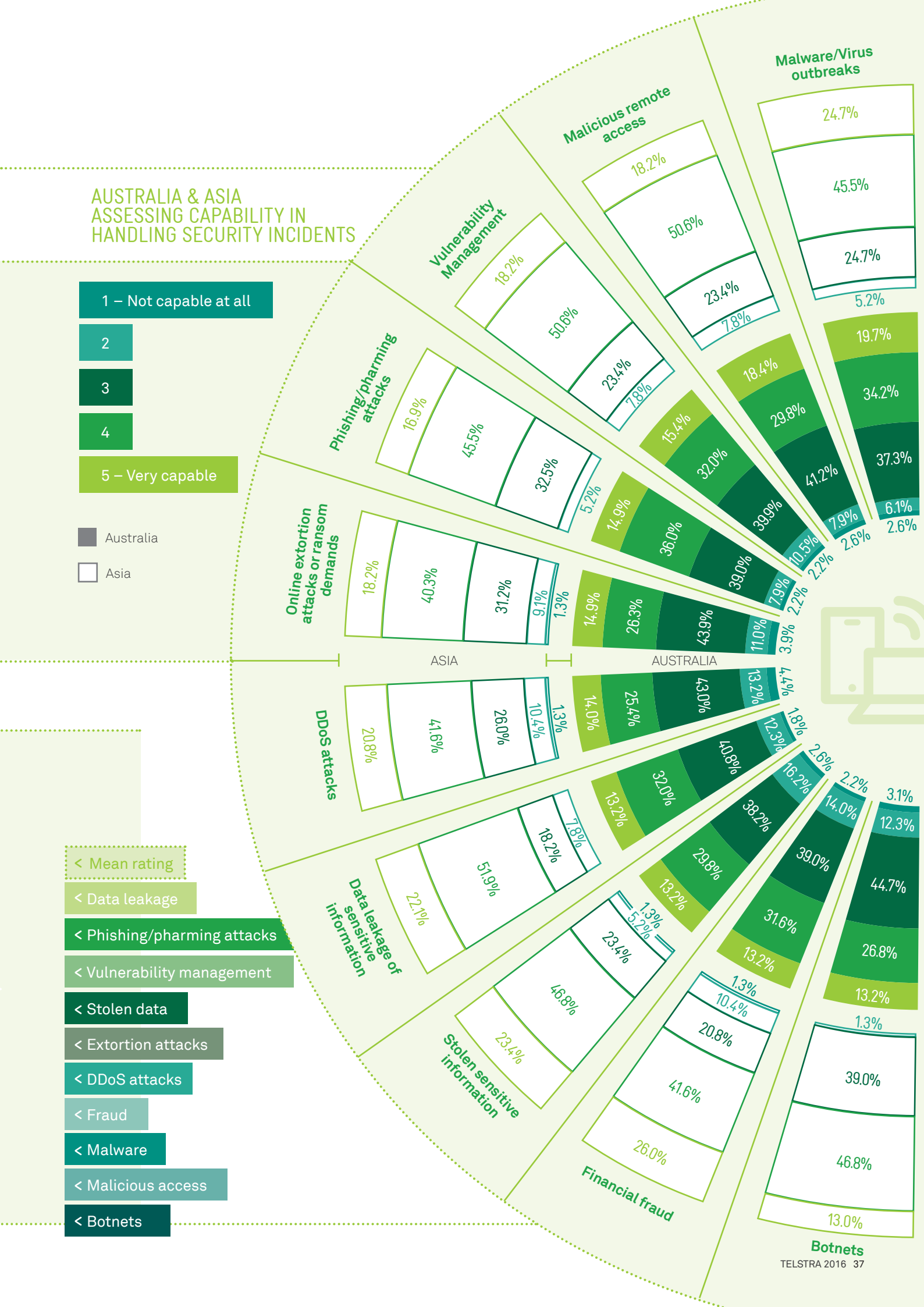
In comparison, most Asian organisations were confident in handling financial fraud which is likely to be based on their dedicated focus on processes, governance and internal controls. Indonesian and Hong Kong organisations were the most confident with their fraud mitigation capabilities.

An important correlation identified was that organisations which conduct security briefings more frequently or that attribute responsibility to C-level or business executives had a higher perceived level of capability in handling security incidents. The readiness of an organisation in handling a cyber incident and the way an organisation responds make a world of difference on how an organisation recovers from such an incident.

AUSTRALIAN CAPABILITY IN HANDLING SECURITY INCIDENTS



AUSTRALIA & ASIA ASSESSING CAPABILITY IN HANDLING SECURITY INCIDENTS

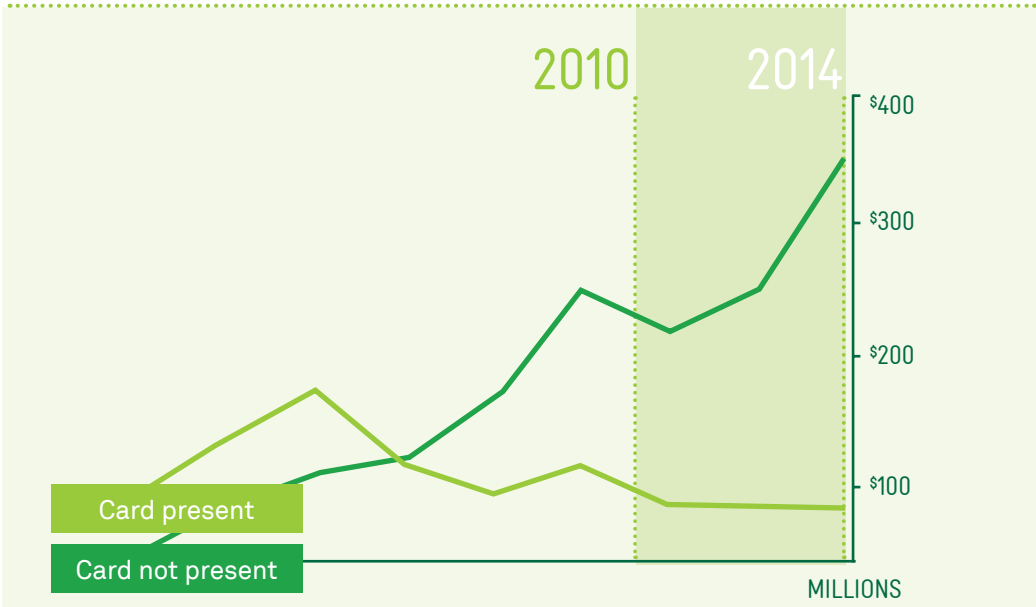


3.2 FREQUENCY OF SECURITY INCIDENTS

The frequency of business-interrupting security events has more than doubled in the past year: 23.7% of Australian organisations surveyed experienced a business-interrupting security incident in an average month in 2015, compared to 10% in 2014. The frequency of business-interrupting security events in Asian organisations was even higher at 45.5% in 2015. This aligns with a study performed by the Ponemon Institute and sponsored by HP, which shows the average annualised costs large Australian organisations incur when responding to cybercrime incidents were $4.85M US in FY 2015 compared to $4.29M US in FY 2014[4].

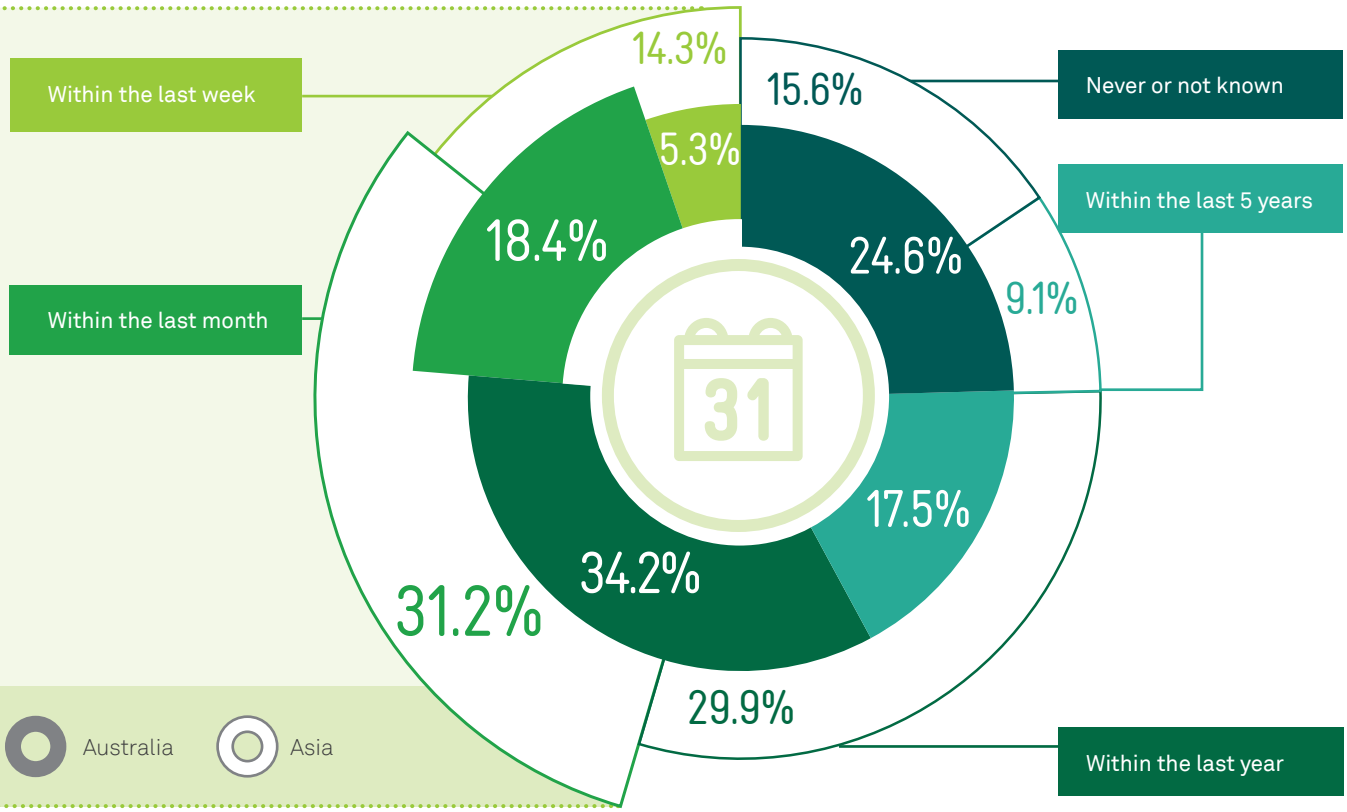
We found that retail organisations had the most reported incidents within the last year and this could largely be due to the value of online transactions via debit or credit cards having doubled in recent years compared to other transaction types including point-of-sale[5]. With the growth in alternate online payment methods, the number of targets from which cyber criminals can choose from has multiplied, paving the way for a 30% increase in fraud on debit, credit and charge cards from international credit card suppliers to $421 million in 2014.

AUSTRALIAN FRAUD ON CARD TRANSACTIONS[6]

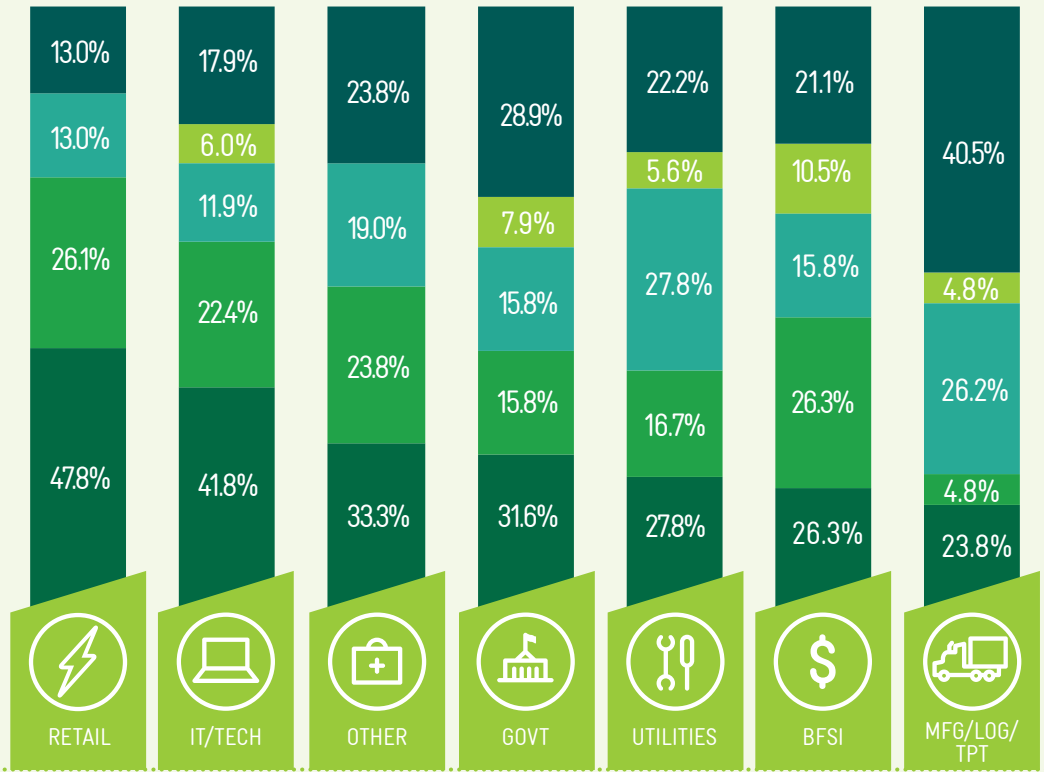


[4] https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5210enw.pdf (2015 Cost of Cyber crime Study: Australia)
[5] http://www.rba.gov.au/publications/annual-reports/psb/2015/retail-payments-developments.html
[6] Payments System Board Annual Report – 2015 (Reserve Bank of Australia)

AUSTRALIA & ASIA 2015
MOST RECENT OCCURRENCE OF A BUSINESS – IMPACTING SECURITY INCIDENT



AUSTRALIA BY VERTICAL IN 2015
MOST RECENT OCCURRENCE OF A BUSINESS-IMPACTING SECURITY INCIDENT



Malware outbreaks and human error were the most common cause of security incidents. Human error still remains a significant contributing factor to the causes of these security incidents. Human error isn't always malicious in nature; there is still a large amount of unintentional errors made by employees whether it is carelessness, lack of training, or the lack of awareness following corporate policies and procedures. Even the most capable organisations with strong security controls are still vulnerable to human error. Successful organisations not only focus on the technology and processes, but people as well. There is often too little investment made to the people aspect of security which can undermine other investments made by the company to protect its assets. Therefore a robust and ongoing security awareness training program for employees is a key component to safeguarding the organisation.

11% of respondents in Australia were still unsure of the cause of their latest security incident, which highlights the need not only to detect and respond, but fully understand the root cause of the incident so it can be successfully prevented from happening again. We found that organisations who do not investigate and determine the likely causes of past security events increase their likelihood of becoming the target of future attacks.

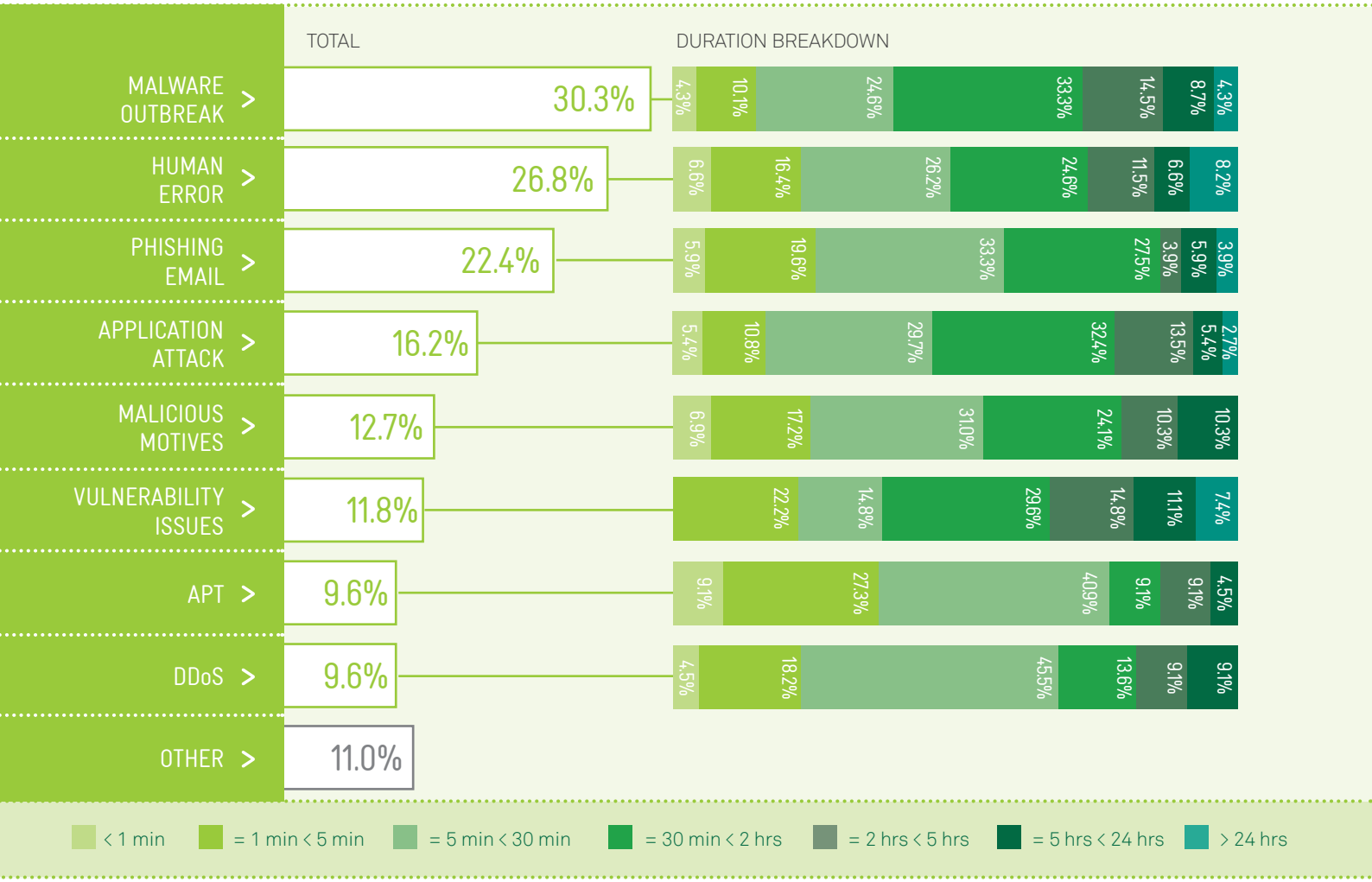
3 CRITICAL SUCCESS FACTORS OF NAVIGATING A CYBER INCIDENT

PLAN
When an incident occurs, having a plan in place makes all the difference

DECISION-MAKING
Get relevant information to people who can make risk-based decisions quickly

COMMUNICATION
Recognising key stakeholders and ensuring communication about the incident, response and recovery is vital

AUSTRALIA 2015
CAUSES AND DOWNTIME FOR SECURITY INCIDENT

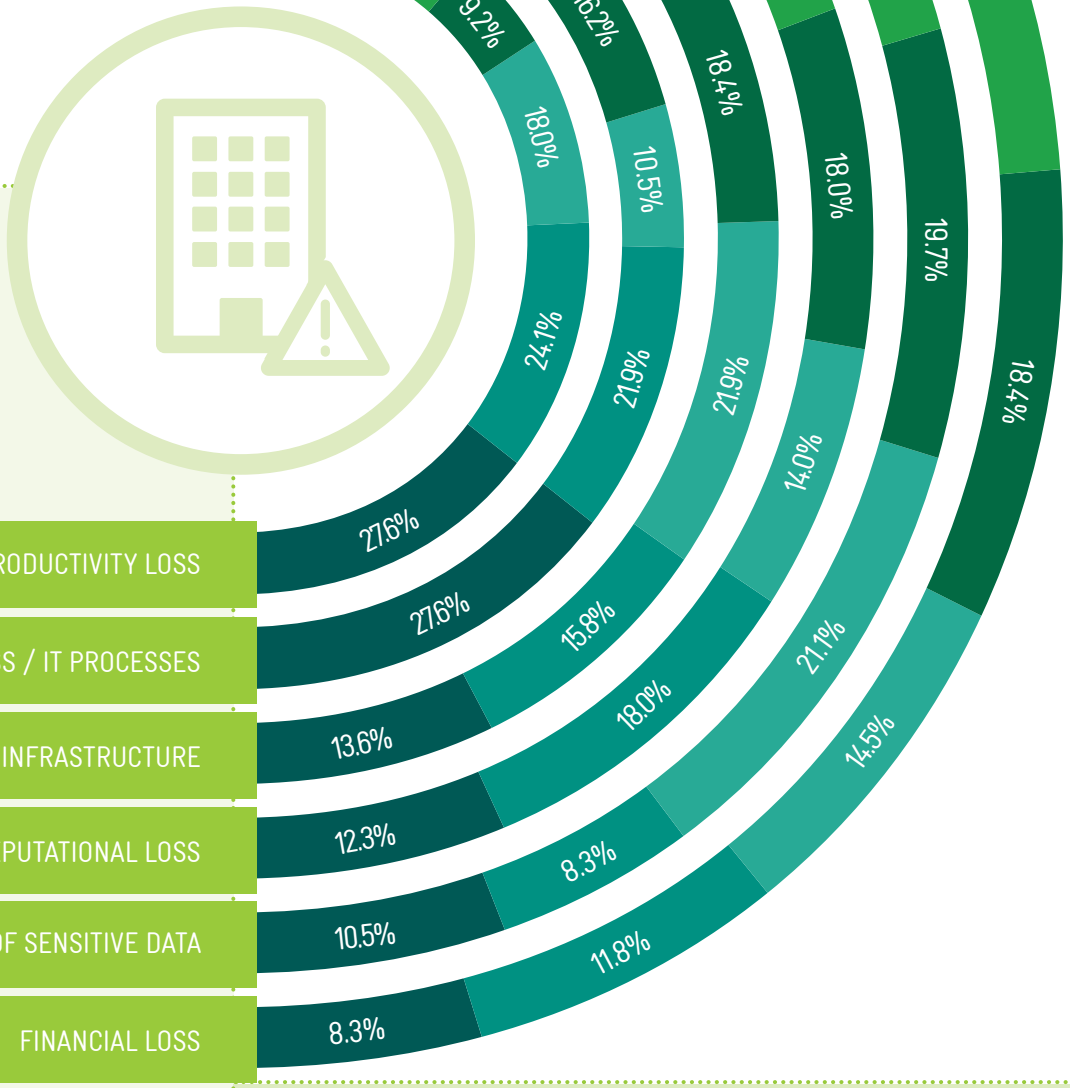


3.3 BUSINESS IMPACTS

IMPACT OF SECURITY INCIDENTS IN AUSTRALIA

The business impacts due to a security incident can range from being short lived and quickly contained, to complex and catastrophic. Impacts can range from damaging a company's brand and reputation to additional IT costs to repair and mitigate the threat, regulatory penalties and fines, business interruption costs and loss of revenue or intellectual property.

We asked respondents to rank the impact of security incidents from 1 to 6 (with 1 representing the highest impact to their organisation), and we found that both Australian and Asian organisations stated that productivity loss and disruption of business operations were the two highest impacts. Organisations in the Utilities and Government industries were the most affected by business disruption and productivity loss resulting from a security incident.



Rank the impact of security incidents from 1 to 6, with 1 representing the highest impact to their organisation:

Highest impact > 1 2 3 4 5 6 < Lowest impact

4.0 SECURITY DRIVERS AND INVESTMENT DECISIONS

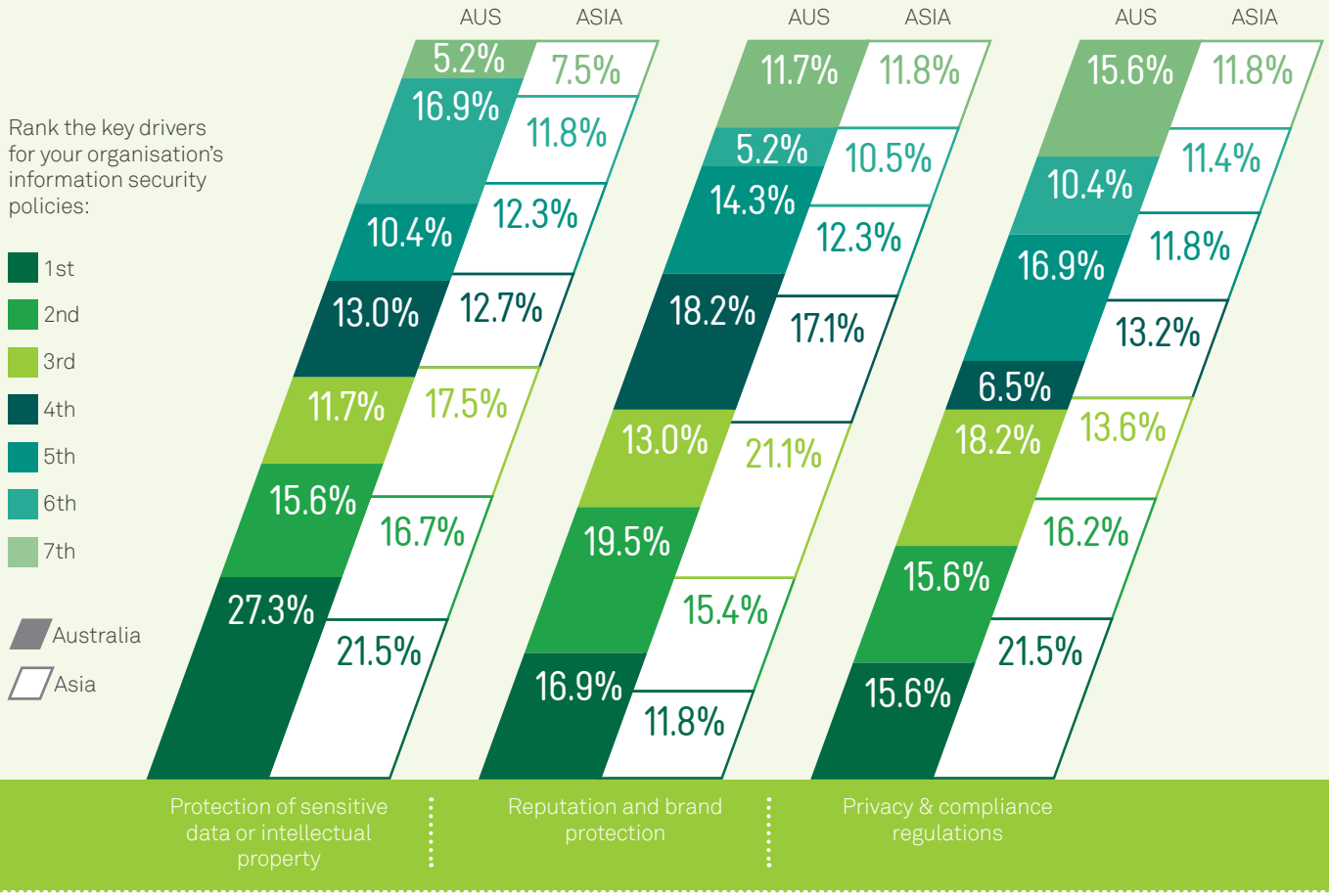
4.1 CYBER SECURITY DRIVERS

Our survey results show that protection of sensitive data and brand protection are the top ranked drivers of Australian respondents when it comes to information security policies. Privacy and compliance are the top drivers among all industries, with the exception of the Manufacturing, Logistics, Transport and Others industries, which identified Intellectual Property (IP) protection as the top driver.

Compliance and the protection of sensitive data are the top ranked drivers for Asian respondents. Among Asian countries, Indonesia ranks privacy and compliance as their highest drivers, and most Malaysian organisations cite protection of sensitive data and IP as their key drivers.

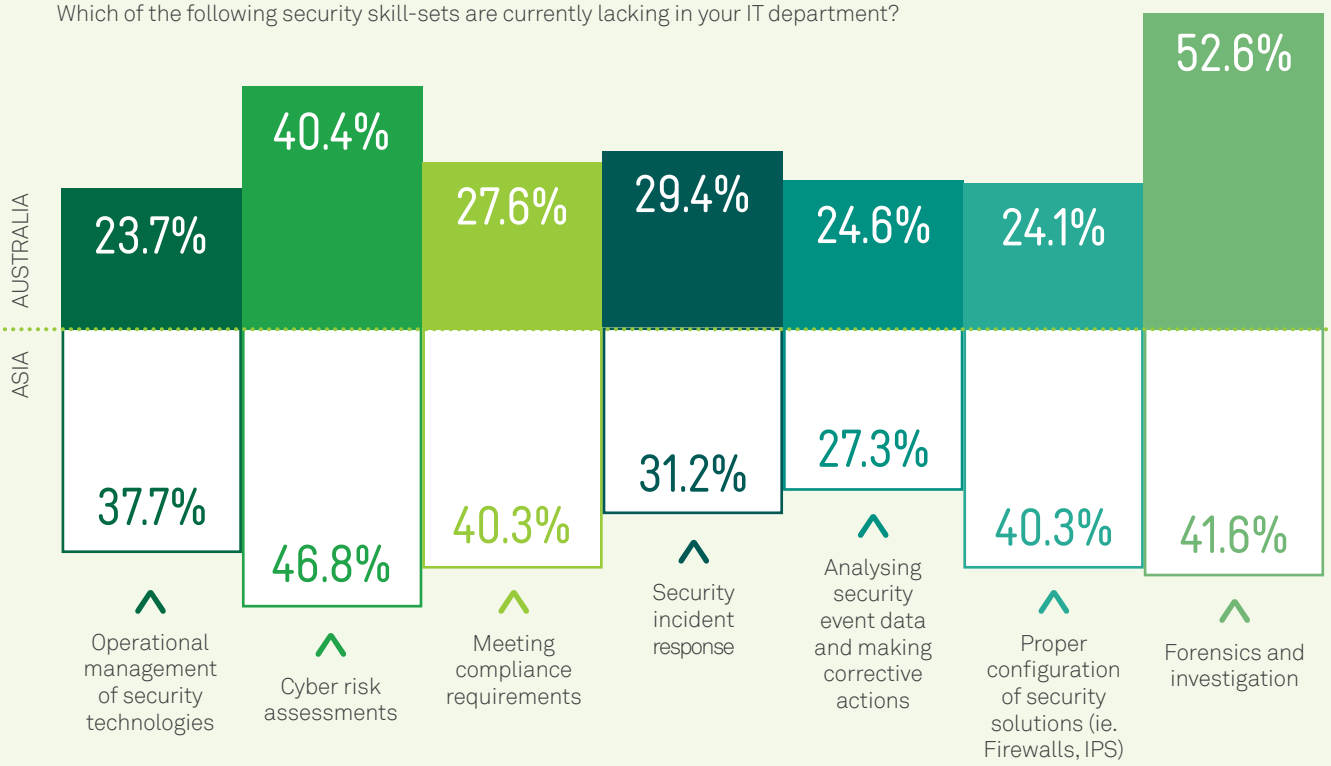
Cyber risk assessment and forensic investigative skills are in demand in both Australia and Asia. Security event analysis and corrective action were security skills which were most lacking in the Utilities sector whereas the IT/Tech and Retail sectors required more configuration skills for security controls.

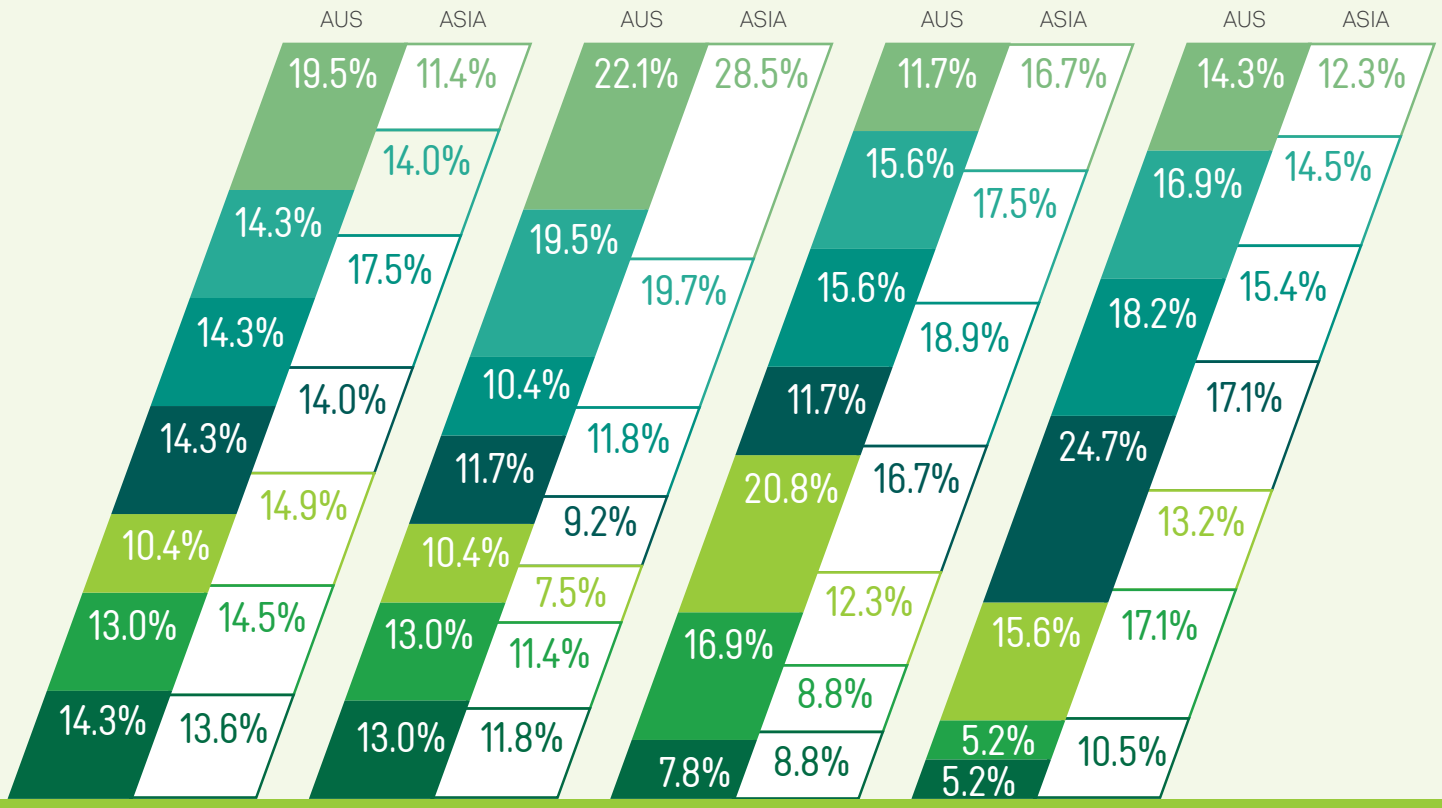
KEY DRIVERS FOR INFORMATION SECURITY POLICIES



SECURITY SKILL GAPS IN IT DEPARTMENTS

Which of the following security skill-sets are currently lacking in your IT department?





4.2
INVESTMENT DECISIONS

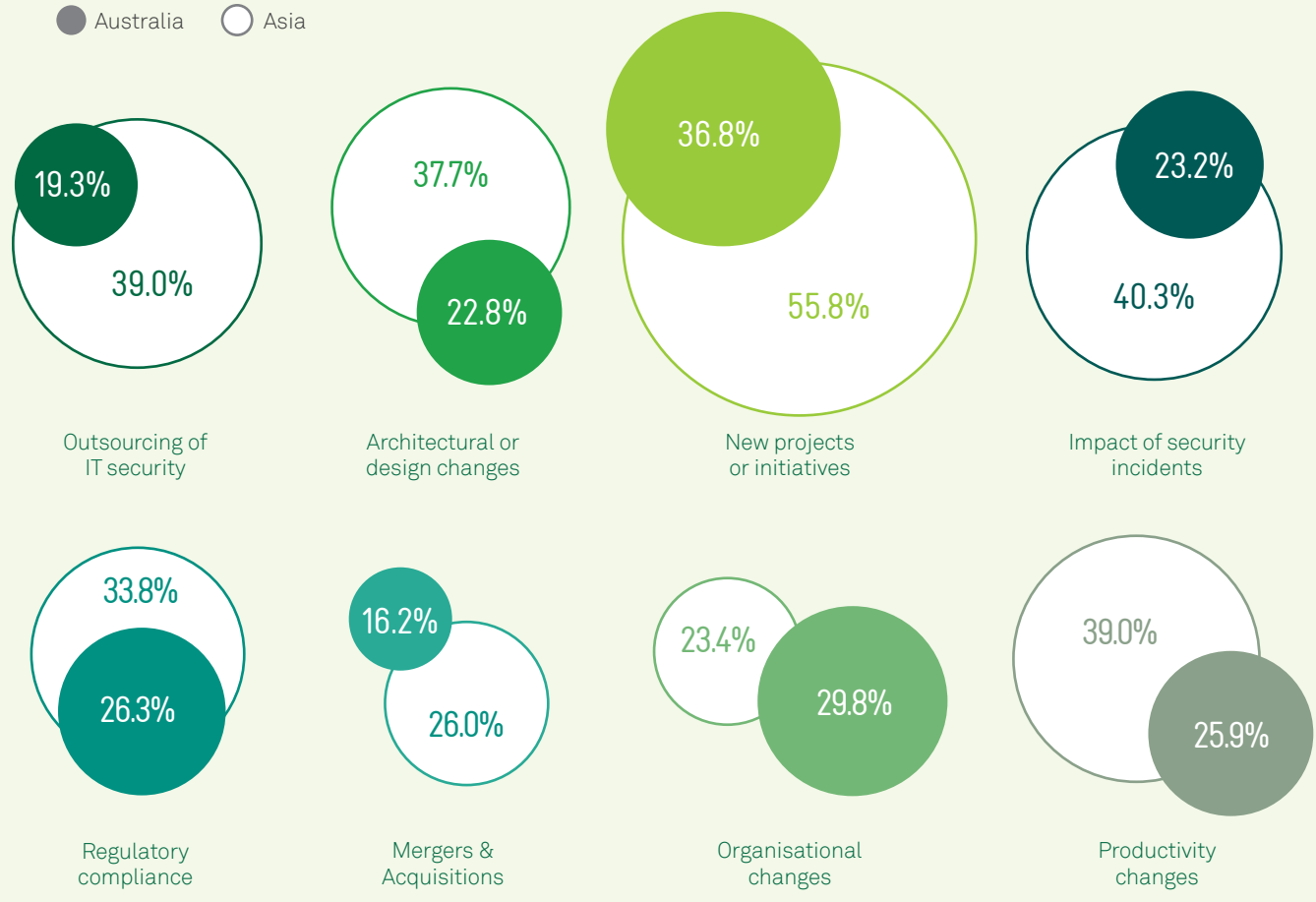
HIGH-PROFILE ATTACKS IN THE MEDIA SPUR SECURITY SPENDING AMONGST ORGANISATIONS

With greater media focus on cyber security over the past year, and reports of high-profile breaches, many Board members are asking questions about their information security readiness, and in response to this our research suggests that companies are boosting their security budgets. Our research indicates that 75% of Australian organisations are increasing their spend on IT security which is in contrast to the results in 2014, where the majority (60%) indicated their spending would remain the same. It is indicative of the growing importance enterprises are attributing to their IT security. Retail and IT/Tech industries are most likely to increase their spending by more than 25%.

Nearly all Asian organisations indicated that they would be increasing their spending on IT security (96%) with nearly 25% of respondents intending to increase their budgets by as much as 20%. This suggests that, while Asian companies have traditionally been behind the curve in implementing up-to-date information security practices, they now understand the risks and are investing accordingly. The data also suggests that those who deferred spending on security initiatives in previous years are now willing to spend as the focus on cyber security gains momentum.

Most organisations in both Australia and Asia indicated that the most decisive factor driving security spending was for new projects and initiatives with the exceptions of the Utilities and the Retail industry, which reported organisational and productivity changes as the key factors.

AUSTRALIA & ASIA – FACTORS INFLUENCING FUNDING CHANGES IN 2015



4.3
SECURITY TECHNOLOGY INVESTMENTS

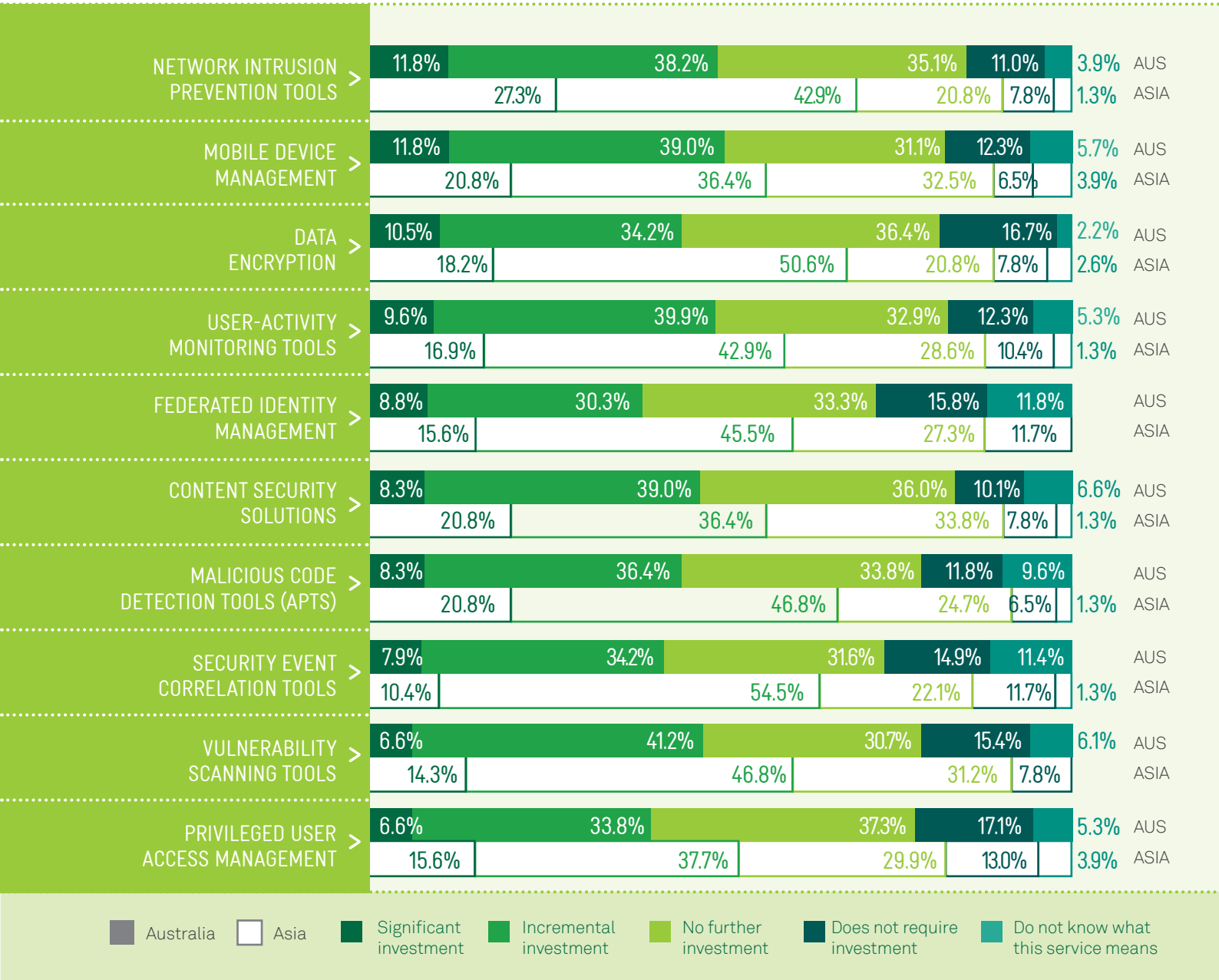
As technologies like cloud and mobile devices provide organisations an opportunity to transform the way they do business, companies are embracing new approaches to their cyber security. Where security was once viewed as an inhibitor, companies are now positioning it as a way to achieve competitive advantages.

Most Australian organisations increased their spending in cyber security capabilities and their top three investment technologies are network intrusion detection tools, mobile device management and data encryption.

The increased spending in mobility in Australia is not surprising with the rise of mobile malware and the increased use of mobiles for data connectivity. Australia's mobile data traffic is forecast to grow six-fold from 2014 to 2019, a compound annual growth rate of 41%[1]. It is expected to grow twice as fast as Australia's fixed IP traffic. Given Australia is an early adopter of mobile technology, our findings indicate a healthy level of investment by organisations in this domain.

Historically, organisations have focused on preventing incidents by spending money on technology such as firewalls and anti-virus software. However, many organisations are increasingly investing in entirely new areas to take advantage of emerging technologies and platforms. For example, Asian organisations increased their spending on new projects for APT tools and web/email content security solutions, driven by their knowledge of the latest attack landscape. The take up of cloud-based security services is also a key area for investment in Asian-based organisations.

INVESTMENT AREAS FOR 2016



[1] http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html

4.4
CYBER SECURITY INSURANCE

Hackers will continue to find new ways to circumvent cyber security safeguards. As a result, many businesses are purchasing cyber security insurance services to help shield their business from internet-based threats and mitigate the financial impact of cybercrimes. Coverage provided by cyber-insurance policies may include first-party coverage against losses such as extortion, theft, hacking, and denial-of-service attacks; liability coverage indemnifying companies for losses to others caused, for example, by errors and omissions, failure to safeguard data, or defamation; and other benefits including regular security audits, post-incident public relations and investigative expenses.

Cyber security insurance is one of the fastest-growing sectors in the insurance market and is predicted to grow to $10 billion in the next five to ten years[2]. However the industry remains in early stages of development; the inclusion and definition of these services is likely to change as the industry matures. Our research revealed that cyber insurance services are increasingly being purchased alongside existing IT security services and insurers are actively partnering with IT security companies to tailor their products for the same markets.

The levels of awareness and the readiness to purchase cyber insurance is generally low in Australia. Most Asian organisations indicated they are likely to purchase cyber insurance soon, or had already purchased. In comparison, most Australian organisations indicated they were unlikely to purchase cyber insurance in the near future. More than 50% of Australian government agencies were not looking into cyber insurance, in contrast to the IT/Tech and BFSI industries, where the majority had purchased or would consider purchasing soon. Industries such as Utilities and Retail expressed relatively strong interest in cyber security insurance, but indicated that they would require more help in complying with the necessary requirements. Our research found that 10.8% of Australian organisations indicated they where interested in purchasing cyber insurance, but were unsure how to go about it.

> CONSIDERATIONS

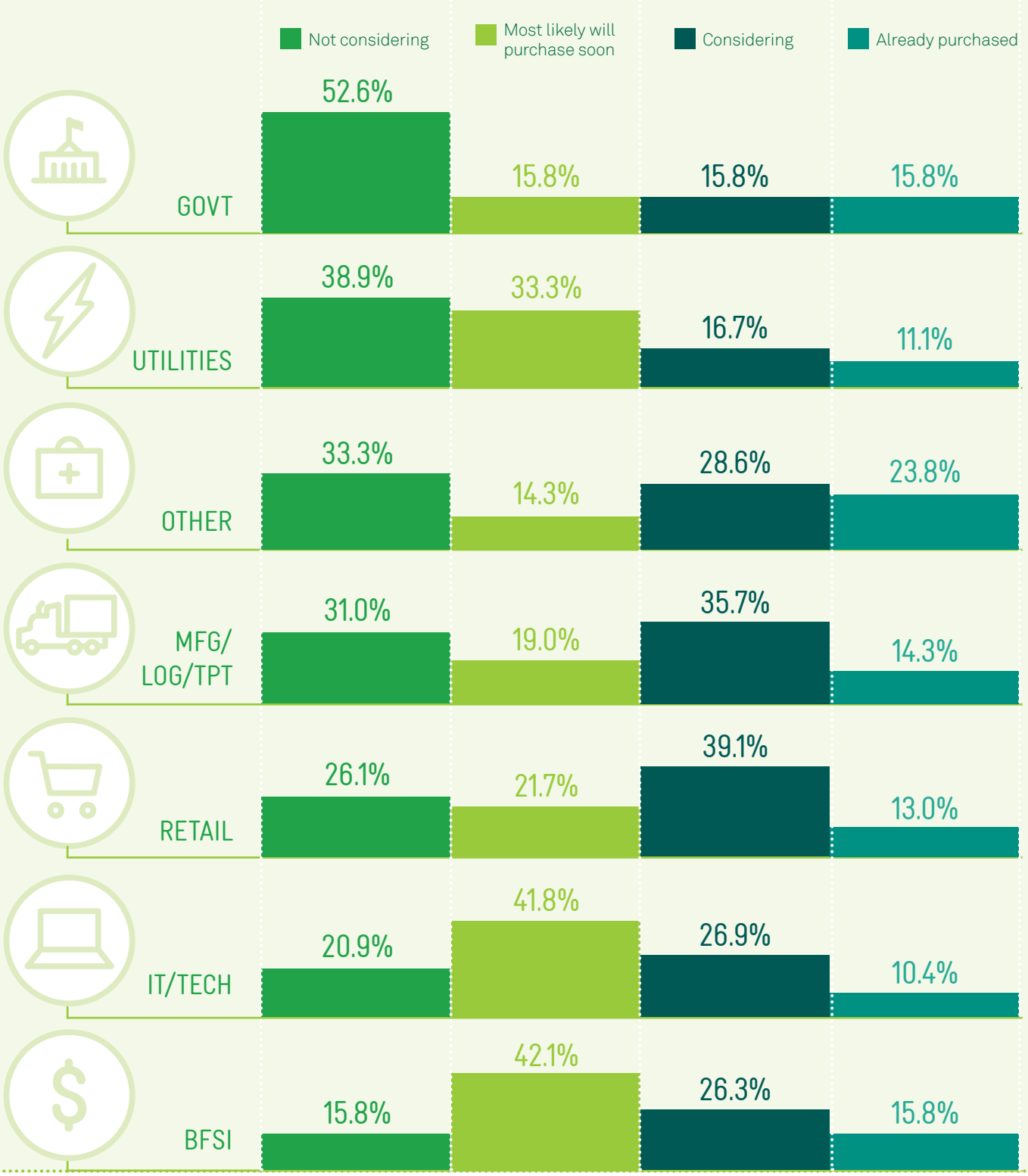
Ensure that your cyber insurance policy covers full cost of a data breach to include: brand and reputation damages, PR cost, investigations, incident response, IT infrastructure repairs, defence and legal fees, regulatory penalties and fines, bankruptcy, business interruption and loss of revenue, ransom and electronic blackmail costs

In most cases, Commercial General Liability insurance excludes cyber liability arising out of social networking and social media

Ensure that you have the appropriate security controls, audits, regular assessments and regular scheduled penetration and vulnerability scan testing in place to meet cyber insurance policy requirements, not just initially, but ongoing

[2] Veysey, Sarah (June 10, 2015). "Data scarce for insurers covering cyber risks". Business Insurance. Retrieved June 11, 2015

PURCHASING BEHAVIOUR CYBER SECURITY INSURANCE IN AUSTRALIA BY VERTICAL



5.0 GLOBAL SECURITY CHALLENGES AND APPROACHES

A BOOMING ECONOMY CREATES A CYBER SECURITY CHALLENGE FOR ASIAN ORGANISATIONS

The Asia Pacific region is seen by investors and businesses as the driving force for growth in the world economy. It is home to some of the world's largest fastest growing economies as well as some of the most impoverished.

China, India and Indonesia are considered the largest growing economies and key emerging markets with large populations to match their economic growth. ICT technology usage, e-commerce and social media adoption is growing significantly in these regions but there are challenges which need to be overcome to ensure they achieve a healthy digital economy. These countries are dealing with major structural shifts moving away from an export-orientated economy to a more balanced trade economy; they have limited infrastructure/accessibility especially in rural areas and limited engagement between businesses and government which limits their legal and technical capabilities to combat cybercrime[1].

Malaysia, Philippines and Thailand are also considered as emerging markets investing in the growth of digital infrastructure due to their high adoption of mobiles and social media in the growing younger generations.

Australia, Japan, Singapore and South Korea are among the most digitally-advanced economies within the Asia Pacific region. They are not expected to experience the same dynamic growth as the emerging markets but they are considered to have highly developed infrastructure, digitised business communities, consumers and governments.

Whatever part of the world multinational corporations operate in, they face significant cultural and legal challenges when dealing with security across international borders. We believe there is an opportunity for companies in APAC to obtain a competitive advantage by leading the development of effective, holistic organisational cultures and postures to combat growing cyber threats.

5.1 GLOBAL SECURITY CHALLENGES FOR ASIA-PACIFIC MULTINATIONALS

CYBER-ATTACKS KNOW NO BOUNDARIES

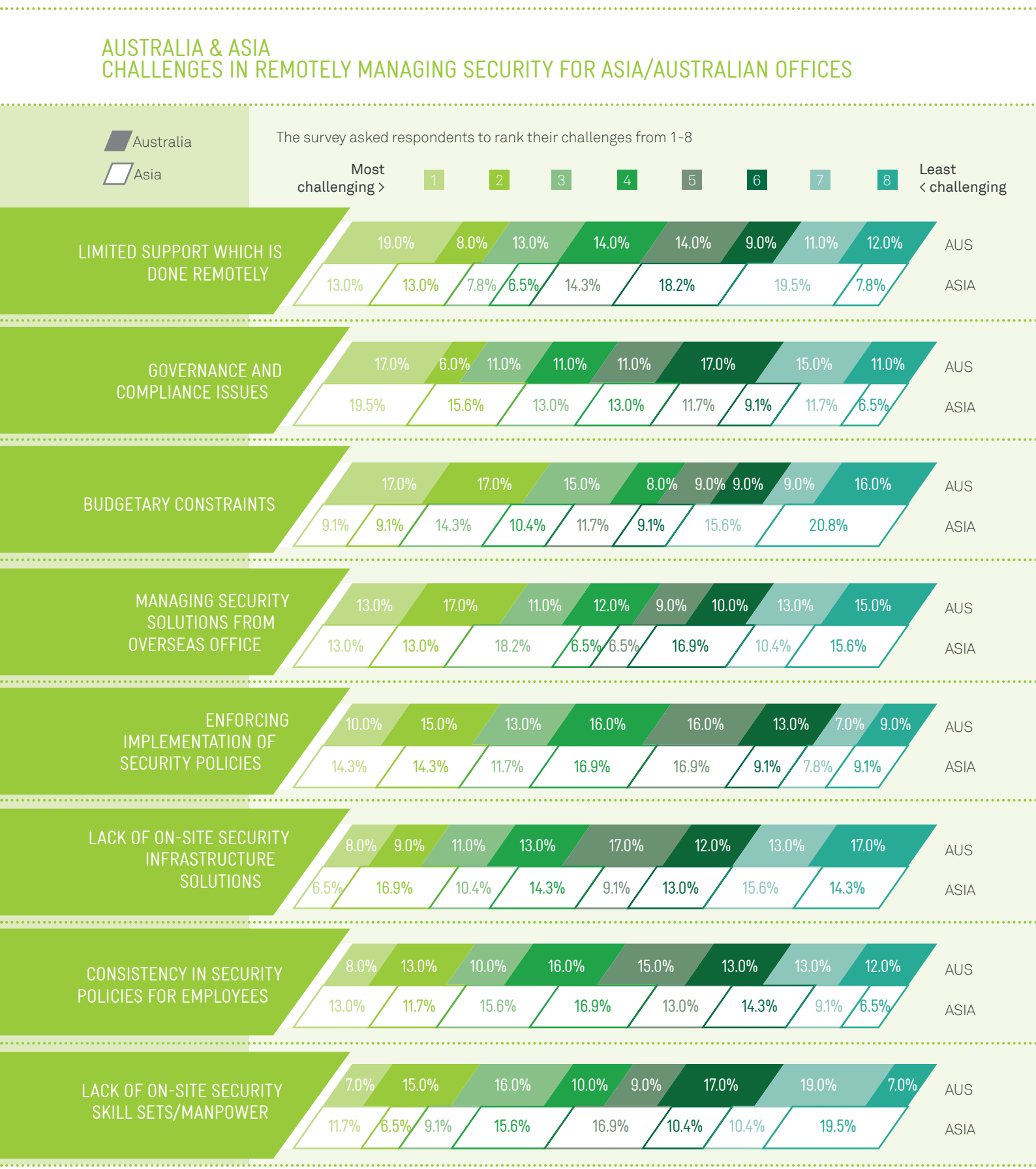
We surveyed 228 Australian organisations with their headquarters in Australia and of these, 130 indicated that they have APAC-based offices. Of these 130, 77% have responsibilities in handling security in their offices outside of Australia.

We investigated how global organisations managed their remote offices within the region and the key challenges they faced. The top three challenges experienced by Australian organisations who remotely managed APAC offices were limited support for remote locations, difficulties with meeting governance/compliance regulations and budgetary constraints.

The top three challenges experienced by Asian organisations that remotely managed Australian offices were difficulties with meeting governance/compliance regulations, enforcement of their security policies and limited support for remote locations. The fast-growing Asian market is increasingly a target for advanced persistent threats due to the presence of more multinational companies (MNCs) and big local brands in the region. These companies often present as a lucrative target because they may not be as well protected as organisations in more mature markets.

[1] https://www.aspi.org.au/publications/cyber-maturity-in-the-asia-pacific-region-2014

AUSTRALIA & ASIA
CHALLENGES IN REMOTELY MANAGING SECURITY FOR ASIA/AUSTRALIAN OFFICES



5.2
GLOBAL SECURITY METHODOLOGIES

More than half of multinational organisations across Australia and Asia have adopted a centralised approach to storing and managing critical information, and this trend is likely to continue. Coordinating and implementing security policies across a number of countries is a challenging task. Apart from the technological and regulatory challenges, there are also cross-cultural communication challenges.

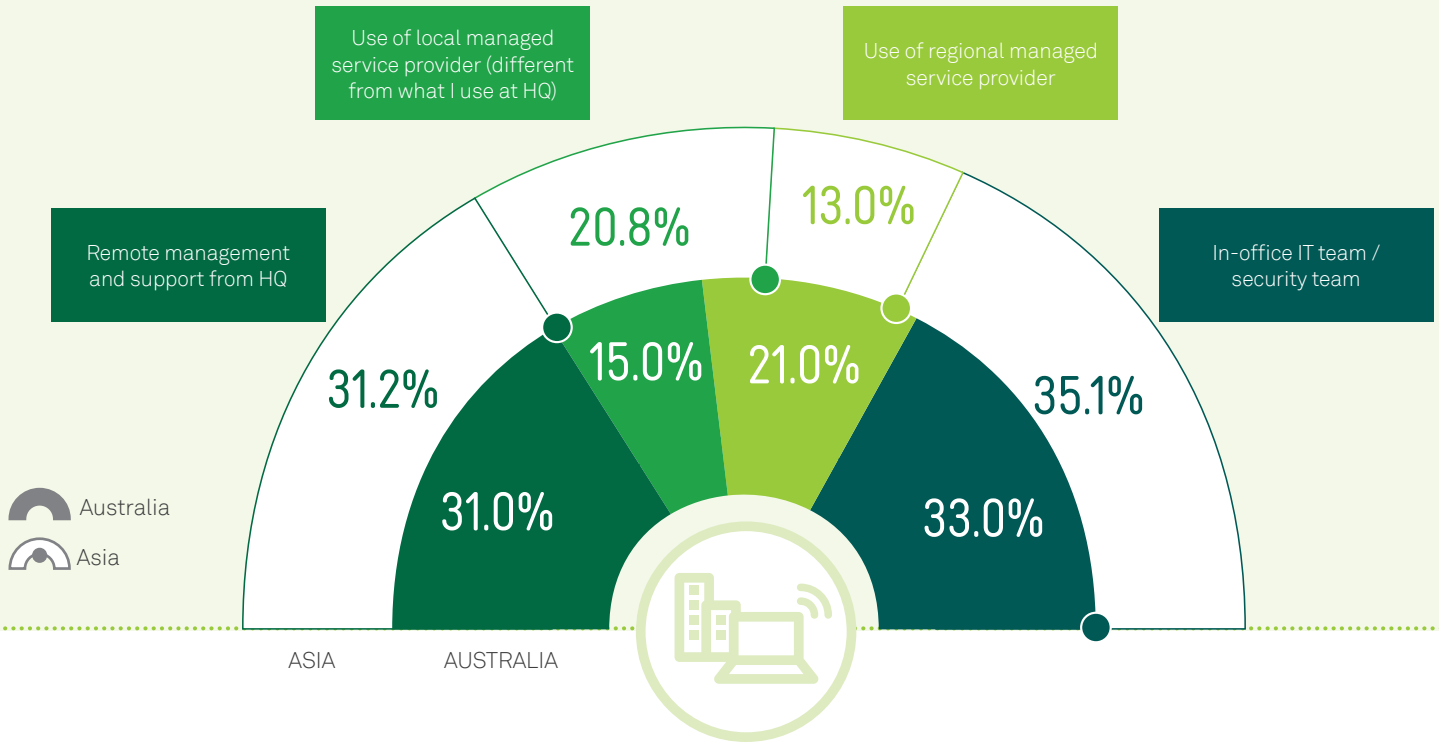
The main benefits for a centralised approach are the efficiencies an organisation can achieve through standardising and centralising systems, locations using compatible systems that are in turn easier to manage, which limits the requirements for many skilled resources to support many disparate systems and would make it easier to offer and maintain a consistent level of services for employees and customers.

The BFSI industry was more likely to adopt decentralised (over 21%) or federation (over 31%) deployments for their critical data management. Corporate policies may be the same globally for these organisations, but the environment in which organisations operate is different. Local regulators and government policies are different between locales and require a greater need to tailor security architectures for different countries within the region.

To help overcome this, organisations are avoiding duplicating communications with different integrators in each country by enlisting the help of one security provider globally.

Managing security is another challenge. Around a third of Asia Pacific organisations use their in-office teams to manage day-to-day security issues. To manage an overseas office, Asian organisations were more likely to use their local service provider rather than a remote service provider. Australian organisations, however, were more likely to use a regional managed service provider than a local service provider. The highest usage of managed service providers came from the Government, BFSI and IT/Tech industries. In contrast, the Utilities and 'Others' industries were more likely to rely on internal resources, such as remote management, support from HQ or an in-house IT/security team.

METHODS FOR REMOTELY MANAGING SECURITY IN OVERSEAS OFFICES



5.3
INCREASING THIRD-PARTY THREATS

DATA BREACHES OFTEN START WITH THE COMPROMISE OF SUPPLIERS, CONTRACTORS AND VENDORS

In the past few years, several large retailers have disclosed costly breaches. In 2014, Home Depot experienced the exposure of 56 million credit card details and customers email addresses[2]. In this case, cyber criminals used a third-party supplier login details to gain access to the Home Depot network which allowed them to deploy custom-built malware on its self-checkout systems to obtain credit card information. This attack was cited to be similar to the U.S based retail giant, Target, in which criminals gained unauthorised access via a third party supplier in 2014[2].

As organisations share data with a widening array of interconnected business partners, supply chains, and contractors, it is essential that they carefully assess the security capabilities of these third parties.

These companies typically have their own IT systems, processes, methodologies and security systems protecting data and information of their customers. Therefore it is critical that organisations hold the same high standards for third parties when it comes to data security. This becomes especially important in regulated environments like Healthcare, Finance, or Insurance – where data breaches are costly and the information is seen as high value to cyber criminals.

As more data is shared through connected business ecosystems, more data is at risk of exposure.

Our research found that there is still a concerning amount of organisations not evaluating the security risks and implications third-party business partners might have on their organisation. 15% of Australian organisations and 26% of Asia Pacific organisations do not perform any audits on their partners or suppliers. Cyber criminals target the weakest entry points into an organisation, which recent trends suggest is increasingly via third-party business partners who have not adequately secured their data.

Due diligence of third-party and supply chain partners must be a critical component of an organisation's overall cyber security program.

While Australian organisations use a variety of methods to evaluate the cyber risk of third-party suppliers, our findings suggest there is still room for improvement given organisations were under represented in the use of any one of these control methods.

Retail, Government, Utilities and BSFI industries tended to do better at implementing technology related security controls for third parties rather than audits or contractual measures. In essence, there should always be a multi-layered approach to security and the risk management of third parties is no different.

Given large organisations may have thousands of vendors that have access to their systems and data, a tiered approach to assessment is required. A tiered framework manages third-party partners based on the risks they present to the business and allows organisations to hold third parties to different levels of accountability. For instance, organisations that share sensitive customer information with external partners should ensure that they adhere to the very highest level of security, while those partners that have access to less sensitive information may not need be held to the most rigorous of standards.

[2] http://www.infosecurity-magazine.com/news/home-depot-breach-third-party/

AUSTRALIA & ASIA MANAGING SECURITY RISKS WITH YOUR BUSINESS SUPPLIERS AND PARTNERS

> DO NOT PERFORM VENDOR CHECKS

AUS 15.4% ASIA 26.0%

> ENGAGE THIRD-PARTY TO PERFORM AUDIT OF VENDOR

AUS 34.6% ASIA 57.1%

> PERFORM RANDOM SPOT CHECKS OF VENDOR SITES

AUS 21.9% ASIA 49.4%

> APPLY ACCESS CONTROLS TO SYSTEMS AND DATA

AUS 46.9% ASIA 70.1%

> ADDRESS INFORMATION SECURITY ISSUES VIA CONTRACT

AUS 36.4% ASIA 50.6%

The following key principles should be in place for third-party partners:

- Perform risk assessments on third-party vendors at least once a year or when there is a major change in the operating model with them
- Perform regular audits on your systems and networks that third parties have access to. Keep an up-to-date inventory of all third parties that handle sensitive data or information
- Audit and categorise the important data within your organisation to ensure that you are managing the protection of this data from end to end use of it (i.e. collection, transport, storage, backup and restore)
- Establish security standards and policies for external third parties and ensure that these are covered in commercial contracts. They should cover privacy and any other government legislation or regulations that you are required to comply with
- Clearly define the security roles and responsibilities and ensure that system access is limited to ensure appropriate constraints and access privileges are in place across all your employees, contractors and third-party access
- Have an incident response process in place to report and handle breaches to and from third parties
- Ensure your network security architecture is segmented to ensure appropriate separation between your public internet, email and web-based services and your internal network that contains critical data and assets
- Layer your security system defences so that you are not relying on a single security system to protect your network and ensure you are using strong user authentication and strong encryption protocols when accessing or moving sensitive data

6.0 SUMMARY

ORGANISATIONS NEED TO BETTER IDENTIFY AND PROTECT THEIR IMPORTANT DATA ASSETS FROM THE MULTIPLE AND VARIED SECURITY THREATS ONLINE

Organisations and individuals are dealing with increasing security challenges and risks, many of which are fuelled by an organisation's adoption of mobility and cloud-based services which are enablers to the way people want to work and interact. Many business leaders told us they are ready to adopt technologies such as cloud computing and big data, or increase their use of mobile technology. Those leaders also recognised that doing so would necessitate increased spending on, and attention to, information security solutions.

Organisations of all sizes are facing an evolving cyber security landscape where threats can be instigated from a number of sources. Typical threats which were prominent in the past year included the use of phishing emails, the rise in the use of exploit kit-based malware, the increase of malware hosted in Australia, and the impact ransomware-based attacks have had in Australia.

We learned that organisations are still struggling with Shadow IT-associated risks, with many not having a high degree of awareness or the necessary skill-sets to address the potential exposure of sensitive corporate data from this. This is made more difficult by finding the right balance between supporting the adoption of unsanctioned SaaS applications while addressing the security risk.

As Australian organisations grow their businesses globally and begin to share data with a widening array of interconnected business partners, supply chains, and contractors, our research found that many organisations acknowledged the need for improvement to ensure the right level of controls and processes are put in place to minimise the risk that these third parties might bring.

The good news is that our research indicates that there is a heightened cyber security awareness among Board members and C-level executives and they recognise the need to have an effective security plan in place and execute the plan to minimise the business exposure to security-related incidents. The majority of organisations have increased funding to implement new initiatives to better detect, prevent, mitigate, and improve their overall information security capabilities.

While implementing security controls is critical to protect an organisation from cyber threats, our findings show that a large number of incidents are still caused by human error which highlights the need to address the human aspects of the risks equation. Moreover, recent public breaches have consistently demonstrated that people are often the weakest link when it comes to cyber security. Therefore, a key component which is often missed is the staff education and awareness of the value of the data in your organisation. It is good practice to take a balanced approach between people, process and technology to manage security risks and protect the valuable data in your organisation.

Telstra's approach to effectively manage your risk is by asking your organisation a number of simple questions which helps frame the complex problem of cyber security in a way that everyone can engage in, from senior executives right through to all staff.

THE FIVE THINGS YOU MUST KNOW TO EFFECTIVELY MANAGE THE RISK

The Five Knows of Cyber Security represents a significant shift in focus - from a technology discussion to one where senior management can engage in and contribute to the effective management of cyber security risk.

KNOW THE VALUE OF YOUR DATA

You need to know what value it has, not just for your organisation and customers but also the value to those who may wish to steal it. All data has value to someone

KNOW WHO HAS ACCESS TO YOUR DATA

You need to know who has access both within an organisation and externally, like who has 'super user' admin rights in your organisation and within your trusted partners and vendors

KNOW WHERE YOUR DATA IS

You need to know where your data is stored. Is it with a service provider? Have they provided your data to other third parties? Is it onshore, off-shore or in a cloud?

KNOW WHO IS PROTECTING YOUR DATA

You need to know who is protecting your valuable data. What operational security processes are in place? Where are they? Can you contact them if you need to?

KNOW HOW WELL YOUR DATA IS PROTECTED

You need to know what your security professionals are doing to protect your data 24/7. Is your data being adequately protected by your employees, business partners and third-party vendors who have access to it?

ACKNOWLEDGEMENTS

TELSTRA CONTRIBUTIONS

Telstra Security Practice

Telstra IP Data and Security Solutions

Telstra Security Operations

Telstra Transport and Routing Engineering

Telstra Corporate Communications & General Counsel

Telstra Marketing

ABOUT TELSTRA SECURITY SERVICES

Managed Security Solutions

- As more security technologies are deployed within organisations, their monitoring and management becomes increasingly complex. To assist with this, Telstra can provide a suite of Managed Security Services that can supplement an organisation's internal capabilities.
- An integral part of this offering is the Telstra Security Operations Centre (TSOC), a dedicated monitoring facility that operates 24 hours a day, 365 days a year to detect malicious activity and help ensure ICT resources are not compromised.
- The TSOC, a government-classified (T4) facility, provides an integrated approach to security for customers. Monitoring activities are fully integrated with Telstra's Global Operations Centre (GOC) which provides service monitoring across the Telstra core networks, and the Managed Network Operations Centre (MNOC) for customer network environments.
- By providing security monitoring across both customer and Telstra's core networks, the Security Response Centre team is able to preempt threats and escalate major issues to Telstra's Computer Emergency Response Team (T-CERT) as required.

Consultancy Services

- Telstra's teams of security experts have been involved in the design, build and management of some of the largest and most complex networks in the country. This real-world experience means they understand the challenges faced by organisations and are well placed to provide advice and guidance on all security-related issues.
- Telstra Consulting works with organisations across multiple sectors including Government, Finance, Utilities, Transport and Manufacturing. Each has different security needs, and Telstra Consulting experts are well placed to deliver the type and extent of support that is required.

For More Information

We can assist your organisation to meet your increasingly sophisticated security requirements. For more information contact your Telstra Account Executive or visit: **https://www.telstra.com.au/business-enterprise/solutions/security-services** for additional information about our security services.

TELSTRA PARTNER CONTRIBUTIONS

FROST & SULLIVAN

Akamai

Check Point SOFTWARE TECHNOLOGIES LTD.

CISCO

elastica A Blue Coat Company

FIRSTWAVE Cloud Technology

IMPERVA INCAPSULA

intel Security

paloalto NETWORKS

QUALYS ON DEMAND SECURITY

AS AUSTRALIAN ORGANISATIONS EXPAND GLOBALLY AND SHARE DATA WITH A WIDENING ARRAY OF PARTNERS, SUPPLY CHAINS, AND CONTRACTORS, RESEARCH FOUND THAT MANY ACKNOWLEDGED THE NEED FOR IMPROVED CONTROLS AND PROCESSES TO MINIMISE THE RISK THESE THIRD PARTIES MIGHT INTRODUCE.

IT'S HOW
WE CONNECT

visit a Telstra store
your Telstra Account Executive
telstra.com.au/business-enterprise/solutions/security-services