# Telstra Cyber Security Report 2017

Managing risk
in a digital world.

# Executive summary

Organisations and individuals are dealing with new security and business opportunities, many of which are fuelled by mobility, cloud based service offerings and the need to have an environment that adapts to the way people and organisations want to work and interact. In order to capitalise on those opportunities, cyber security risk must be managed to acceptable levels. Every organisation must determine for itself what constitutes an acceptable level of risk.

The insights shared in this report are based on our understanding of the security risks that organisations face in the Asia Pacific region. We hope that it offers useful guidance on identifying and managing risk, and improve your awareness in the field of information security. These insights aim to support your organisation as it strives to make vital decisions about security and its operational impact. It is important that those decisions are well-informed as good information security is now critical to the success of any modern organisation.

Some of the findings are sobering: we learned that 59 per cent of organisations in Australia have detected a business interrupting security breach on at least a monthly basis, which is more than twice as often compared to 2015 (24 per cent). The findings aligned with Asian businesses who also experienced an incident on at least a monthly basis, as reported by 59 per cent of respondents.

We found that ransomware was the number one type of malware downloaded in the Asia Pacific region, with 60 per cent of Australian organisations stating that they experienced at least one ransomware incident in the last 12 months. Of the organisations who experienced a ransomware incident, 57 per cent paid the ransom. Our research found that nearly one in three of the organisations who paid a ransom did not recover their files. This clearly dispels the myth held by a number of people that there is "honour among thieves" in that if you pay a ransom, the criminals will unlock your files and leave you alone. You really are rolling the dice if you choose to pay a ransom and your chances aren't good. This problem is of particular importance to small- to medium-sized organisations as they are less likely than large organisations to have extensive security controls and to back up their data.

We also found that C-level executives are taking a greater level of responsibility in security initiatives such as education and the sponsorship of security improvement programs. Two out of three C-level executives have a high or very high involvement in their organisation's cyber security initiatives in Australia and Asia. This may well be due to the finding that C-level executives are being held to account more often in the event of a security incident. The recently passed amendments to the Australian Privacy Act, affecting most organisations and requiring data breach notifications to both the victims and the Privacy Commissioner, will drive further awareness and accountability, as did the first legislation of this kind when it was introduced in California in 2003.

The rapid adoption of cloud services, while delivering significant agility and portability benefits, continues to present a security challenge. More than half of Australian organisations that adopted cloud services see data theft as their number one risk in doing so; yet more than 30 per cent of those organisations adopting cloud services reported that they are not yet ready to handle this risk in Australia. That organisations are prepared to take such acknowledged risks speaks to the urgency of their move to cloud services.

The heightened awareness of security breaches and the business impacts of these incident's has led to increased IT security spend, with 95 per cent of organisations in Asia increasing their budget this year compared with 81 per cent in Australia. Last year we reported an increase in the IT security budget for 75 per cent of Australian organisations, which demonstrates a continued increase in importance of information security to organisations.

That finding is a welcome one, because taking advantage of new technologies requires a willingness to invest in people, processes and technology appropriate for today's information security environment.

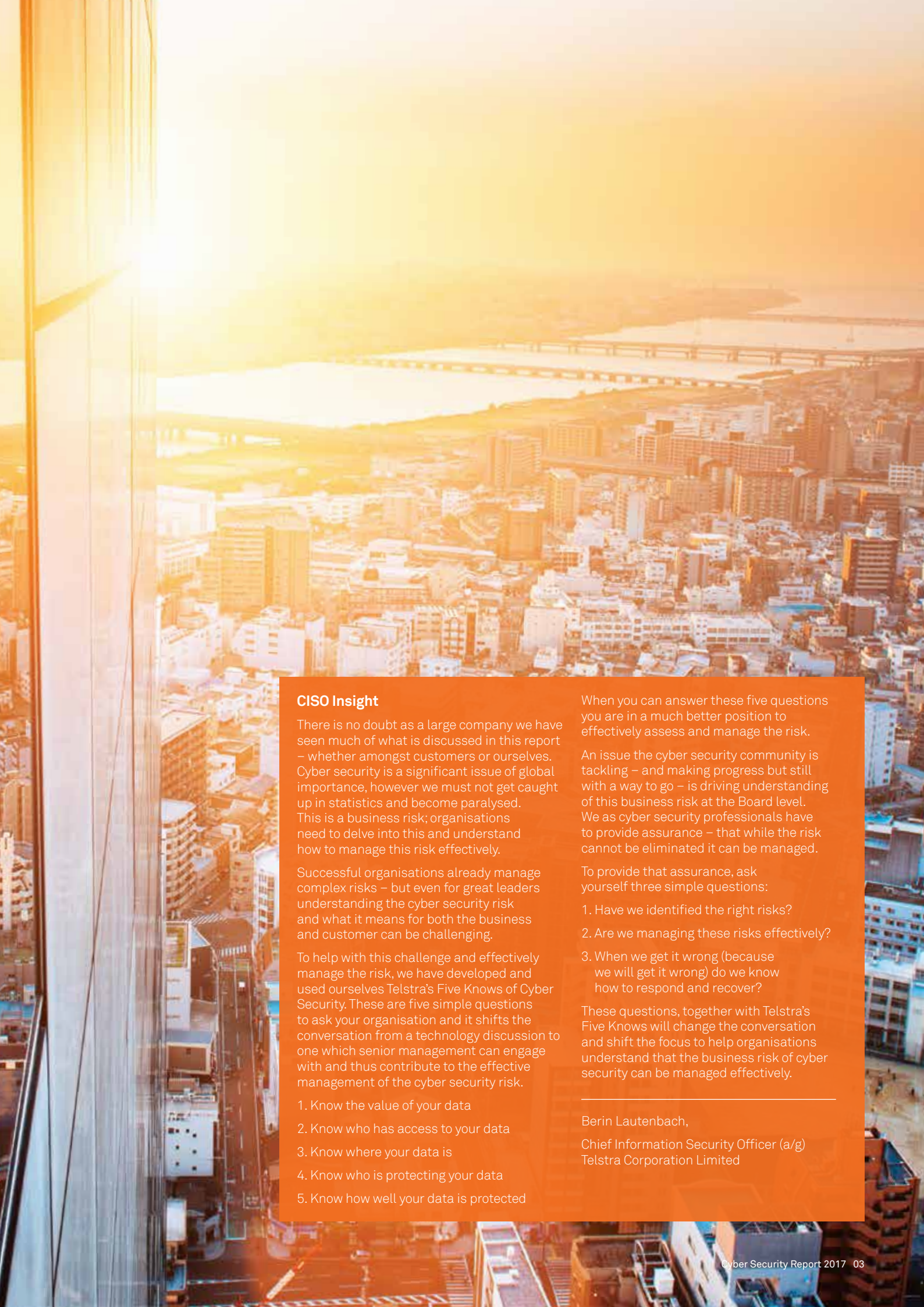
It is our hope that this report supports your organisation's increased focus, as it is designed to help you to understand the threats you face and the actions you can undertake to better secure your organisation and its success.

**Neil Campbell,**

Director, Global Security Solutions
Telstra Corporation Limited

**Berin Lautenbach,**

Chief Information Security Officer (a/g)
Telstra Corporation Limited



## CISO Insight

There is no doubt as a large company we have seen much of what is discussed in this report – whether amongst customers or ourselves. Cyber security is a significant issue of global importance, however we must not get caught up in statistics and become paralysed. This is a business risk; organisations need to delve into this and understand how to manage this risk effectively.

Successful organisations already manage complex risks – but even for great leaders understanding the cyber security risk and what it means for both the business and customer can be challenging.

To help with this challenge and effectively manage the risk, we have developed and used ourselves Telstra's Five Knows of Cyber Security. These are five simple questions to ask your organisation and it shifts the conversation from a technology discussion to one which senior management can engage with and thus contribute to the effective management of the cyber security risk.

1. Know the value of your data
2. Know who has access to your data
3. Know where your data is
4. Know who is protecting your data
5. Know how well your data is protected

When you can answer these five questions you are in a much better position to effectively assess and manage the risk.

An issue the cyber security community is tackling – and making progress but still with a way to go – is driving understanding of this business risk at the Board level. We as cyber security professionals have to provide assurance – that while the risk cannot be eliminated it can be managed.

To provide that assurance, ask yourself three simple questions:

1. Have we identified the right risks?
2. Are we managing these risks effectively?
3. When we get it wrong (because we will get it wrong) do we know how to respond and recover?

These questions, together with Telstra's Five Knows will change the conversation and shift the focus to help organisations understand that the business risk of cyber security can be managed effectively.

---

Berin Lautenbach,

Chief Information Security Officer (a/g)
Telstra Corporation Limited

# Methodology

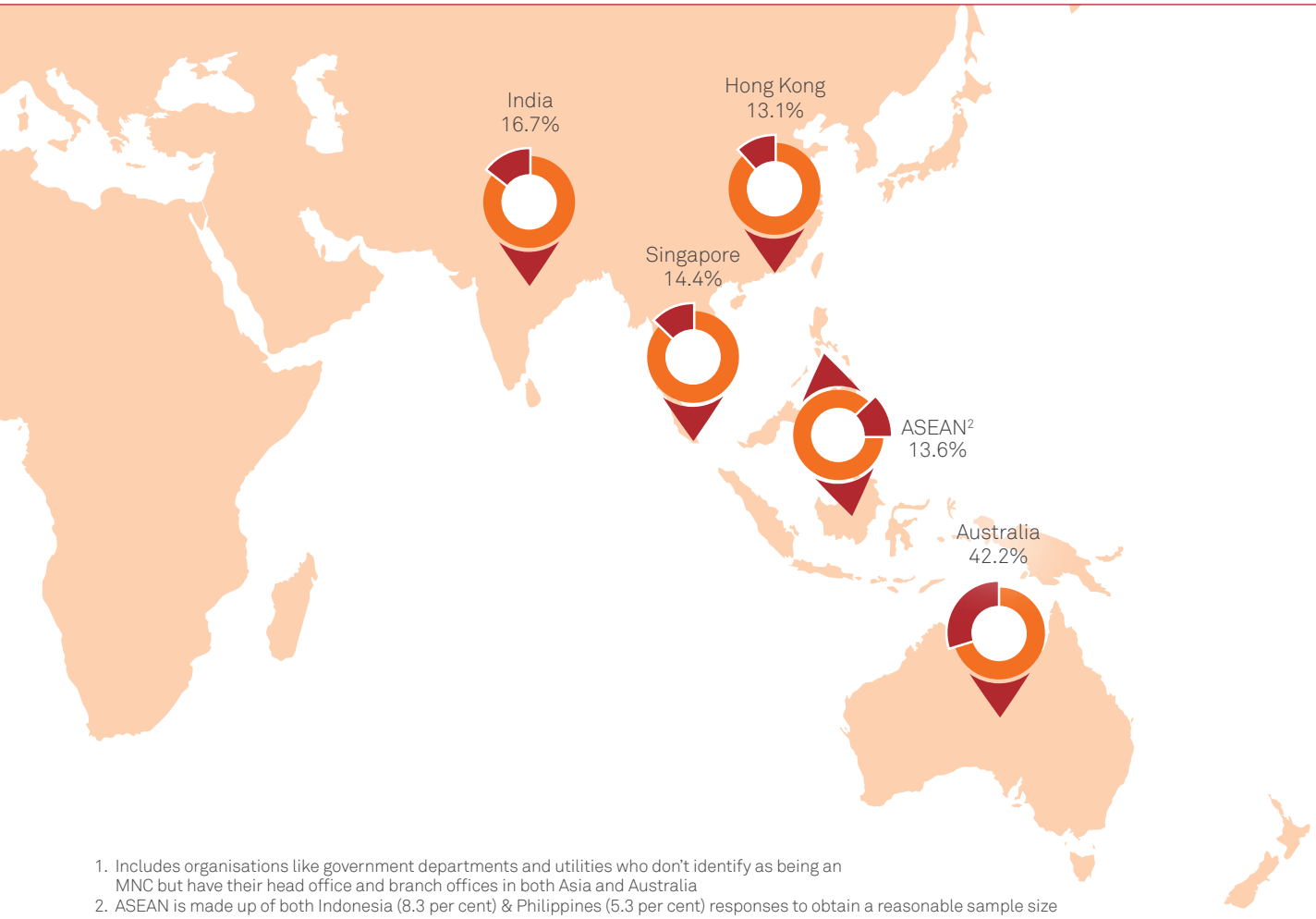
Telstra's Cyber Security Report 2017 provides insights into the current cyber security landscape to arm organisations with information on how to manage and mitigate their business risks.

Telstra engaged a research firm, Frost & Sullivan, to interview professionals responsible for making IT security decisions within their organisation to obtain a number of key insights on a range of security topics. The report also draws on analysis of security information and data gathered from Telstra infrastructure, security products and our third-party security partners.

The research firm's online surveys obtained 360 responses. 58 per cent of these responses were from Asia and the remaining 42 per cent were from respondents based in Australia. All the businesses who were interviewed in Asia have an Australian branch office and include responses from India, Singapore, Hong Kong, Indonesia and the Philippines. 87 per cent were multi-national organisations[1] and the remainder only have offices in Australia (13 per cent). C-level executives including Chief Executive Officers, Chief Financial Officers, Chief Information Officers, Chief Operating Officers, Chief Technology Officers, Chief Information Security Officers and Chief Security Officers accounted for 37 per cent of respondents across both Australia (43 per cent) and Asia (33 per cent). The remainder were in IT security managerial roles. All respondents either have some influence or complete control over the security investment within their organisations for their respective regions.

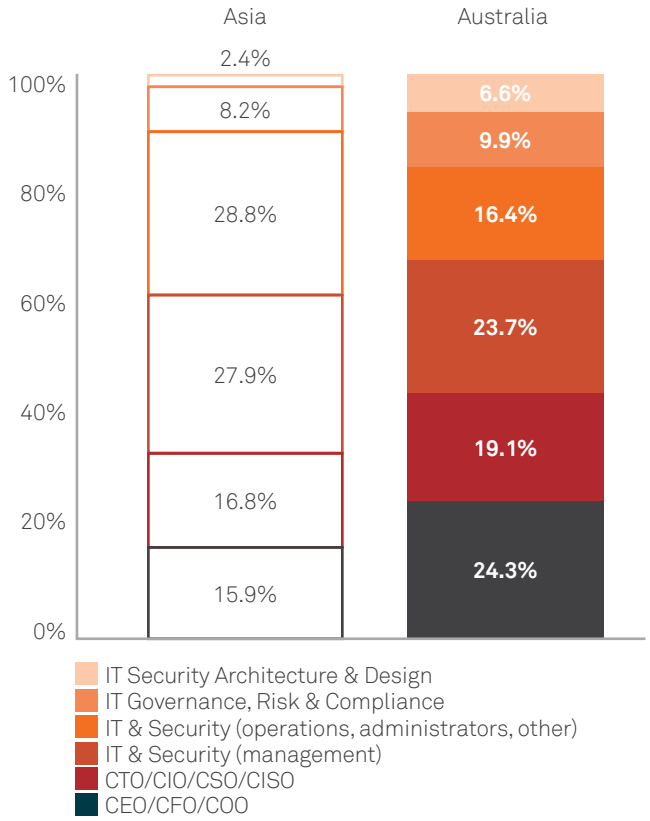
A large proportion of our survey results were based on large organisations where 77 per cent of total respondents worked for organisations employing 500 or more employees globally. The responses from Asia with 500 or more employees (89 per cent) and the responses from Australian responses with 500 or more employees (61 per cent). 81 per cent worked for organisations with 200 or more locally based employees across Australia (71 per cent) and Asia (89 per cent).

## Locations of respondents from Asia and Australia

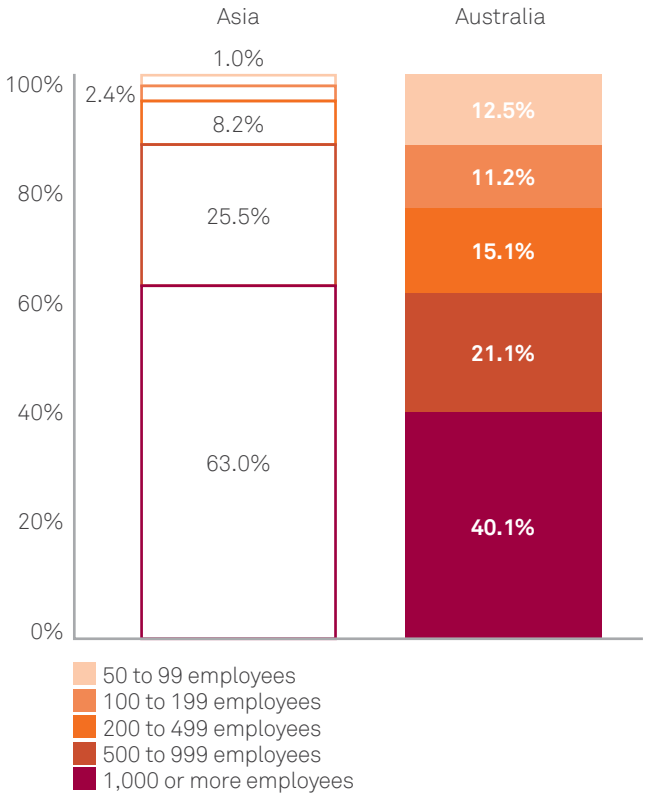



1. Includes organisations like government departments and utilities who don't identify as being an MNC but have their head office and branch offices in both Asia and Australia
2. ASEAN is made up of both Indonesia (8.3 per cent) & Philippines (5.3 per cent) responses to obtain a reasonable sample size

## Respondent's organisational role from Asia and Australia

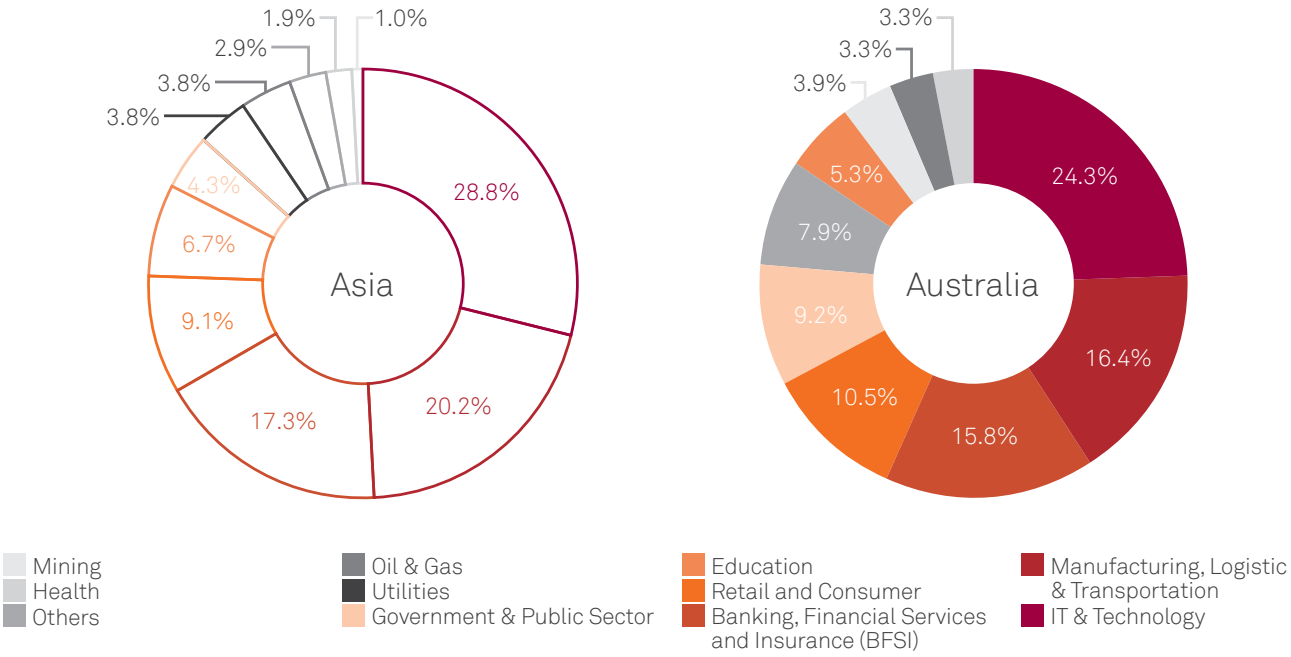



## Size of organisations globally




The industry segment with the highest percentage of responses was the IT & Technology sector from both Asia and Australia. The second highest percentage for responses in Australia was the Public sector, which included health care and education. The Manufacturing, Logistics & Transportation sector was the second highest industry for respondents from Asia.

## Australian and Asian respondents by industry sector



# Contents

# Cyber security readiness and maturity

## Cyber security engagement and involvement to enable your business

Companies need to place an explicitly commercial lens on cybersecurity, coolly assessing business risks and incorporating these risks' implications deeply into procurement, product development, sales, service and procurement processes.[3]

In today's interconnected world, we do not operate in isolation; our business processes and systems collect, analyse and share data from financial, product, operational, customer and employee data to our partners, suppliers and distributors. Companies need to consider the commercial and contractual risks by including cyber security capabilities as part of their sourcing and selection criteria and mandating the handling of data as part of contractual terms and conditions.

Companies need to progress from layering security controls on top of their technology architectures, and business and commercial processes, to embedding cyber security and integrating it into their business model in a way that does not adversely affect the customer experience. The key is to integrate cyber-resilience into enterprise-wide management and governance processes. This means conducting discussions across organisational silos to integrate considerations related to protecting information deeply, but also flexibly, into business processes like product development, marketing, sales, customer care, operations and procurement. The companies that do this most aggressively will not only reduce their risk, but also increase their operating efficiency and improve their value proposition with customers.[4]

Our research has shown that the involvement of all stakeholders in cyber security initiatives is high to very high amongst both Australian and Asian organisations, with the majority of respondents also recognising the importance of cyber security to carry out their functions across the business. Not surprisingly, the IT department is seen as the main group involved in cyber security initiatives and are identified as the key group who understand the importance of cyber security to carry out their functions effectively.

The good news is that C-level executives are perceived to be taking a more active role in cyber security by understanding the importance of cyber security initiatives, increasing their involvement in these initiatives and are increasingly taking responsibility for security incidents when they occur. In Australia, the CEO is regarded as almost as responsible as the IT department. Interestingly though, the perceived responsibility of the CISO in Asia is much greater than in Australia. Our survey results indicate that the IT department is primarily held responsible for security breaches for the organisations surveyed in Australia in 2016, when compared to the accountability of individual C-level roles in Australia. However, there has been a significant shift in responses towards the C-level executives as a group being held responsible for security incidents from 19 per cent in 2015 to 61 per cent in 2016 and away from the IT department being held responsible for security incidents with a decrease in responses from 62 per cent in 2015 to 34 per cent in 2016.

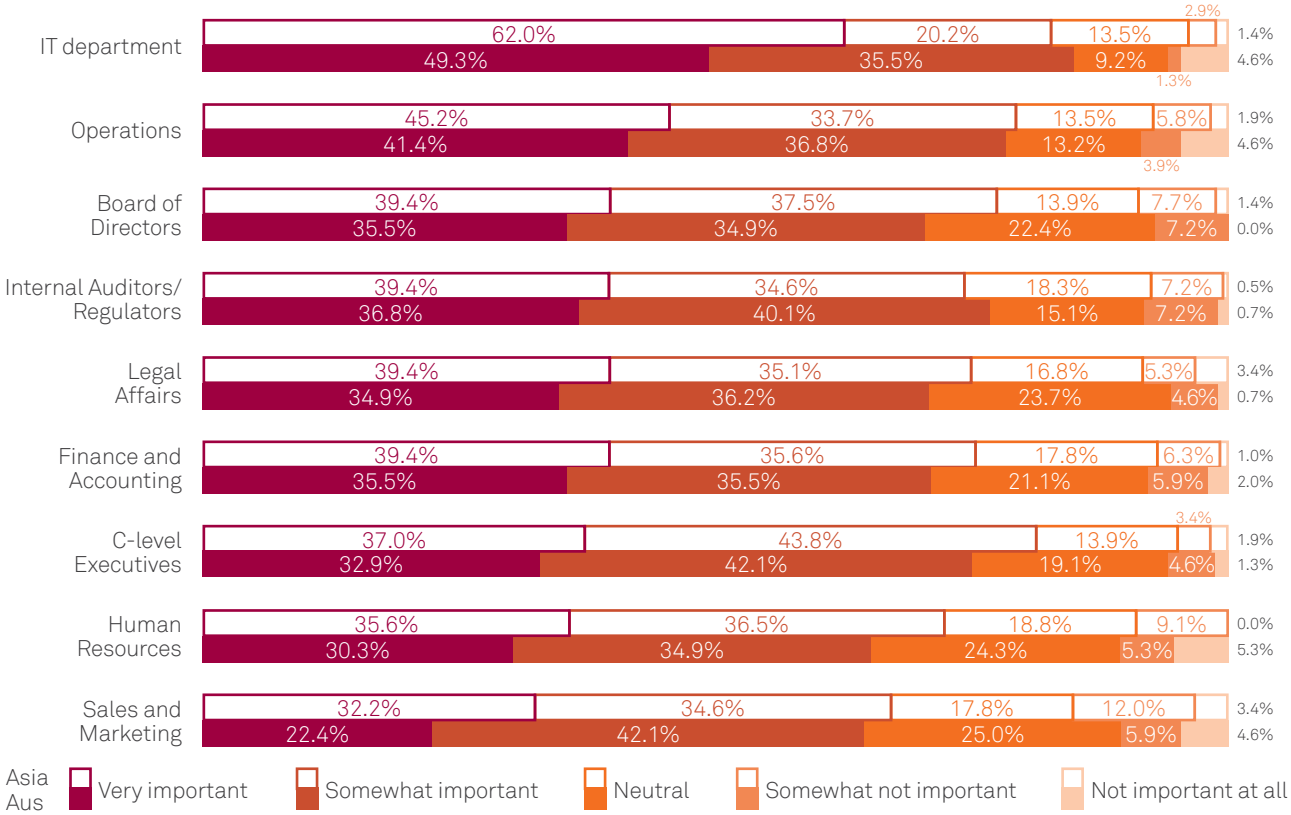
Similar to Australia, the perceived accountability of the IT department has dropped significantly amongst Asian organisations surveyed from 83 per cent in 2015 to 54 per cent in 2016. The C-level executives in Asia are perceived to be the primary stakeholders in taking responsibility for security incidents, which has increased from 35 per cent in 2015 to 65 per cent in 2016. This significant responsibility shift may reflect the growing involvement of the C-suite executives in the cyber security strategy and responsibility within their organisations.

The research identified that there are a number of opportunities to improve engagement within the business. Sales and marketing were seen as the least likely to view cyber security as an enabler and they were seen as having the lowest engagement in security initatives. This is despite the fact that they are heavily involved in capturing and using customer data. This is potentially a missed opportunity for sales and marketing to influence the online customer experience that occurs via their company's web portals, mobile applications or social media channels. They need to be engaged to ensure that customers are not overwhelmed with cumbersome or clunky authentication experiences. There is an opportunity to tailor security controls to different types of customers by getting their requirements from market surveys and focus groups to ensure the customer's voice is heard on how they want to access their data, products and services in a secure manner. Sales and marketing should be engaged and take a more proactive role to ensure that customer data and marketing information is secure; especially when it is shared with ad agencies or marketing and analytic companies.

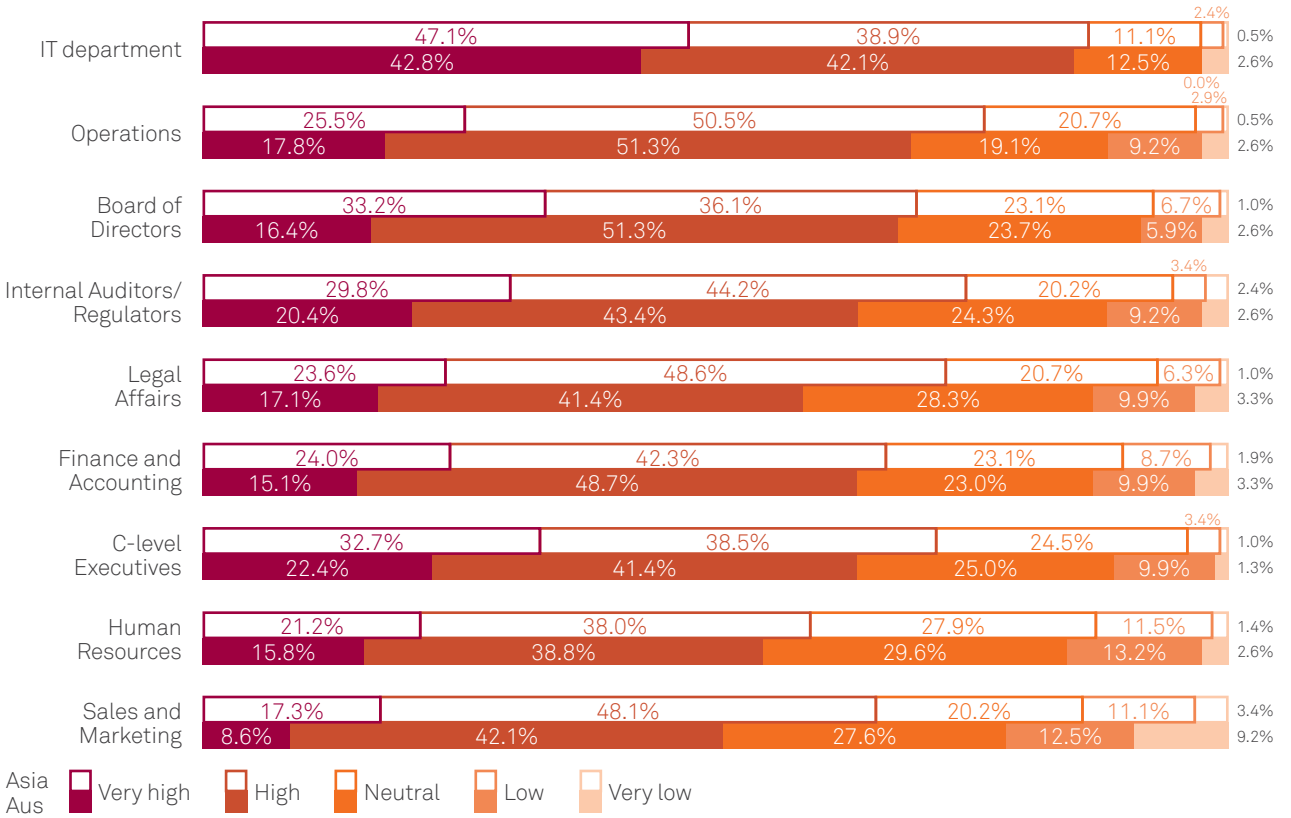
It was also surprising that HR was another group who had a lower involvement in cyber security initiatives as they are handling sensitive data for employees, contractors and potential new hires. They should be involved in how this data is collected, stored and secured as they need to consider the implications if this data is corrupted, lost or stolen.

3. Handbook of System Safety and Security by James M. Kaplan (McKinsey and Company)
4. Handbook of System Safety and Security by James M. Kaplan (McKinsey and Company)

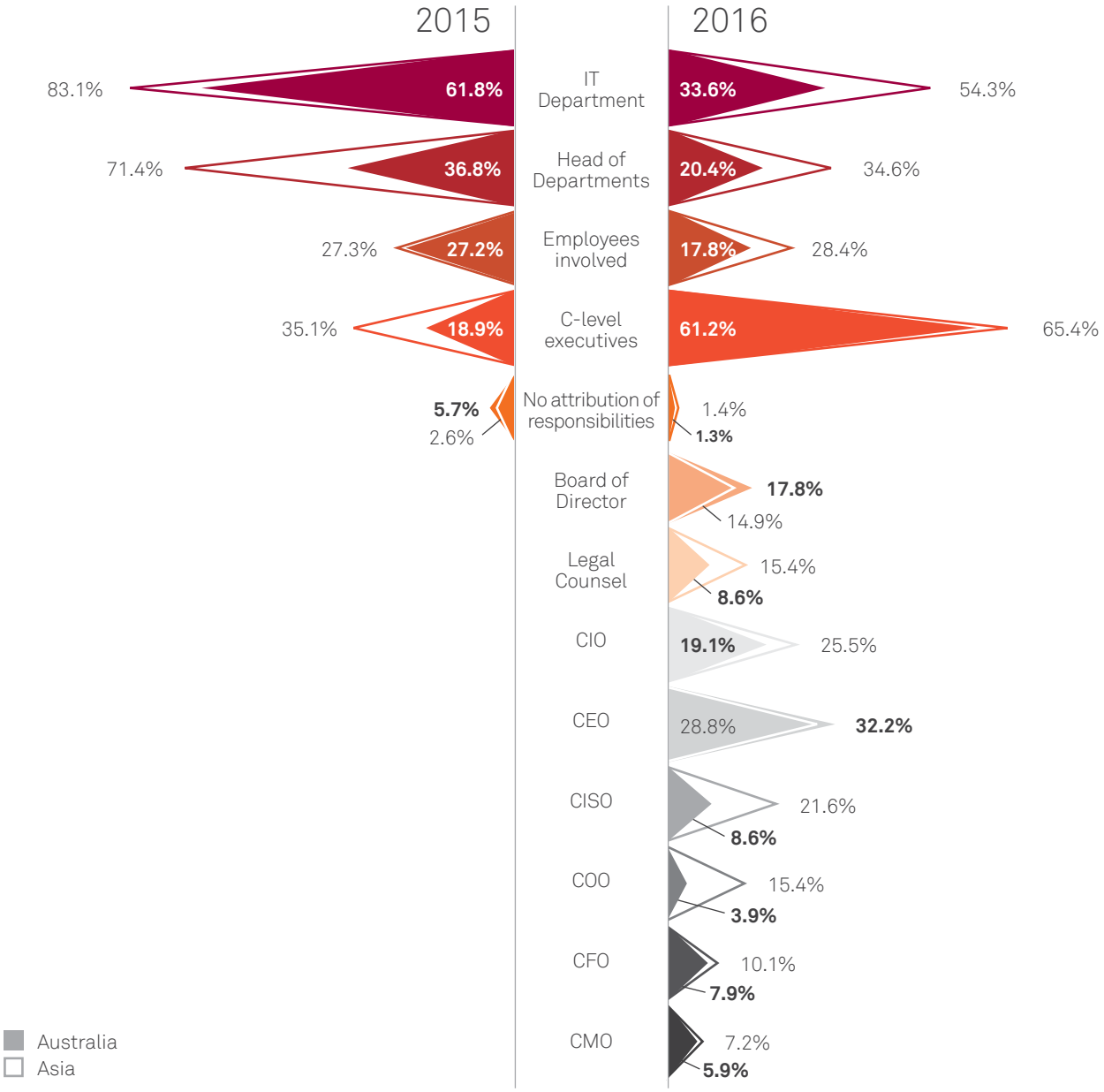
## Rating the importance of cyber security within the organisation – Asia and Australia




## Level of involvement in cyber security initiatives – Asia and Australia



## 2015 vs 2016 comparison of responsibility for security breaches – Asia and Australia




HR is responsible for handling personal employee or contractor information such as bank account details, tax file numbers, remuneration, résumés, employee contracts/offers and security checks that may be collected and shared with other third parties like HR service, system providers or recruitment companies. The HR department's involvement in cyber security has increased in some countries, such as the UK, where initiatives such as free cyber security courses for HR Professionals have been created by the UK Government and the Chartered Institute of Personnel Development (CIPD). The course was developed to assist HR workers to protect their companies' sensitive information.[5] This HR training initiative outlines the importance of providing cyber security awareness training to key stakeholders who are handling sensitive and important company data.

In Australia, the internal auditors and legal affairs team are perceived to have a relatively low level of involvement in cyber security. This is despite the fact that cyber security has a relatively high level of importance to their job functions and responsibilities. Interestingly in Asia, for internal auditors and board of directors, cyber security has a relatively low level of importance to their job functions and responsibilities, despite both groups having a high level of involvement in cyber security. This highlights the need to improve communications and engagement across the silos within the business to ensure that the right business and security engagements are in place to address legal, regulatory, privacy and commercial risks.

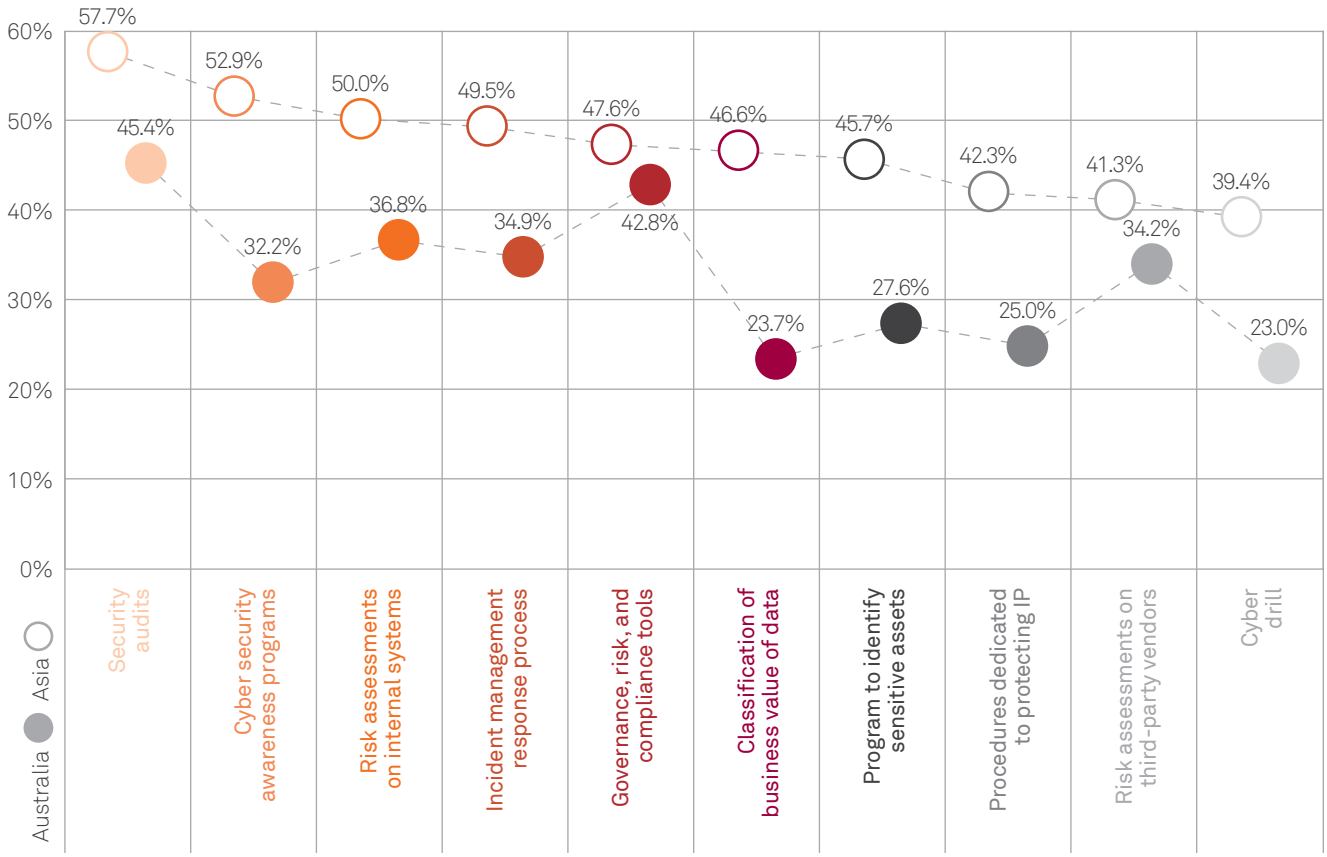
It is also worth noting the need for further engagement with physical and electronic security counterparts, driven by the proliferation of connected security devices and increasing market demand for converged solutions that combine electronic and physical security, identity management and information security.

5. https://www.cipd.co.uk/about/media/press/040216-cyber-security#

# Adoption of security guidelines, governance and procedures

Cyber security awareness has increased and appears to be driving the adoption of certain frameworks to conduct security audits to assist with formulating security policies within businesses; however, it's important that this doesn't just become a tick and flick exercise. As we have discussed, companies with great security posture don't just layer security controls across their business; they embed security into all areas of their business to ensure an integrated approach. Our results found that Australian and Asian companies tend to focus more on conducting security audits and less on conducting cyber drill programs within their organisations. The value of conducting cyber drills for a range of security incidents cannot be underestimated as it can highlight any deficiencies within the incident response procedures and the associated business continuity plans. The business needs to continue to deliver key products and services to acceptable business levels during a security incident and recover as quickly and effectively as possible.

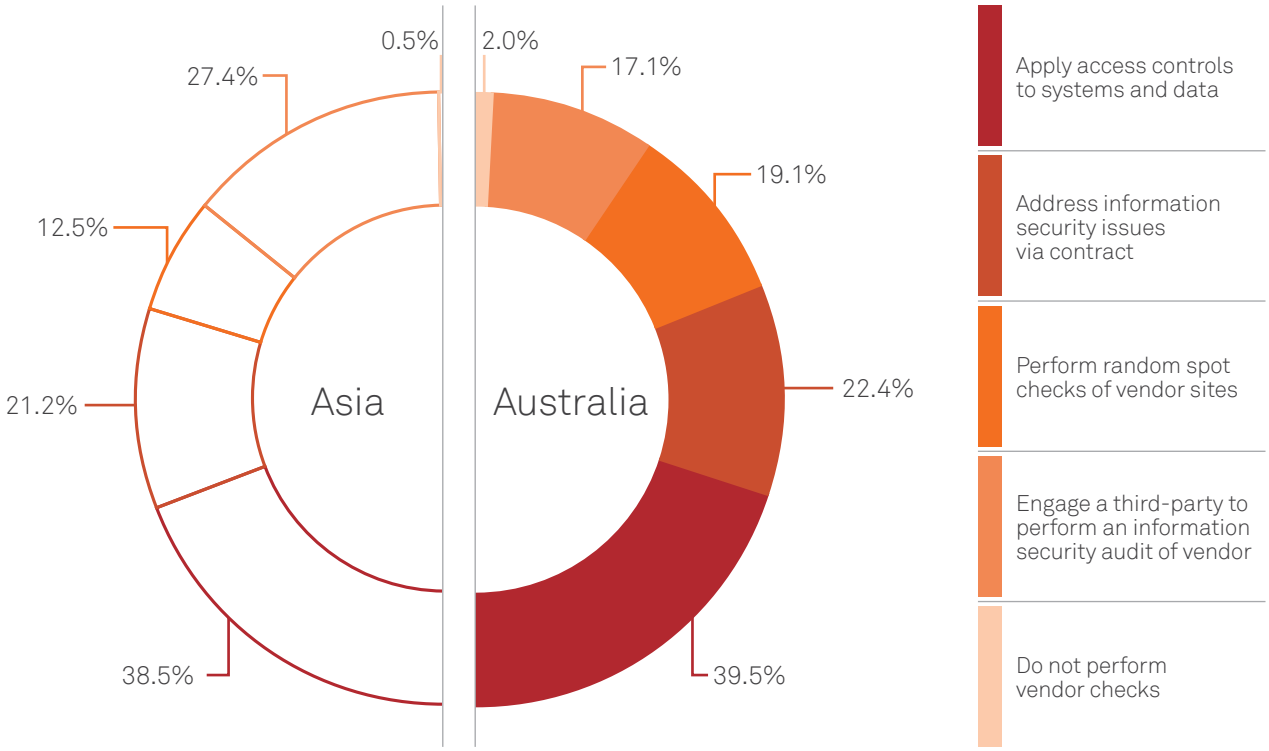
## Security governance, processes and skills in your organisation – Asia and Australia




Australian Prudential Regulation Authority (APRA) and the Australian Cyber Security Centre (ACSC) guidelines are the most popular security standards and frameworks adopted by both Australian and Asian organisations. It's important that the standards that companies adopt meet their regulatory, contractual and commercial requirements and align with their business objectives. In contrast, SANS Top Critical Controls and PCI were chosen by only nine per cent of Australian respondents. The low adoption of PCI security standards with Australian respondents is surprising as every Australian business who accepts and processes credit or debit card information is required to comply to ensure a secure payment card environment. This result may be due to the outsourcing of credit card payment functions to third parties or a lack of involvement in the PCI compliance security initatives by the majority of respondents. This may be due to a lack of engagement, awareness or silos within the organisation regarding PCI compliance.

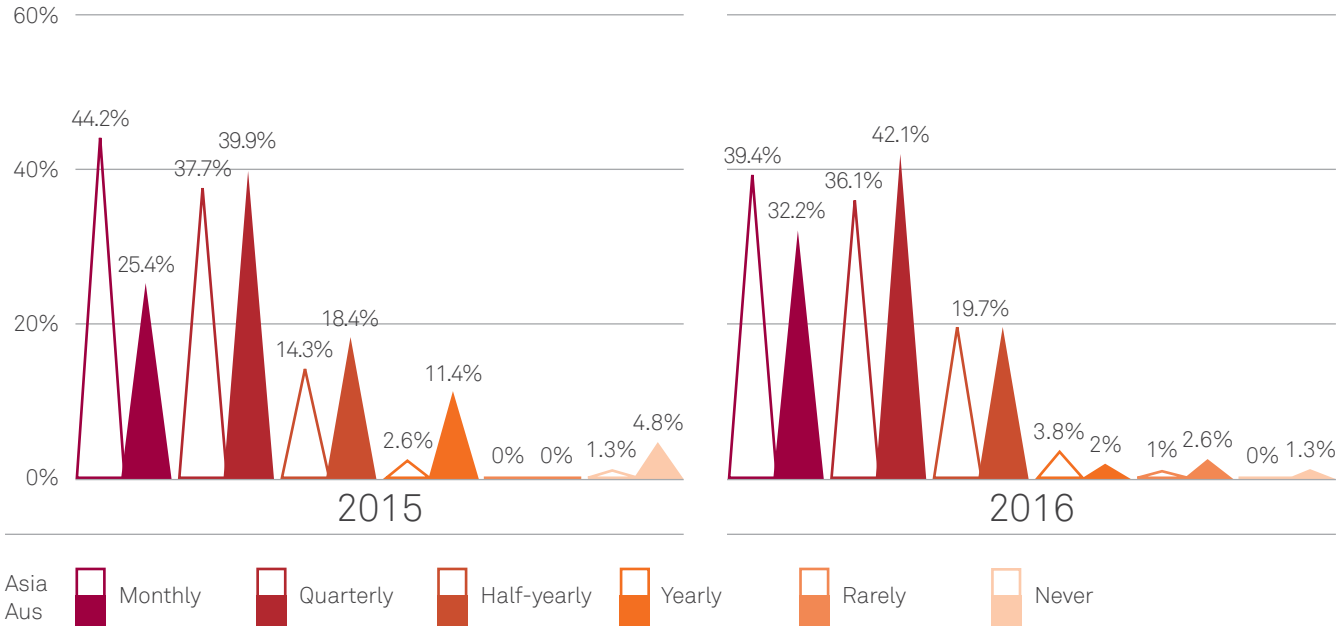
Almost all of the organisations surveyed in Australia and Asia adopt various methods to control IT security risks with their business suppliers and partners with the most popular being the application of access controls to data and systems. Two per cent of respondents from Australia and one per cent from Asia indicate that they do not perform vendor checks on their business partners.

## Controlling IT security risks with business suppliers and partners – Asia and Australia




In Australia, the good news is that we are conducting more frequent board briefing sessions, the percentage of enterprises conducting their briefings on a yearly basis has significantly reduced from 11 per cent in 2015 to two per cent in 2016. On the contrary, in Asia the frequency of briefings has declined slightly, with 39 per cent of organisations now doing this monthly. However, 57 per cent of ASEAN (Indonesia and the Philippines) and 50 per cent of Indian respondents are running monthly briefings, which is higher than the 32 per cent recorded for Australian businesses.

## Frequency of briefs to board members/senior management on cyber risk and security mitigation – Asia and Australia



# Security threats and trends

## Email threats and phishing campaigns

### Phishing Campaigns

#### Phishing emails remain the most popular method to deliver malware.

Email continues to be the primary communication channel for businesses so it is not surprising that the most popular delivery method for cyber threats is via phishing emails. The next most popular delivery method is via malicious websites/URLs. Opportunistic phishing emails aim to trick a recipient into clicking on a malicious link or attachment and the malware is downloaded and executes on the end point into the network. The malware can then establish a backdoor to the Command and Control (C&C) server, obtain escalated user privileges and then move laterally through the network to the target data. Typical examples of phishing emails include delivery emails related to parcels, invoice payments or utility bills, and when an end user clicks on the link or attachment it delivers malware to the end user's device.

Spear phishing emails target a specific person within a company, and emails that target senior executives are sometimes called 'whaling'. Whaling or spear phishing emails are typically well researched using both social media and publicly available company information like annual reports and shareholder updates. They will appear legitimate and to be from trusted contacts in the user's social network, which makes them much harder to detect compared to other opportunistic phishing emails. Typically the objective is to obtain sensitive data that may include customer's personal information, intellectual property (e.g. design blueprints and source code), commercially sensitive information like financial results, investments, merger & acquisition information, corporate roadmaps and strategic information for fraudulent purposes or to block access to a system or data files for financial gain through the delivery of ransomware.

According to our survey in 2016, approximately one-third of both Asian and Australian businesses experienced a phishing email incident which impacted their business on at least a monthly basis. 21 per cent of respondents in Asia said that it took five hours or more to recover from these incidents compared to 13 per cent of respondents in Australia who said that it took five hours or more to recover from phishing email incidents.

As social engineering attempts by cyber attackers continue to improve and become more sophisticated, organisations should work on driving more cyber security awareness training for their staff and implement social media and email handling policies within the organisation. Mitigating the risks associated with staff and contractors using email or social media cannot be underestimated where private and sensitive company information may be exposed due to malware infections or shared inappropriately.

### Inbound Email Threats

Firstwave Cloud Technology delivers Telstra's Internet Protection – Email and Web Content Security for government departments, enterprises and businesses in Australia. In 2016, Firstwave scanned over 500 million inbound and outbound emails across Australian customers' mail servers.

Email content security provides a multi-layered approach to protecting organisations against spam and malware. In 2016, Firstwave identified almost 47 million inbound threats across inbound emails, representing a range of threats including profanities, offensive materials, PCI security standards breaches, spam and malware. In 2016, Firstwave rejected 35 million emails[6] at the "reputation" layer and then captured 12 million emails at the advanced second level of defence preventing these threatening emails from reaching the recipient. The number of emails captured at the advanced second level of defence has reduced by 13 per cent in 2016 compared with 2015.

Firstwave also detects and scans potentially infected zip files, which is a common method used to evade detection by cyber criminals. This system generally captures between 30,000 and 45,000 potentially dangerous emails each month.

### Business Email Compromise

Business Email Compromise (BEC), as defined by the FBI, is a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorised transfers of funds.[7] Formally known as Man-in-the-Email scams, these schemes typically compromise official business email accounts, by using spear-phishing emails, and key logger malware, to then conduct unauthorised fund transfers. This type of scam has not been widely publicised but is growing in popularity due to the lucrative nature of this scam. According to the FBI, the BEC scam attempts have hit US$3 billion in June 2016, and the FBI has recorded a 1,300 per cent increase since January 2015. This includes BEC reports by US and foreign victims from a number of sources including complaints filed with the FBI, international law enforcement agencies and financial institutions.[8] The results of our survey found 30 per cent of businesses in Australia experienced a BEC on at least a monthly basis and 20 per cent of these businesses took five hours or more to recover from these incidents. The results were similar in Asia with 30 per cent of respondents who experienced a BEC on at least a monthly basis. 18 per cent of these businesses took five hours or more to recover from these incidents.

6. Note: these numbers are approximated by using statistical methods on representative data samples and provided by Firstwave
7. https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise
8. https://www.ic3.gov/media/2016/160614.aspx#fn1

To mitigate BEC risks it's important that the financial functions within the business have appropriate governance in place, with adequate approvals for funds transfers. Transaction approval should satisfy certain characteristics – including but not limited to integrity, non-repudiation and separation of duties. The key point is that (above a certain transaction value) an email shouldn't constitute approval as it's too easy to forge. Finance policies may still want to conduct transfers using email approvals but the business needs to determine their risk tolerance levels depending on how many low-value transactions they are willing to lose due to fraudulent email requests. If the business still insists on performing email transfer approvals then it's important that they conduct appropriate cyber security awareness training with the finance department as financial staff need to be weary and scrutinise email requests to determine if the request is legitimate. It is also important to use only previously verified transfer details and to not use transfer details provided in email. Implement appropriate transfer request processes to add phone verification or implement a secondary sign-off by company personnel for these email payment transfer requests, especially when banking details have changed.

## Outbound Email Threats

Organisations need to put in place safeguards to protect themselves against threats that may occur from internal sources. Considered 'outbound threats', these threats often occur when employees either intentionally or unintentionally distribute email communications that contain inappropriate, confidential or threatening content.

The weight of this risk can be seen with approximately 10 million outbound threats being recorded by the Firstwave platform in 2016. These threats could have represented real reputational risks if these companies had not put in place measures to stop the outbound distribution of spam, viruses, malware, profanities, offensive images and credit card information.

## Impacts of Offensive Content

Anti-discrimination legislation[9] is important for all Australian businesses to understand and adhere to given the financial and reputational risks associated with breaches. In 2016, Firstwave identified almost 810,000 inbound and outbound emails, which contained inappropriate content such as profanities and offensive images.

Offensive content being received and distributed by company employees can lead to businesses being exposed to harassment, bullying or discrimination claims in some instances as well as reputational and financial losses as a result of these inappropriate emails being received or distributed by the organisation.

This shows the importance of having in place a reliable content security system to monitor and block inappropriate emails from reaching employees or being sent outside the organisation, potentially to clients, suppliers or other members of the public.

Firstwave also identified that cyberbullying is still very prevalent, particularly with inbound emails. While there was a slight decrease from 2015 in relation to inbound emails that contained cyberbullying content, more than a million were still identified across the platform in 2016. This is a big concern for companies as cyberbullying is not only damaging to the victim, but also has higher business costs due to potential impacts on company productivity and litigation costs.

## PCI Compliance Impacts

Protection of customers' personal and sensitive information is also of significant importance for businesses. Compliance with the PCI's security standards is mandatory for all Australian businesses if they plan to accept and process payments via credit or debit cards.[10] A company's email should be identified as a traceable channel that can be proactively used to monitor and protect against these data leaks. Firstwave have seen almost 450,000 emails which contained PCI data and were attempted to be sent throughout 2016 (although this was a drop of over half since the previous year). This shows that Australian businesses are exposed to potential PCI breaches when they do not have appropriate data leakage protection systems in place to mitigate this risk.

There are real and serious email threats that are commonly taking place every day that can threaten your business reputation and brand. Failure to meet compliance obligations can lead to financial losses, penalties and/or litigation. With trends such as malware bypassing reputation/signature-based defence systems and internal staff continuing to expose businesses with risky behaviour, it is essential that all businesses put in place appropriate cyber security training and security solutions to control, monitor and block email threats from entering or exiting their internet communications before the damage takes place.

9. http://www.findlaw.com.au/articles/4266/workplace-discrimination-laws-in-australia.aspx
10. http://www.cio.com.au/article/400300/what_pci_compliance_/

# Malware and ransomware

## Malware Threats

### Australia was the main target for malware in 2016 in the Asia Pacific region.

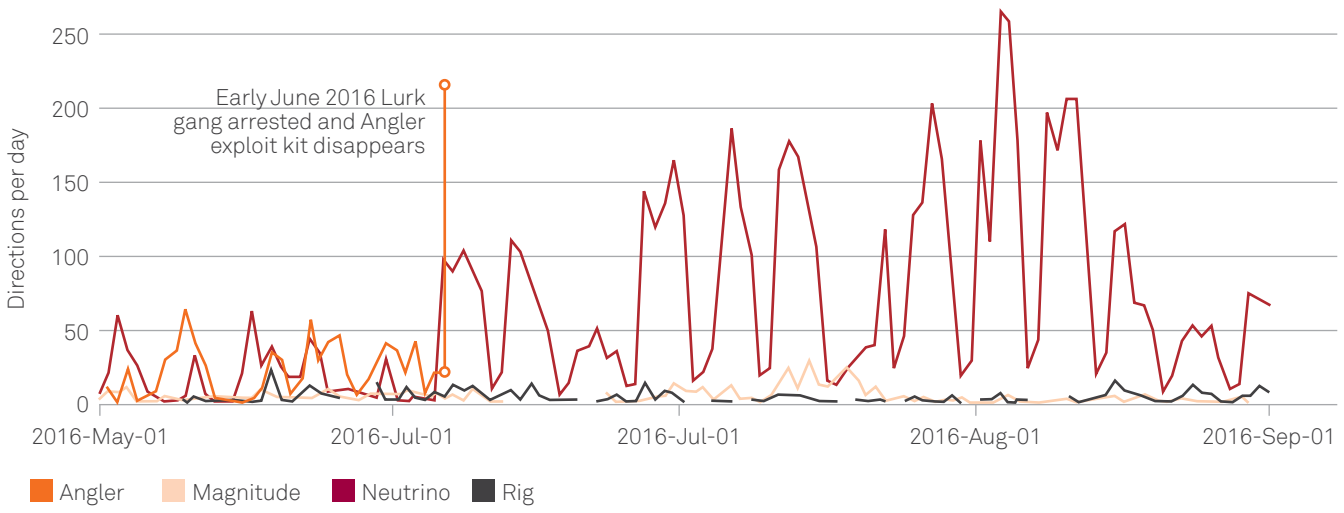
Australia was the main target for malware in 2016, with the highest number of malware download attempts in the Asia Pacific region, according to Palo Alto. Australia is a likely cyber criminal target due to its economic growth combined with its high adoption of technology compared to other countries in the region. The most common types of malware families seen by Palo Alto are 'Ransomware', 'RATs' (Remote Access Trojans) and 'Infostealers' (Information stealing malware). Check Point research has found that Australia is experiencing a significant growth in ransomware and a reduction in other types of malware. The decline in banking Trojans may be due to the large investment required in infrastructure and people to convert the compromise into cash compared to the minimal effort required to distribute ransomware and the use of Bitcoins to launder the ransom payments. Our research indicates, 26 per cent of Australian respondents and 30 per cent of Asian respondents experienced a malware/virus outbreak on at least a monthly basis. According to our survey results, 28 per cent of respondents in Australia and 27 per cent of respondents in Asia said that it took five hours or more to recover from these incidents.

The growth of malware threats targeting Australia and the Asia Pacific region is a booming industry due to a number of factors:

- The rising number of exploit kits and malware tools that are being sold in the cyber criminal markets.
- The increasing number of malware distributors who are using these user-friendly exploit kits and tools to distribute unknown malware.
- The agility of exploit kits that are continually evolving to evade detection and taking advantage of new vulnerabilities, mobile devices and Internet of Things (IoT) to widen their infection campaigns.
- The rate of economic growth within the Asia Pacific region making it an attractive and lucrative target for cyber criminals.
- The rise of Ransomware-as-a-Service (RaaS) increasing the volume of malware distributors and ransomware distributed.

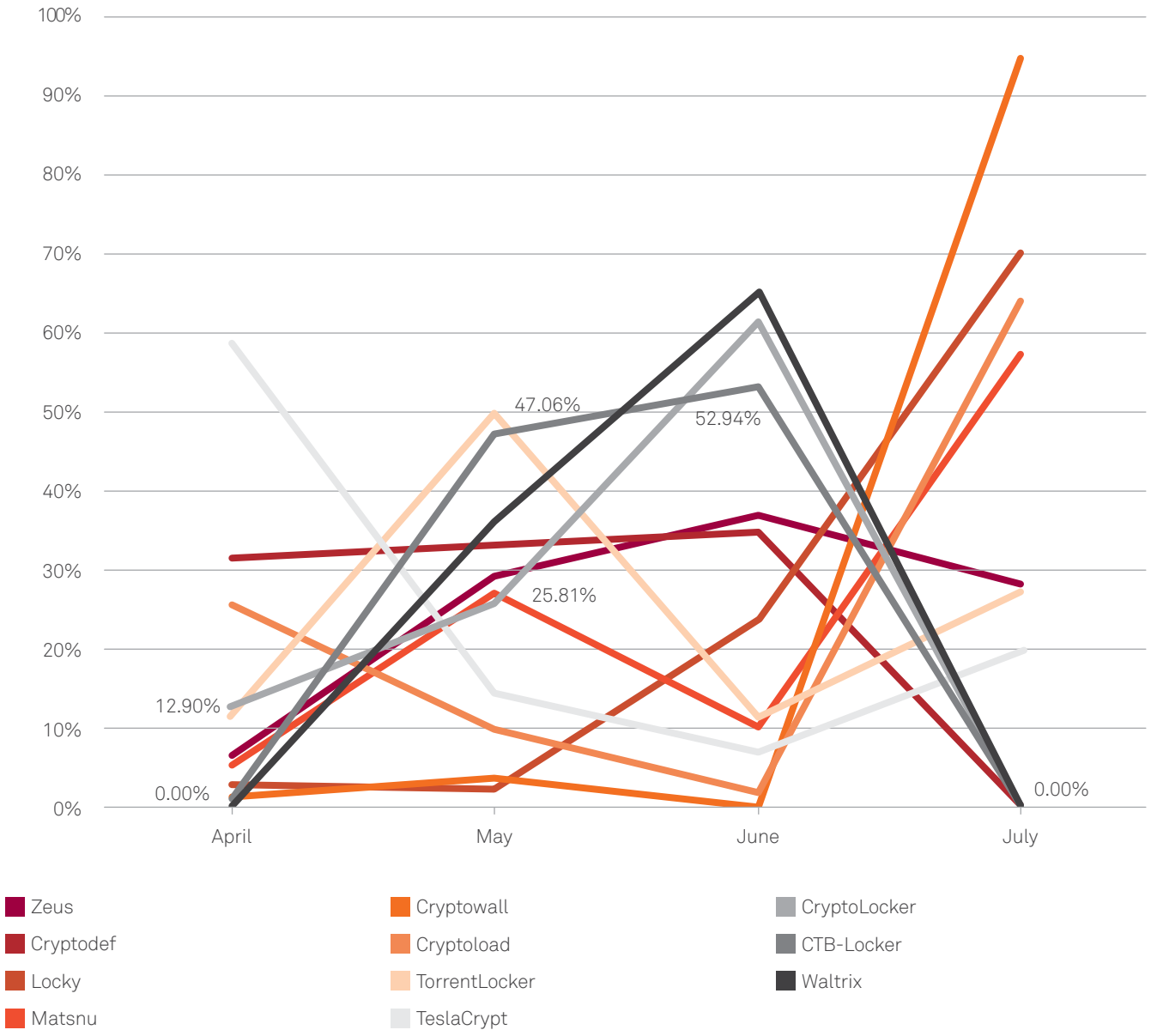
The two primary threat vectors used to deliver malware are via large scale phishing emails and exploit kits. A typical exploit kit provides criminals with a user-friendly web interface to deliver malicious software by taking advantage of certain vulnerabilities in the targeted device. Exploit kits are used primarily for drive-by downloads, when a user is unknowingly redirected to a malicious website from a legitimate vulnerable website, or infecting a legitimate website using exploit kits to target a specific group, called a watering hole attack.[11] The exploit kit of choice for cyber criminals prior to July 2016 has been the 'Angler' exploit kit. However, cyber criminal group 'Lurk', who had developed and were selling the Angler exploit kit as a service to other cyber criminals, were arrested in Russia around early June 2016.[12] Palo Alto observed the number of Neutrino sessions increase in late June 2016. This was the result of cyber criminals moving to adopt the Neutrino exploit kit for their criminal campaigns. However, Cisco recently reported that the popular Nuclear and Neutrino exploit kits have abruptly disappeared from the threat landscape in 2016, which has created a void for other exploit owners to take their place.[13] RIG and Magnitude may become prevalent in the future as they would be the next popular in the APAC region now that Angler, Nuclear and Neutrino have disappeared.

## Exploit kit activity in APAC - Palo Alto




11. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/Threat-Report-FortiGuard-Eye-of-Storm.pdf
12. http://www.theregister.co.uk/2016/08/31/anglers_obituary_super_exploit_kit_was_the_work_of_russias_lurk_Group
13. http://b2me.cisco.com/en-us-annual-cybersecurity-report-2017

## Top 10 malware families 2016 in APAC region – Check Point




The popularity and activity of exploit kits and malware is very dynamic with cyber criminals switching between different exploit kits and the malware used on a regular basis to keep ahead of the security defenders, as shown by the daily exploit kit graph provided by Palo Alto and the monthly malware graph from Check Point.

Palo Alto research indicated that 'Locky' ransomware was the most prevalent malware family downloaded in the Asia Pacific region, in 2016. It is typically delivered in a Microsoft word document within a phishing email but has also been delivered using exploit kits on infected websites and most recently as JavaScript's inside zip files. Palo Alto found 'Usnif' was also pervasive in 2016. 'Usnif' is a banking Trojan which has been targeting Australian banks with recent variants utilising the Tor network and typically delivered using phishing emails or via the Neutrino exploit kit (with 21 per cent of downloads).

The majority of the Top five viruses according to Fortinet were associated with the JavaScript Nemucod family of malware in the Asia Pacific region. The Nemucod exploit kit is a popular delivery method for ransomware and has also been used to deliver a new payload to its victims called Win 32/Kovter that delivers a backdoor to a Command and Control (C&C) server with ad-clicking capability.[14]

14. http://www.welivesecurity.com/2016/08/09/nemucod-back-serving-ad-clicking-backdoor-instead-ransomware/

## Typical malware life cycle – Palo Alto


### Ransomware

## Ransomware was the most common malware in the Asia Pacific region.

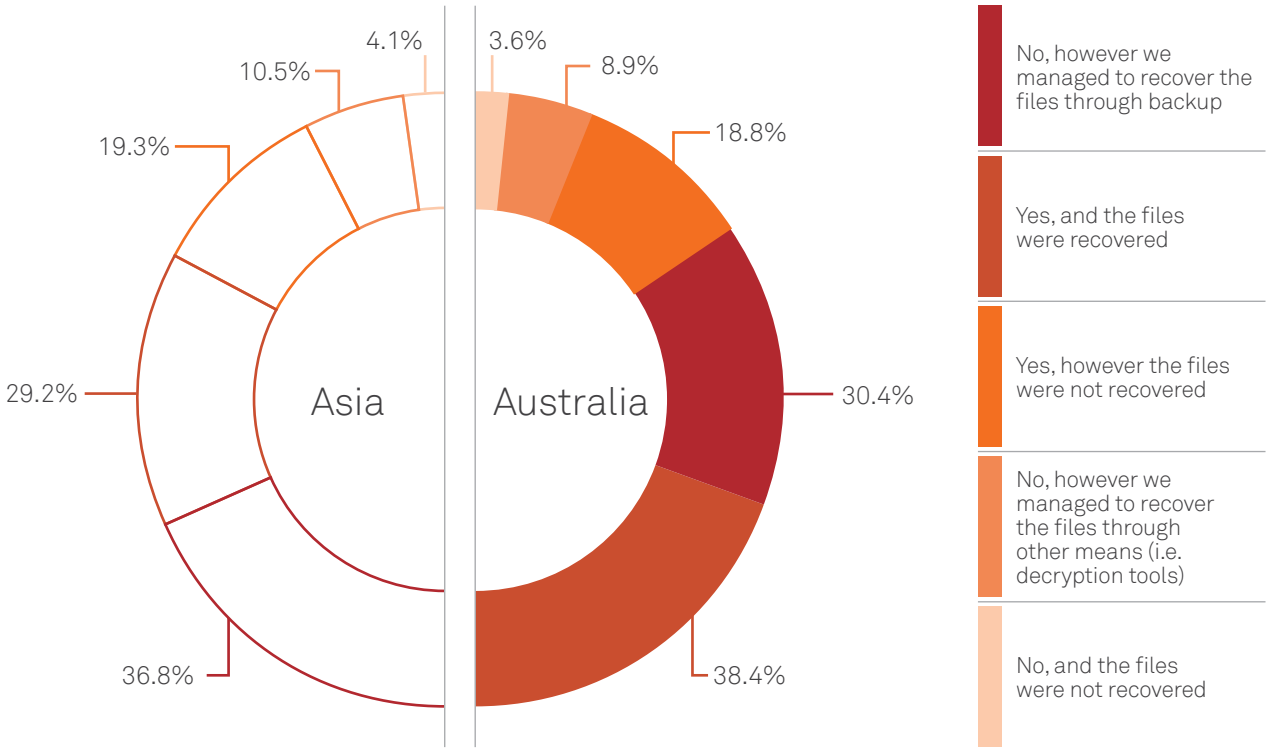
Ransomware is a form of malicious software that holds a device or system hostage by blocking access until a ransom is paid to remove the restriction. Ransomware can be delivered as attachments or dropped onto vulnerable devices by exploit kits when the user visits or is redirected to a compromised website. The most common variants are categorised as crypto-ransomware where certain files on the target device are encrypted and some are able to spread across networks and servers to encrypt other file systems. Certain types of ransomware are able to delete or encrypt back-up files before demanding payment for a decryption key. This may make it more compelling to pay the ransom if the backup cannot be used to restore the files but it is not the recommended course of action. Other variants of ransomware include locking the screen or preventing the operating system from loading until a ransom is paid to remove these restrictions.

According to our survey, in 2016 24 per cent of Australian businesses experienced a ransomware incident which impacted their business on at least a monthly basis and it took the same proportion five hours or more to recover from these incidents. Similarly, 26 per cent of Asian businesses experienced a ransomware incident which impacted their business on at least a monthly basis. 22 per cent of respondents in Asia said that it took five hours or more to recover from these incidents. Check Point research indicates that the average lifespan of new ransomware is now 58 seconds with 90 per cent of attacks/exploits seen only once.

Our vendor research found that ransomware was the most downloaded malware in the Asia Pacific region in 2016 and that approximately 60 per cent of Australian organisations reported that they experienced at least one ransomware incident in the last 12 months. Of the Australian organisations surveyed, 42 per cent reported paying a ransom to cyber criminals. However, the approach towards ransom requests in Asia varies with the majority of India, ASEAN and Hong Kong enterprises agreeing to pay the ransom, whilst the majority of enterprises in Singapore tended not to accede to ransom requests and managed their recovery through backup files instead.

Nearly one out of every three Australian organisations who experienced a ransomware incident and paid the ransom did not recover their files. The impacts for Asian organisations were slightly higher with 40 per cent of respondents who paid the ransom but did not recover their files. A number of companies are choosing to quietly pay a ransom demand, which is typically in the hundreds of dollars, to restore their business operations, to avoid embarrassment and the potential reputational impacts with the hope of retrieving their lost data. The reality is that you could receive further ransom demands, that the data may be exposed or sold on to other third parties and there are no guarantees for recovering your data. It is evident that implementing a proper back-up strategy helps to mitigate the rising threat of ransomware, and can be seen as an effective strategy as per the survey results for the majority of Singapore organisations.

## Ransomware recovery survey results – Asia and Australia



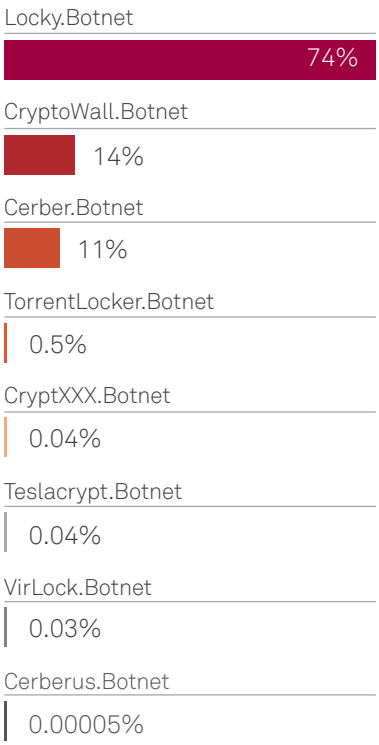

## Benefits of hindsight - Invest in an appropriate back-up strategy rather than paying a ransomware demand.

Ransomware-as-a-Service (RaaS) is where ransomware authors have developed user-friendly interfaces for their malware and they offer it to others to become distributors. The service offers cyber criminals, without coding experience, the opportunity to make money by either paying a once-only price or a profit share arrangement to distribute the ransomware. Some examples of RaaS offerings that were promoted on underground forums and marketplaces include: 'Hostman Ransomware', 'Flux Ransomware', 'Cerber' and 'Ransomware affiliate network'.[15,16] Each RaaS instance offers different features to recruit distributors based on claims of detection avoidance options and different profit models. RaaS feature options may include different encryption options, the worm feature to infect more users, multiple language options, the promise of future versions infecting mobile devices and customisation of the software to select different target files, Bitcoin addresses and/or ransom amounts. RaaS prices vary from US$9.95 for a limited use version to US$150 for a copy of the source code. Some RaaS offerings are free initially with approximately 15 per cent to 40 per cent of the profit share going back to the author, which maximises the returns for the author if the malware is successful in the long run.[17] The FBI announced that ransomware is expected to become a US$1 billion dollar industry in 2016, which is a substantial increase compared to 2015, when ransomware was reported as a 'mere' US$24 million criminal industry.[18]

According to Fortinet in March 2017, 'Locky' was the largest ransomware campaign in the last 12 months with 74 per cent of the ransomware downloads, followed by 'CrytoWall' with 14 per cent that was prevalent earlier in 2016, with nearly 100 thousand detections per month in Australia alone. The third most prevalent ransomware, according to Fortinet, is 'Cerber' with 11 per cent of ransomware downloaded in the Asia Pacific region the last year. 'Locky' can be delivered using the JavaScript Nemucod downloader malware and is primarily used as an infection vector to plant various families of ransomware onto a victim's computer to encrypt files and demand Bitcoin ransom payments.[19] 'Cerber' is a RaaS offering with a network of distributors with a profit share arrangement.[20] Palo Alto research suggests that 'Locky' is designed by experienced cyber criminals and is known to delete shadow copies of files to make local backups unusable.

15. http://blog.fortinet.com/2017/02/16/ransomware-as-a-service-rampant-in-the-underground-black-market
16. http://blog.checkpoint.com/2016/08/16/cerberring/
17. http://blog.fortinet.com/2017/02/16/ransomware-as-a-service-rampant-in-the-underground-black-market
18. http://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646
19. https://blog.fortinet.com/post/cryptowall-teslacrypt-and-locky-a-statistical-perspective
20. http://blog.checkpoint.com/2016/08/16/cerberring/

## Top ransomware in Asia Pacific (March 2016 – March 2017) – Fortinet




**Ransomware Mitigation Recommendations:**

- Identify critical data and ensure regular offline backups are performed to avoid the situation where backups are also encrypted by the malware.
- Conduct regular security patching/ updates for operating systems and applications to mitigate risks associated with exploit kits and malware, especially for Java, Adobe Reader, Flash, Silverlight and other applications regularly targeted by exploit kits.
- Ensure that incident response plans and business continuity plans are in place and regular disaster recovery drills are performed to ensure that back-up data can be used to return the business back to normal operation within acceptable time frames.
- Email security gateways with Anti-spam to block phishing emails.
- Employ web security gateways to block malicious code being downloaded and block connections to command and control servers.
- Implement application whitelisting to keep unknown executable files from running.
- Deploy advanced endpoint protection on laptops, mobiles and servers.
- Ensure security awareness and phishing awareness training is conducted by all users on your network.

Unfortunately, ransomware is a situation where prevention is better than a cure but if you find that you have been affected by ransomware with all your back-up files encrypted, it is worth calling in incident response experts to see if they can assist you. There is also a new anti-ransomware alliance made up of security vendors and law enforcement organisations that has been established a website to assist affected organisations. The alliance website is called the No More Ransom Project; it offers prevention advice and you can check to see whether they have the tools for decrypting your files using recovered keys.[21] Some direct links to keys are available where the ransomware has been reverse engineered or if law enforcement agencies have taken down control servers and obtained decryption keys.[22] Other advice is available from CERT Australia[23] to assist with managing ransomware risks, reputable security vendors and security service providers.[24] Paying the ransom should always be an activity of last resort and avoided where possible.

21. https://www.nomoreransom.org/
22. http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-dec-2016.pdf
23. https://www.cert.gov.au/advisories/ransomware
24. https://blog.fortinet.com/2016/04/06/10-steps-for-protecting-yourself-from-ransomware

# Mobile malware

Mobile malware is becoming more popular and is expected to take over traditional malware as the popularity of mobile devices increases. Check Point is seeing 300 per cent growth in mobile malware month over month in the Asia Pacific region. Mobile malware infection rates in Australia have increased by two per cent to be over seven per cent in Q3 2016, compared to Q2 2016, according to McAfee.[25] This trend is not surprising as traffic from wireless and mobile devices is expected to account for 66 per cent of total IP traffic by 2020 and wired devices will account for only 34 per cent.[26] Many of the countries in Asia connect via mobile rather than fixed-line broadband. For instance, fixed-line internet only reaches one per cent of the Indonesian population and three per cent of the population in the Philippines while mobile connectivity reaches 42 per cent of the population in these countries. China has the world's largest online population with more than 688 million internet users with 66 per cent of these connecting via smartphones (~ 459 million mobile users).[27]

There are a number of different ways that mobile malware can be delivered to a mobile device; obviously phishing emails and compromised websites can be used as a delivery mechanism for malware targeting mobile devices. Another method is when users have mobile operating systems or applications that may have security flaws or vulnerabilities that may be exploited by malware on the same network segment or Wi-Fi network. The malware could be delivered via social media applications or SMS or MMS or other mobile messaging applications. The mobile application may already contain malware when it is downloaded from an online application store or users may be vulnerable if they are using jailbreak/root kits to bypass their Mobile Device Management (MDM) corporate solutions. Unfortunately, when a mobile is affected by mobile malware the worst case scenario is that they may obtain full remote escalated privileged access or root access to the device that would give them full access to the data available through your mobile device. If the device is used to access your corporate network or corporate email then the cyber criminal would have access to this data as well. The cyber criminal may also be able to perform functions such as remotely make a phone call and send texts, take pictures, stream video and audio, open a URL in the internet browser, delete call logs, record calls and audio, intercept text messages, initiate a HTTP DoS flood, open an application and retrieve information like contacts, status, call logs, messages and location.

According to Check Point, mobile users are using new jailbreak/rooting kits to bypass Mobile Device Management (MDM) systems that exposes these mobile devices to exploitation and makes them vulnerable. Gartner is now recommending additional security to mobile devices in addition to MDM. It's worth investing in a reputable mobile IPS (Intrusion Prevention System) client as cyber criminals can buy AV (Anti-Virus) bypassing software for as little as US$7, where the software is able to obscure any known malicious signature pattern. It is also important to ensure applications and mobile operating systems are kept up to date with patches and upgrades to mitigate the threats associated with using older versions of software.

25. http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-dec-2016.pdf
26. http://b2me.cisco.com/en-us-annual-cybersecurity-report-2017
27. https://www.aspi.org.au/publications/cyber-maturity-2016/ASPI-Cyber-Maturity-2016.pdf

# Advanced Persistent Threats

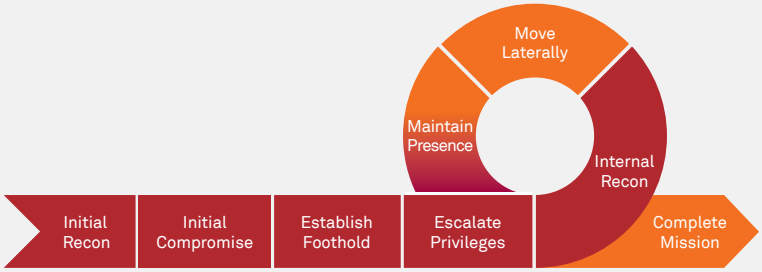
These new waves of targeted cyber-attacks are well researched, co-ordinated, continually evolving and highly sophisticated in nature. Advanced malware that employs many intrusion techniques to evade detection and silently extract company or government information is collectively known as Advanced Persistant Threats (APTs).

APT threat actors use social engineering reconnaissance to research a target organisation and initial victim. Further investigation is performed on the target IT infrastructure to gather further information including: network topologies, domains, DNS and DHCP servers, internal IP addressing and exploitable ports and services. The initial compromise is typically achieved through spear-phishing emails or a malicious payload delivered from a compromised website. Many APT attacks utilise zero-day vulnerabilities to evade detection, where once the zero-day exploit executes on the device it delivers malware to install a backdoor to communicate back to Command and Control (C&C) servers and/or obtain root access on the compromised device. The attacker then harvests access credentials from users to obtain escalated privileges. The persistent nature of an APT attack is achieved through establishing presence by deploying backdoors on multiple computers that are used to communicate back to C&C Servers. These are used for remote discovery activities and then moving laterally to the targeted systems to exfiltrate the desired data.

According to our survey in 2016, 22 per cent of Australian respondents and 26 per cent of Asian businesses experienced an APT attack on at least a monthly basis and reported an increasing recovery time compared to the 2015 survey results. These results indicate that the time to remediate and recover from an APT attack is getting more complex. The research from Mandiant indicates the extent of the remediation activity required for these threats is extensive with the average number of compromised machines found equal to 78 and an average time the compromises went undiscovered of 17 months.[28]

CrowdStrike research has found that China appears to be the most active in carrying out targeted intrusion activity in the APAC region; however, they have seen a good amount of activity from adversaries in India and Pakistan this year, but much of this is focused on each other. At the 2015 G20 Summit in Turkey, there was a provision discussed that has led to a number of informal international agreements between China and some G20 countries and includes provisions relating to commercial cyberespionage and hacking outlined in Paragraph 26 in the G20 Leaders' Communiqué. Paragraph 26 is clearly aimed at addressing specifically commercial cyberespionage. The communiqué leaves room for the pursuit of legitimate intelligence and national security activities, but distinguishes those activities from the 'theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.'[30] China has established new bilateral cyber security agreements with the US, UK, India,and Russia covering issues including intellectual property theft and cybercrime. [31]

## APT attack life cycle model shows the typical phases of an attack[29]




**The Initial Recon**
Socal engineering reconnaissance of target organisation and network infrastructure investigation.

**The Initial Compromise**
May be through a spear-phishing email or strategic web compromise.

**Establish Foothold**
Move laterally within the environment to establish persistence by deploying backdoors on multiple computers. Backdoors are programs for communicating back to C&C servers on the internet.

**Escalate Privileges**
Steals privileged credentials.

**Internal Recon**
To identify their target data.

**Move Laterally**
Infiltrating other computers or servers through further reconnaissance and credential theft.

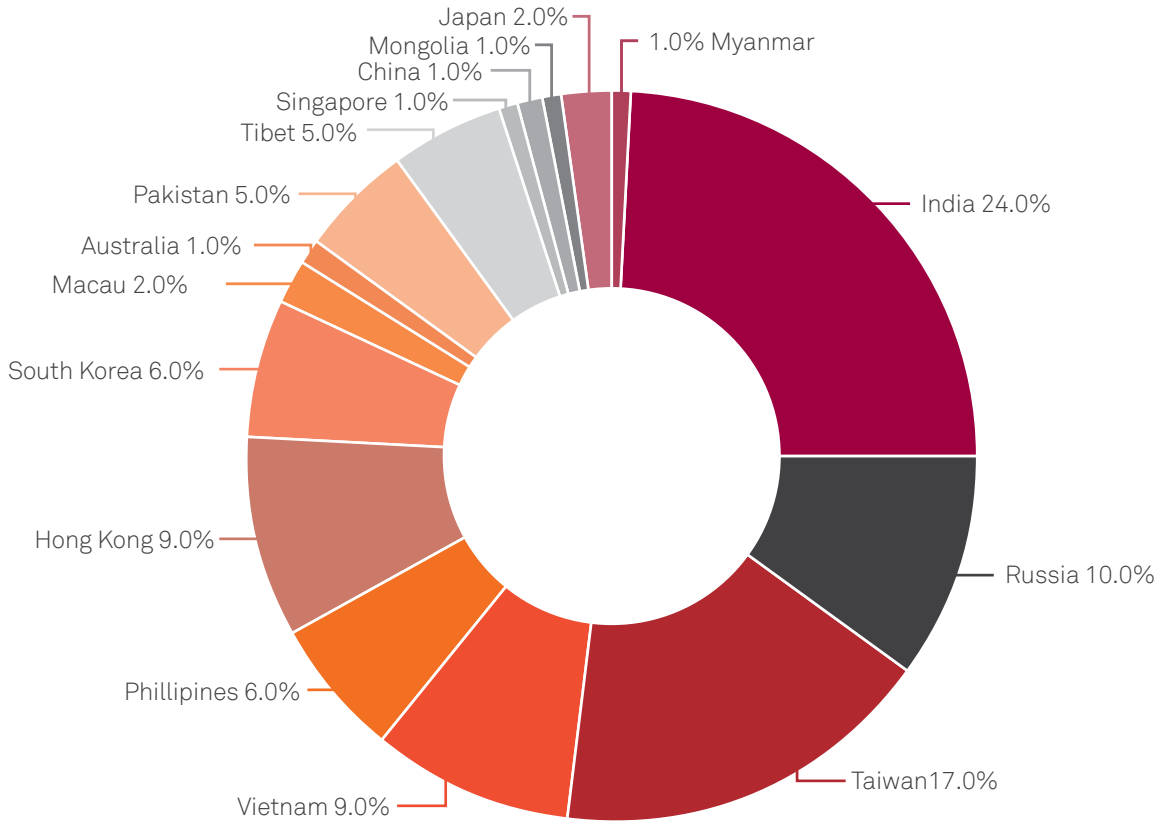
**Maintain Presence**
Establish multiple backdoors to C&C servers and typically removal of malware once privileged credentials are obtained.

**Complete Mission**
Exfiltrating and stealing sensitive data.

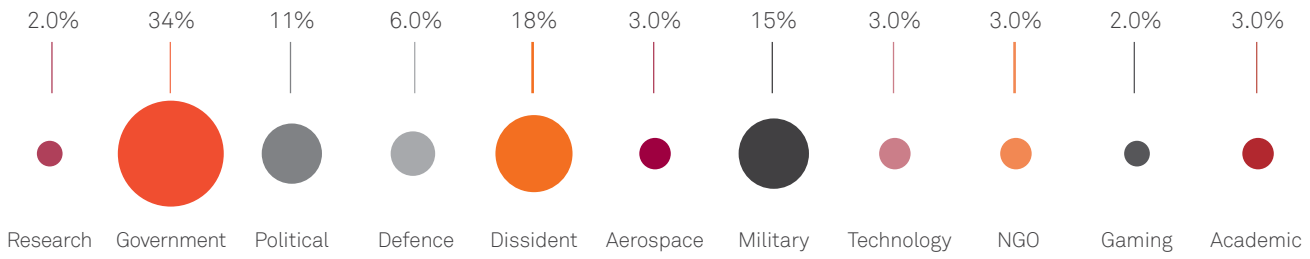
In the ICT environment, just as elsewhere, states have a special responsibility to promote security, stability, and economic ties with other nations. In support of that objective, we affirm that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors. All states in ensuring the secure use of ICTs, should respect and protect the principles of freedom from unlawful and arbitrary interference of privacy, including in the context of digital communications.[32]

28. https://www2.fireeye.com/m-trends-2016-asia-pacific.html
29. http://resources.infosecinstitute.com/anatomy-of-an-apt-attack-step-by-step-approach/#gref
30. https://www.lawfareblog.com/cyber-sections-latest-g20-leaders-communiqu%C3%A9
31. https://www.aspi.org.au/publications/cyber-maturity-2016/ASPI-Cyber-Maturity-2016.pdf
32. A brief extract from Paragraph 26, in the G20 leaders' communiqué is provided:https://www.lawfareblog.com/cyber-sections-latest-g20-leaders-communiqu%C3%A9

## APT statistics by targeted country in APAC region – CrowdStrike




## APT statistics by sector in APAC region – CrowdStrike



## Mandiant – APAC Incident Response investigation statistics for 2015[33]

| APAC IR Response Results | Quantity (Average) |
|---|---|
| Number of days compromise went undiscovered (median) | 520 |
| Number of machines analysed in an organisation | 21,584 |
| Number of internet points | 4 |
| Number of compromised machines | 78 |
| Number of user accounts compromised | 10 |
| Number of admin accounts compromised | 3 |
| Average amount of stolen data | 3.7GB |

The APT statistics, provided by CrowdStrike, indicates that the focus of APT activities in the Asia Pacific region is primarily against Government departments, political organisations, dissident groups opposing official policy of a ruling entity, military and defence organisations who supply arms and technology.

These results align with the informal bilateral agreements that have been agreed to in regards to protecting intellectual property, trade secrets and confidential business information with the exclusion of activities associated with cyberespionage.

**Key Mandiant APAC Findings:**

- The majority of breaches never made news headlines as most governments and industry-governing bodies did not report breaches.
- Many organisations had conducted forensic investigations in the past but failed to eradicate the attackers from their environments. They sometimes made matters worse as they destroyed or damaged forensic evidence needed to understand the full extent of a breach or to attribute activity to a specific threat actor/group.
- Average machines analysed in an organisation = 21,584. Comprehensive investigations are required to cover every system in the environment to understand the full extent of the breach and remediate effectively. Otherwise you risk tipping off the attackers and being re-compromised.
- Average compromised machines = 78. Once an attacker has full access to an environment with escalated privileges they minimise the number of compromised machines and typically remove the malware and migrate to use corporate remote access solutions. The compromised systems now have no malware installed making them undetectable to Anti-Virus and End Point Protection solutions.
- Average user accounts compromised = 10 and average admin accounts compromised = 3. Investigators must hunt for threat actors who pose as 'insiders' using legitimate credentials. Determining which compromised credentials were used during the attack is critical to understanding the full extent of a breach.
- The average amount of stolen data = 3.7GB. Likely to be under reported as this is based on the forensic data available during the investigation and sometimes there are missing log files, which may be due to some logs being overwritten over time due to storage constraints.
- Classification of information stolen from APAC organisations was 40 per cent email, 20 per cent sensitive documents, 20 per cent Personally Identifiable Information (PII) and 20 per cent Infrastructure Documents.[34]

**APT Mitigation Recommendations:**

- Conduct phishing awareness training to mitigate initial compromises.
- Ensure operating systems are supported and patch maintenance is performed and enable automatic updates, if possible, to minimise vulnerabilities on your devices and host servers.
- Conduct regular penetration tests and external and internal vulnerability scans and then implement security plans to mitigate the prioritised vulnerabilities and weaknesses found.
- Deploy advanced end point protection on both laptops/desktops and host servers.
- Deploy Mobile Intrusion Prevention System (MIPS) and Mobile Device Management (MDM) to provide security protection for mobile devices.
- Deploy appropriate network segmentation and User and Entity Behaviour Analytics (UEBA) within your network to identify any behavioural anomalies' to protect your key data assets.
- Ensure number of staff with administrator passwords is limited based on business need, not easy to obtain/guess and unique across multiple IP domains.
- Ensure that you have incident response plans in place and that you review and test them regularly to ensure that you are prepared to respond and remediate incidents in a timely fashion.
- Consider the use of inherence factors from electronic and biometric security data for additional authentication.

33. https://www2.fireeye.com/m-trends-2016-asia-pacific.html
34. https://www2.fireeye.com/m-trends-2016-asia-pacific.html

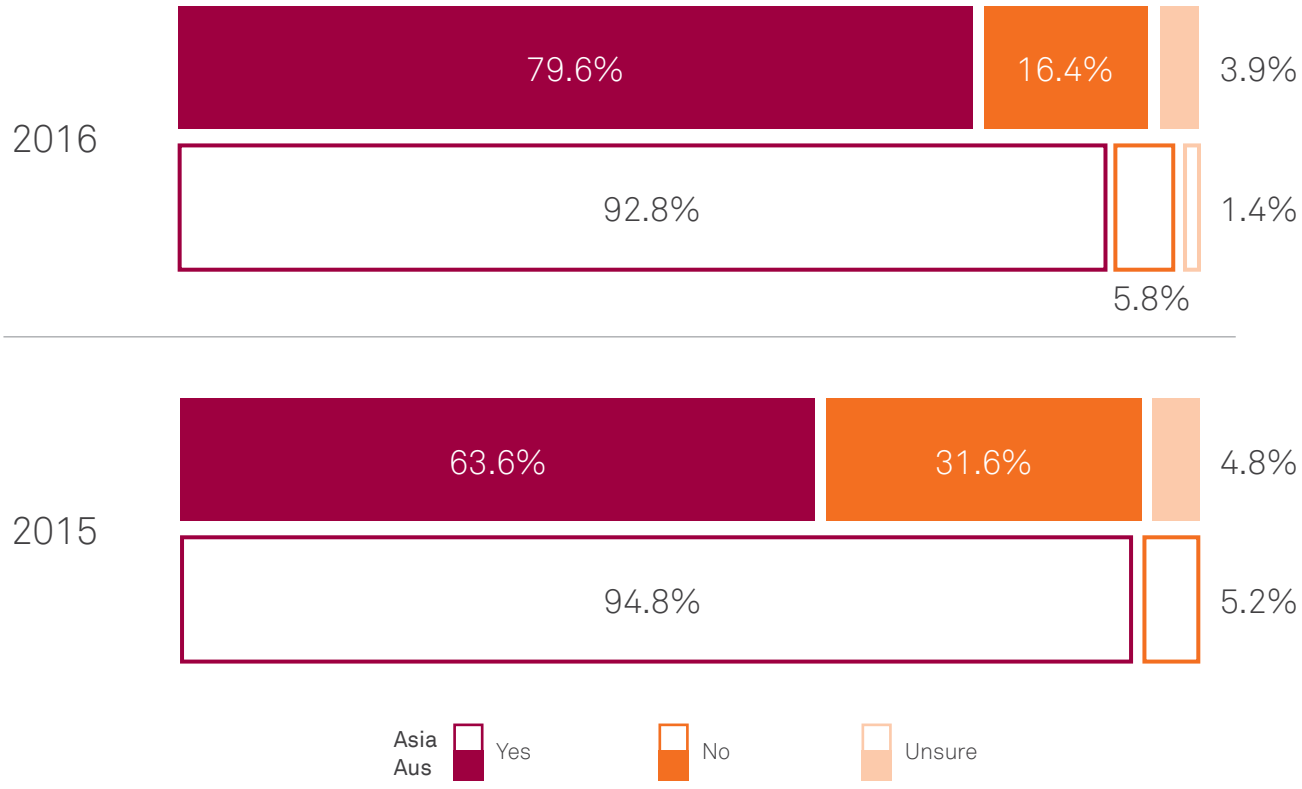
# Cloud security

The migration of applications and services to virtualised private and public cloud environments is not surprising due to the speed, flexibility and ease of application deployments. Traditional data centres add months to these new application deployments and aren't very scalable; however, the security is simpler as the traffic only travels between servers and the security gateway in a north-south direction so all traffic is inspected for threats by the security gateway. The security implications of running applications and services in these virtualised cloud environments or software defined network environments need to be considered as the traffic changes to allow east/west data flows of up to 80 per cent between virtualised applications and network sectors. [35] This east/west traffic is effectively able to bypass the perimeter security gateway and is therefore not visible or controlled within the virtual cloud environment. Security management is complicated further due to the dynamic nature of these virtualised applications that are able to be moved between host servers as their resource demands change. The rise of mobile applications and cloud based environments means that there is a heightened risk of malware spreading laterally throughout your IT environments.

Therefore, to maintain IT security in virtualised public and private clouds, it is important to segment your network, users and applications by using a virtual secure gateway at the switch layer to obtain visibility and control of any malicious traffic moving laterally in your cloud environment. High visibility and control of cloud based applications, network segmentation and user groups is critical for securing cloud-based applications and services through a centrally managed, software-based, distributed micro-segmented security solution.

According to our research, 93 per cent of the respondents in Asia have indicated they are currently using cloud services compared to 80 per cent of Australian respondents. The adoption of cloud services amongst Australian organisations was 80 per cent in 2016 up from 64 per cent in 2015. According to F5, 47 per cent of respondents in Asia Pacific (excluding Japan) indicated that on-premise private clouds will see the largest amount of investment in 2017 and Asia-Pacific leads the other regions in cloud-first strategies with 54 per cent reporting a cloud-first preference before making new IT investments. However, almost 33 per cent of Asia Pacific respondents expressed concerns with implementing consistent cloud security policies, according to F5.[36]

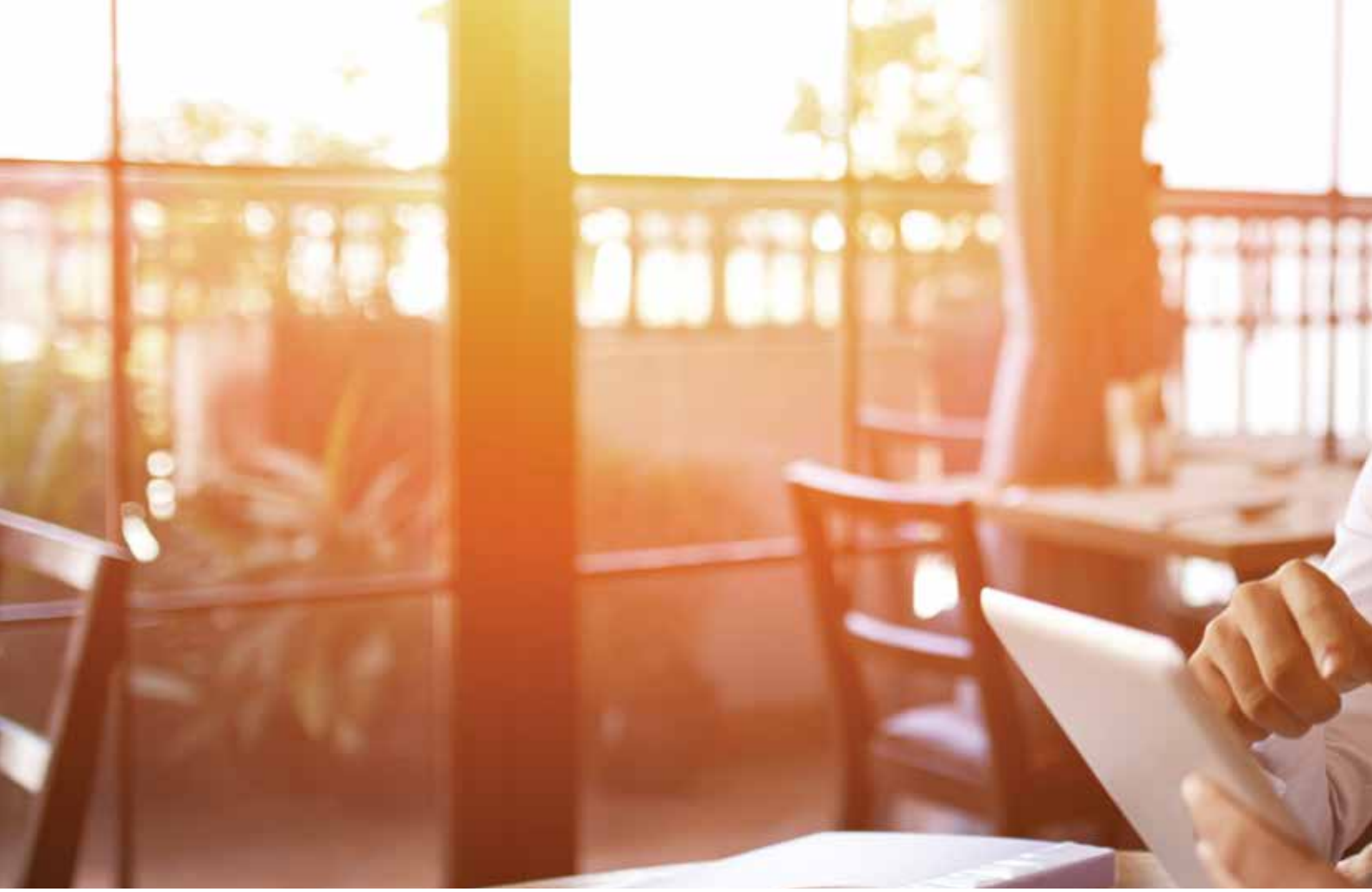
## Organisations using cloud services year on year trend – in Australia and Asia




35. http://pages.checkpoint.com/security-report.html
36. https://f5.com/about-us/news/the-state-of-application-delivery

## Ranking of potential risks due to adoption of cloud services – Asia and Australia


## Organisations' level of readiness to handle cloud service risks – Asia and Australia



## Cloud Security

'Theft of company data' was the most nominated top potential risk of adopting cloud services by both Australian and Asian organisations. Australian respondents were also concerned about 'employee actions/human error', whilst Asian respondents were also concerned about 'network attacks or outages'.

However, in the survey results from 2015, 'data sovereignty' was rated as the top potential risk of adopting cloud services. Our research indicates that this is due to the increasing presence of local cloud service providers in Asia, so data sovereignty has become less of a concern for Asian enterprises. The focus now shifts towards effective security controls to mitigate risks of using cloud services, such as SaaS, where 80 per cent of Australian respondents and 95 per cent of Asian respondents are already adopting or considering adopting Cloud Access Security Broker (CASB) solutions. This further supports the notion that the paradigm has shifted from whether to migrate to the cloud to, "How can I secure my data in the cloud?"

Data theft from cloud services remains a top concern.

The majority of respondents from Asia indicate that they are ready to handle all the cloud adoption risks in the survey.

However, respondents from both Australia and Asia have the lowest confidence in their ability to handle the 'theft of company data'. The survey indicates that 43 per cent of Asian respondents are prepared to manage the risks of data theft, whilst 27 per cent of them classify theft of corporate data to be their top threat. This suggests that despite the fact that most organisations are either currently using or considering the use of the latest cyber security tools, they still lack the confidence in dealing with data theft incidents in the cloud. Australia is even less confident in dealing with cloud related data theft incidents compared to their Asian counterparts. This could be attributed to the fact that many organisations are lacking the visibility into privileged users that have access to the data stored in private clouds on-premise or in public cloud environments. The lack of controls in place makes it harder for organisations to detect or identify internal threats that may cause the loss of corporate data. In addition, the shortage of skilled security professionals and/or IT security resources to manage these cloud related security risks adds an additional layer of complexity to managing the security threats when adopting cloud services.

## Shadow IT Data Exposure Risks

Shadow IT refers to the adoption and use of applications/services by employees without the knowledge or consent of the IT department. Gaining visibility and control of these cloud applications is an important step for cloud security. Even when an organisation has implemented a successful Shadow IT policy that limits employees to use of sanctioned enterprise applications, like Box or Salesforce or Office365, there is still a risk of data being exposed due to compromises through users uploading and sharing sensitive data.[37]

**Insights into cloud application usage:**

- An enterprise has, on average, 841 cloud applications in use.
- 11 per cent of enterprise cloud apps are still vulnerable to one or more major exploits.
- 71 per cent of business cloud apps do not provide multi-factor authentication.

37. http://images.machspeed.bluecoat.com/Web/BlueCoat/%7B2f3a44c7-7445-442a-9425-de48041ab3c9%7D_ShadowDataReport_1H_2016_Digital-Screen_compressed.pdf

- 87 per cent of cloud applications do not adequately encrypt data. Only 13 per cent of business applications encrypt data at rest and 85 per cent use SSL to secure data in transit. If your business application is used for Personally Identifiable Information (PII) or Payment Card Industry (PCI) data then it should encrypt data at rest and in transit.
- 23 per cent of all files stored in the cloud are broadly shared (within the whole organisation, with third parties and publically on the internet) and 12 per cent of these broadly shared files contain sensitive data.
  - 43 per cent of the broadly shared documents contain source code e.g Java, Python, etc.
  - 36 per cent of the broadly shared documents contain PII data.
  - 14 per cent of the broadly shared documents contain PHI data.
  - Six per cent of the broadly shared documents contain PCI data.
- Unfortunately, the percentage of PII and PCI exposed data has increased compared to last year's report from 33 per cent to 36 per cent and five per cent to six per cent respectively but the good news is that exposure of source code data has decreased from 48 per cent to 43 per cent compared to last year's report.
- The potential financial impact on the average organisation from the leakage of sensitive cloud data was just over US$2 million compared to US$1.9 million in the previous year.[38]

**Shadow IT Cloud Recommendations: Discovery Phase**

- Discover the cloud applications that are being used.
- Identify suitable applications to be endorsed by the business, based on business risk, and block unsuitable applications.

**Monitoring Phase**

- Monitor how employees and external users are sharing and collaborating with applications.
- Monitor data sharing to ensure that it is appropriate and not shared indiscriminately.
- Determine if accounts or devices have been compromised and for risky exploit/data exfiltration.
- Determine users' risk rating to your organisation.
- Monitor data that is stored and shared in the cloud: Source code, PII, PHI or PCI data.

**Governance and Control Phase**

- Develop a cloud governance strategy.
- Develop guidelines for approved or blocked cloud applications and vendors.
- Develop Acceptable Use Policy for Cloud Applications based on departments/roles.
- Establish Data Classification scheme and establish a corporate usage policy.
- Define and develop a Data Loss Prevention policy that defines the types of sensitive data and risk assessment if exposed.
- Develop an Incident Response Plan for when/if sensitive data is exposed.[39]

38. http://images.machspeed.bluecoat.com/Web/BlueCoat/%7B2f3a44c7-7445-442a-9425-de48041ab3c9%7D_ShadowDataReport_1H_2016_Digital-Screen_compressed.pdf
39. http://images.machspeed.bluecoat.com/Web/BlueCoat/%7B2f3a44c7-7445-442a-9425-de48041ab3c9%7D_ShadowDataReport_1H_2016_Digital-Screen_compressed.pdf

# Web and application vulnerabilities

According to Qualys, there is no slow-down in the rate of new vulnerabilities that were found during 2016 with an increase of 16 per cent in total vulnerabilities seen, compared with 2015. Looking at the top 10 vulnerabilities found for both external and internal networks in the Asia Pacific region, it is clear that remediation activities are still lagging with the majority of these vulnerabilities disclosed in 2014 or earlier. 80 per cent of vulnerability exploit kits are now available within a few days of the vulnerability's public release if not already available.

Secure Socket Layer (SSL) and other encryption technologies like Secure Shell (SSH) were developed to provide secure online communication but the delays with organisations implementing patch management is leaving organisations exposed to cyber criminals eavesdropping on these 'secure' communications. In terms of the external top 10 vulnerabilities found in the Asia Pacific region in 2016, it is worth noting that five of the top 10 are related to SSL with POODLE[40] and BEAST[41] vulnerabilities still prevalent in 2016. These can be addressed by making the appropriate SSL configuration changes and one of the best resources with recommendations can be found at the following website: https://www.ssllabs.com/projects/best-practices/.

In terms of SSH (OpenSSH), which make up another four of the top 10 external vulnerabilities, keeping up to date with the most recent releases and patching for this software is critical. For the internal top 10 vulnerabilities found in the Asia Pacific region in 2016, SSL implementation again rears its head as the number one internal vulnerability. The uncomfortable reality is that no security control will ever be perfect, so it's best to focus on those controls that have the biggest impact in reducing risk while optimising an automated approach for implementing and measuring these controls to maintain continuous security and compliance.

It's not easy being a CISO or CIO today, with the advent of cloud computing, Shadow IT, and mobility, and with increasing convergence with electronic security, the surface area of risk for enterprises has increased dramatically, while IT budgets for patching and upgrades is constrained and skilled cyber security talent is difficult to find. No two vulnerabilities are equal and are different for each environment, which is dependent on technology and controls. Therefore you cannot treat all vulnerabilities with the same priority level as you will leave dangerous gaps that attackers are actively trying to exploit. The question is how to prioritise and know which vulnerabilities should be immediately addressed, especially when new vulnerabilities are being disclosed every day.

To clearly and precisely prioritise remediation work, security teams must correlate the steady stream of vulnerability disclosures against their organisation's IT asset inventory, a connect-the-dots process that requires intense data analysis. Today, organisations live in a perimeter-less world. Those clearly defined physical boundaries in which their IT infrastructure were housed have been pushed out, blurred, transformed and in some cases even erased. It is therefore critical that as a first step organisations need to gain visibility of their assets and their security posture that is unique to their business and its supporting systems.

According to our survey results, 23 per cent of Australian businesses experienced a web application attack on at least a monthly basis and 26 per cent said that it took five hours or more to recover from these types of attacks. 29 per cent of Asian businesses experienced a web application attack on at least a monthly basis and 24 per cent of respondents in Asia said that it took five hours or more to recover from these types of attacks.

## Top 10 external and internal vulnerabilities in Asia Pacific region in 2016 – Qualys

| Rank | External vulnerability name | Qualys ID |
|---|---|---|
| 1 | SSL/TLS use of weak RC4 cipher | 38601 |
| 2 | SSL/TLS Server supports TLSv1.0 | 38628 |
| 3 | SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE) | 38603 |
| 4 | SSL Server Has SSLv3 Enabled Vulnerability | 38606 |
| 5 | SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST) | 42366 |
| 6 | Windows Remote Desktop Protocol Weak Encryption Method Allowed | 90882 |
| 7 | OpenSSH LoginGraceTime Denial of Service Vulnerability | 42413 |
| 8 | OpenSSH Commands Information Disclosure Vulnerability | 42382 |
| 9 | OpenSSH "X SECURITY" Bypass Vulnerability | 38611 |
| 10 | OpenSSH Xauth Command Injection Vulnerability | 38623 |

| Rank | Internal vulnerability name | Qualys ID |
|---|---|---|
| 1 | SSL/TLS use of weak RC4 cipher | 38601 |
| 2 | SMB Signing Disabled or SMB Signing Not Required | 90043 |
| 3 | Enabled DCOM | 90042 |
| 4 | Administrator Account's Password Does Not Expire | 90080 |
| 5 | Oracle Java SE Critical Patch Update – October 2012 | 120604 |
| 6 | Oracle Java SE Critical Patch Update – June 2013 | 121279 |
| 7 | Insecure Microsoft Internet Explorer Intranet Zone User Setting Detected | 100012 |
| 8 | Oracle Java SE JVM 2D Subcomponent Remote Code Execution Vulnerability (Oracle Security Alert for CVE-2013-1493) | 120970 |
| 9 | Microsoft Windows Gadgets Remote Code Execution Vulnerability (KB2719662) | 90961 |
| 10 | EOL/Obsolete Software: Microsoft XML Core Services 4.0 Service Pack 2 Detected | 105458 |

40. https://www.wired.com/2014/10/poodle-explained/
41. https://blog.qualys.com/ssllabs/2013/09/10/is-beast-still-a-threat

# Denial of Service (DoS) attacks leveraging the Internet of Things (IoT)

## DDoS Overview

Distributed Denial of Service (DDoS) attacks are an attempt to make an online service unavailable by overwhelming it with traffic from multiple compromised devices. DDoS attacks are growing significantly year-on-year with Imperva experiencing 100 per cent[42] growth of both Network and Application layer attacks and Akamai seeing a 71 per cent increase in total DDoS attacks globally.[43] One of the main drivers behind this is the increasing use of DDoS-for-hire services that enable anyone to launch attacks for as little as US$5 per minute.[44] The ease of access to these services means that anyone can launch an attack, from cyber criminals and activists to disgruntled customers or employees, which means that any business is a potential target. Cyber criminals can easily turn a profit by sending DDoS extortion requests for Bitcoin payments and using DDoS-for-hire services to launch their attacks. Criminal perpetrators of DDoS attacks often target services on e-commerce web servers, which can lead to a loss of sales revenue, business disruption, and reputational damage and in some cases used to hide network breaches and the extraction of sensitive data. The waves of DDoS attacks are likely to increase in volume and quantity with the advent of new malware targeting unsecured internet-enabled devices that can be used to launch these attacks. According to our survey in 2016, 59 per cent of Australian businesses experienced a DDoS attack on at least a yearly basis and reported a recovery time within 30 minutes (36 per cent). 68 per cent of Asian businesses experienced a DDoS attack on at least a yearly basis. 43 per cent of respondents in Asia indicated that the time to recover from these attacks was within 30 minutes.

## New DDoS Attack Utilising IoT Devices

On the 20 September 2016, the website of cyber security writer and blogger, Brian Krebs, (www.krebsonsecurity.com) was on the receiving end of a 623 Gbps attack, the biggest attack that Akamai had ever mitigated to date, which used IoT

42. https://www.imperva.com/docs/gated/2015-16-DDoS-Threat-Landscape-Report.pdf
43. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q3-2016-state-of-the-internet-security-report.pdf
44. https://www.imperva.com/docs/gated/2015-16-DDoS-Threat-Landscape-Report.pdf

devices including CCTV cameras, Digital Video Recorders (DVRs) and routers to launch the attack.[45] Subsequently, on 30 September 2016, a HackForum user by the name of 'Anna-senpai' leaked the source code for the botnet malware behind this attack called Mirai.[46] Imperva found that Mirai botnets were also behind a similar GRE DDoS attack on 17 August with peak network/application layer attacks of 280 Gbps and 130 Mpps. Imperva uncovered 49,657 unique IPs in 164 different countries with Mirai-infected devices.

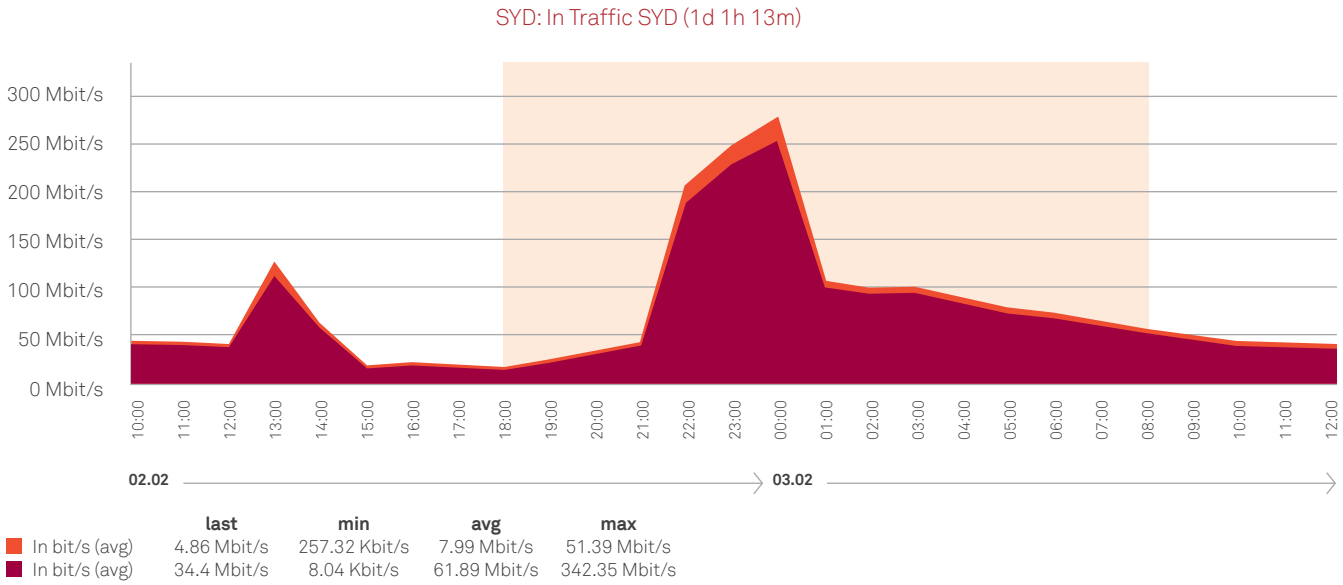
Mirai is a piece of malware that infects IoT devices and is used as a launch pad for DDoS attacks from a remotely distributed Command and Control (C&C) system.

1. Mirai performs wide-ranging scans of IP addresses to locate unprotected IoT devices that are remotely accessible.
2. The next stage is to use a brute force login technique for guessing passwords based on a dictionary list of more than 60 default usernames and passwords to gain remote access to the device.
3. Once it has control, it has several scripts that eradicate other malware and prevent other malware from hijacking the device by prohibiting remote connections.
4. Mirai's attack function enables it to launch application and various network (OSI layer 3-4) DDoS attacks at its intended target by its C&C system.[47]

Juniper performed audits of firewall configurations and identified that approximately 30-35 per cent of hosted customers have created security policies to explicitly permit all telnet traffic from the untrusted internet. This could allow a threat actor to obtain remote admin access to their infrastructure using a similar brute force login technique to obtain an appropriate username/password and is not a recommended security practice.

45. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q3-2016-state-of-the-internet-security-report.pdf
46. https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html
47. https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

## Network DDoS attacks in APAC region – Imperva



## How to Prevent the Spread of IoT Botnets

Everyone can take precautions to prevent their IoT devices from being hijacked by malware and used in DDoS attacks:

- Purchase IoT devices from reputable manufacturers that provide regular security upgrades/patches on their website to mitigate new security vulnerabilities.
- Update administrator username and passwords to become strong and unique.
- Disable remote access to your devices and block/close unauthorised access using the following protocol ports but not limited to: SSH (22), Telnet (23) and HTTP/HTTPS (80/443).
- Universal Plug and Play (UPnP) and other similar technologies should be disabled on home routers and modems as they automatically program some firewalls which support this technology and pose a potential security risk.
- Perform updates/patching and review changes in features and settings on a regular basis for IoT as per any other computer on your network.
- Ensure staff responsible for Electronic Security and Physical Security are educated on the precautions required when purchasing and deploying security devices such as IP-enabled surveillance cameras.

## Network DDoS Attacks

DDoS attacks have increased by 211 per cent year-on-year. This may be due to the increasing use of DDoS-for-hire services and account for 90 per cent of all network-based attacks.[48] According to Imperva, the majority of these network attacks are under 30 minutes in duration in the Asia Pacific region (60 per cent). The largest network attack seen by Imperva peaked at 470 Gbps but many attacks were over the 200 Gbps and are becoming more frequent.[49] The largest network attack seen in APAC by Imperva peaked at 342 Mbps.

## Application DDoS Attacks

According to Imperva, 46 per cent of all targeted APAC businesses were attacked more than once by application layer attacks and 10 per cent were attacked more than five times, according to Imperva. The increase in multiple attacks could be linked to the use of hit-and-run tactics such as consecutive bursts launched against a target over a long period of time to:

- Exhaust mitigation teams by keeping them on high alert around the clock for weeks.
- Force prolonged activation of on-demand mitigation solutions, often leading to service degradation.
- Create a state of stress and confusion to draw attention away from other malicious activities (e.g. network breach, data extraction, etc.)

The largest application attack seen by Imperva peaked at 80,065 requests per second (RPS) in APAC and 268,000 RPS globally. This is large when you compare it to the fact that most servers can only handle a few hundred RPS. Compared to network layer assaults,it requires far fewer botnet resources to launch application layer attacks and as a result 31 per cent of application attacks last longer than one hour according to Imperva in APAC (compared to 44 per cent globally). Three vectors account for 95 per cent of all web application attacks: SQL Injection (SQLi), Local File Inclusion (LFI) and Cross-Site Scripting (XSS) and the majority of web application attacks continue to take place over HTTP (68 per cent) as opposed to HTTPS (32 per cent).[50]

## How to Mitigate DDoS Attacks

Engage with DDoS prevention specialists to put together a DDoS incident response plan:

- Incorporate business continuity plans into your response plan to ensure that the restoration time frames meet the business requirements.
- Ensure that your key stakeholders, security, operations, customer service groups are engaged so that if a DDoS attack does strike everyone understands their role to ensure there is a co-ordinated response to the attack.
- Communication during an attack is essential so that customers, staff and affected third parties know that you have control of the situation.
- Ensure that the plan protects against both network and application DDoS attacks and test these plans on a regular basis.

The IoT botnet threat has now become a reality and Mirai has shown how easy it is to take advantage of poor security practices within a range of consumer appliances. There are many more IoT devices, such as toys, household appliances and IP-enabled surveillance cameras, which may have similar vulnerabilities and will prove tempting for malware developers. It is highly likely that malicious actors are now working to understand how they can capture their own huge botnet of IoT to create the next tsunami of DDoS attacks. There is also the potential for a range of new types of security breaches if IP-enabled surveillance cameras and electronic access systems are exploited then the potential losses are even greater and could extend beyond network downtime and data losses to the loss of physical assets as well. The manufacturers of these consumer-grade electronics are connecting them to stream data on the internet but many are omitting to build the appropriate security controls and software that can be updated and patched to address new security vulnerabilities.[51]

48. https://www.imperva.com/docs/gated/2015-16-DDoS-Threat-Landscape-Report.pdf
49. https://www.imperva.com/docs/gated/2015-16-DDoS-Threat-Landscape-Report.pdf
50. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q3-2016-state-of-the-internet-security-report.pdf
51. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q3-2016-state-of-the-internet-security-report.pdf

# Security incidents and business impacts

## Frequency of security incidents and future threats

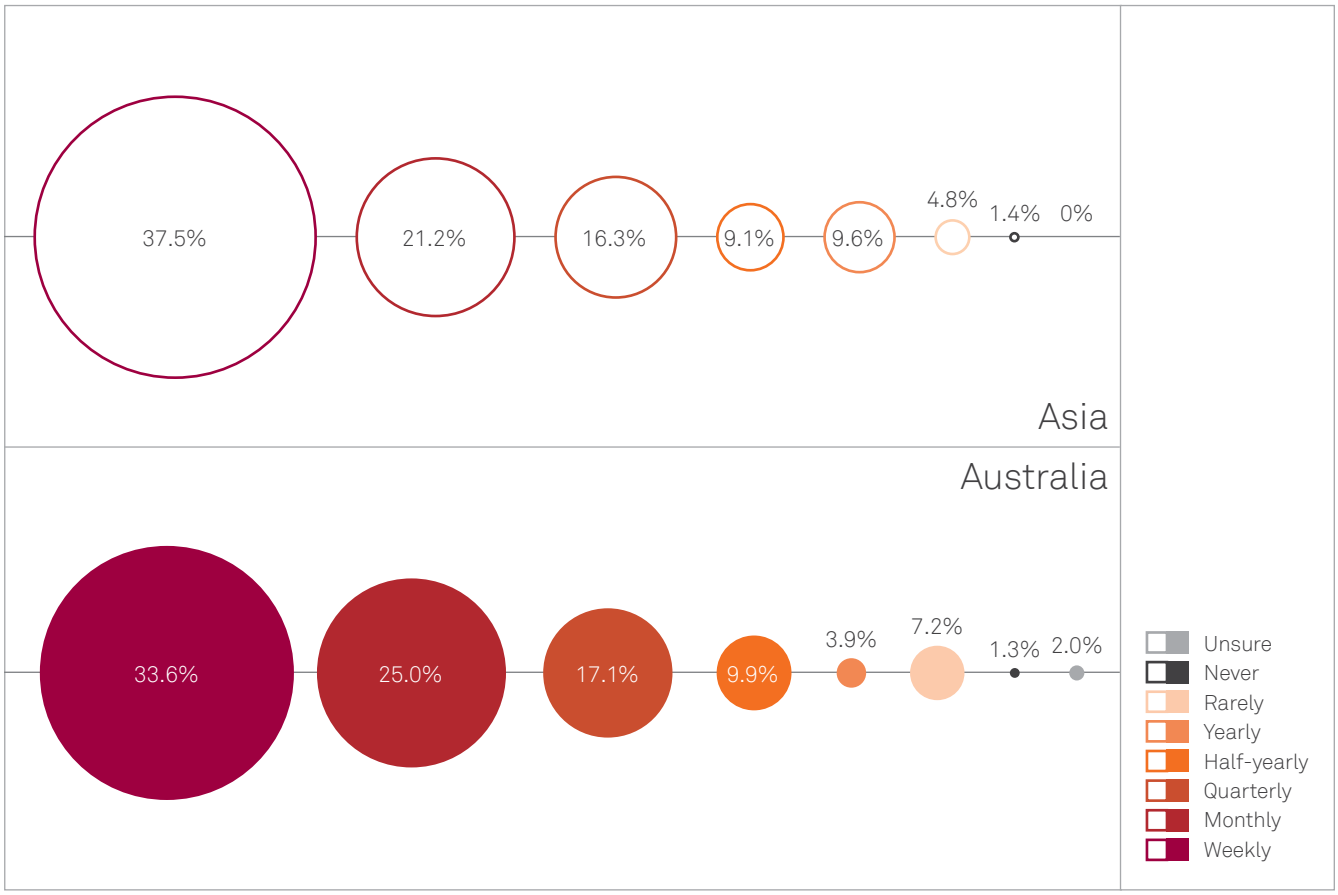
Security incidents are continuing to hit headlines across the world with a number of high-profile data breaches announced in 2016. Not surprisingly, C-suite managers and boards of directors are beginning to understand the importance of implementing appropriate cyber security controls to mitigate these types of incidents and are increasingly taking more responsibility.

Our research found 59 per cent of respondents from both Australia and Asia indicate that their business is impacted by at least one security incident on at least a monthly basis. A small percentage (~one per cent) of organisations indicate that their business is never impacted by any security incident.

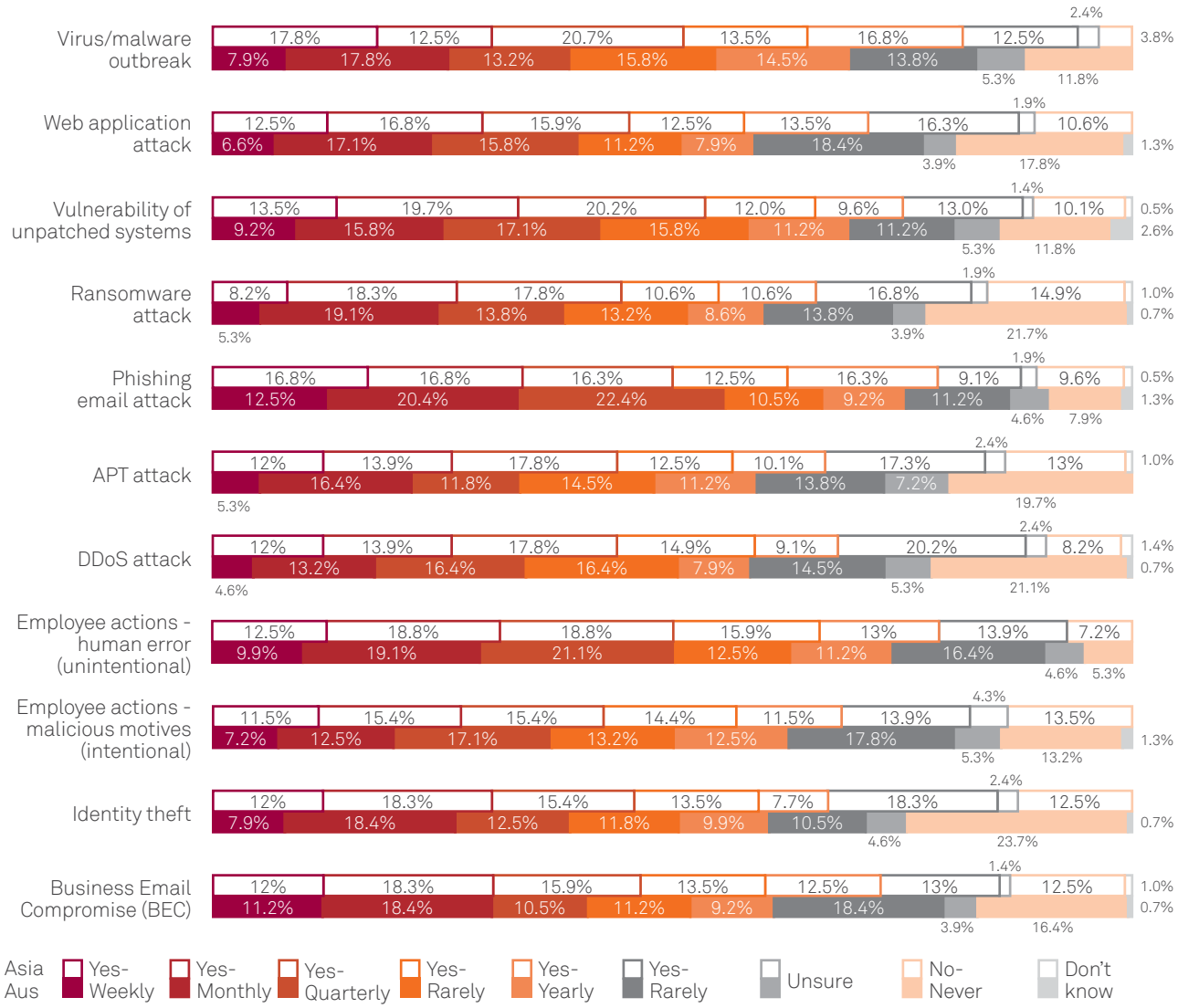
Phishing email attacks and Business Email Compromise (BEC) are the top two incident types occurring on a weekly basis in Australia. In Asia, virus/malware outbreak is the top incident type reported on a weekly basis. Phishing email attacks are selected as the second highest amongst Asian organisations surveyed, with the exception of Singapore who ranked phishing emails as the highest weekly occurring security incidents impacting their businesses. Weekly attacks are reported as impacting Asian organisations more regularly than Australian organisations.

Respondents from both Australia and Asia highlight that external hackers followed by criminal syndicates and then employees are the greatest potential threat to their organisations in the future.

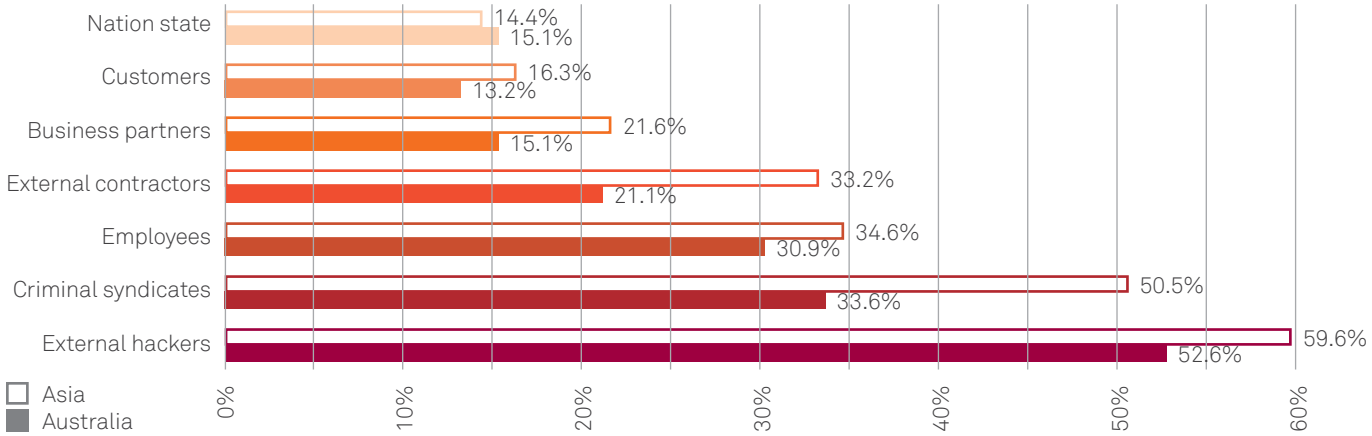
Occurence of business impacting security incidents in 2016 – Asia and Australia



## Occurence of business impacting security incidents in 2016 – Asia and Australia (%)




## Potential sources of future threats – Asia and Australia (%)

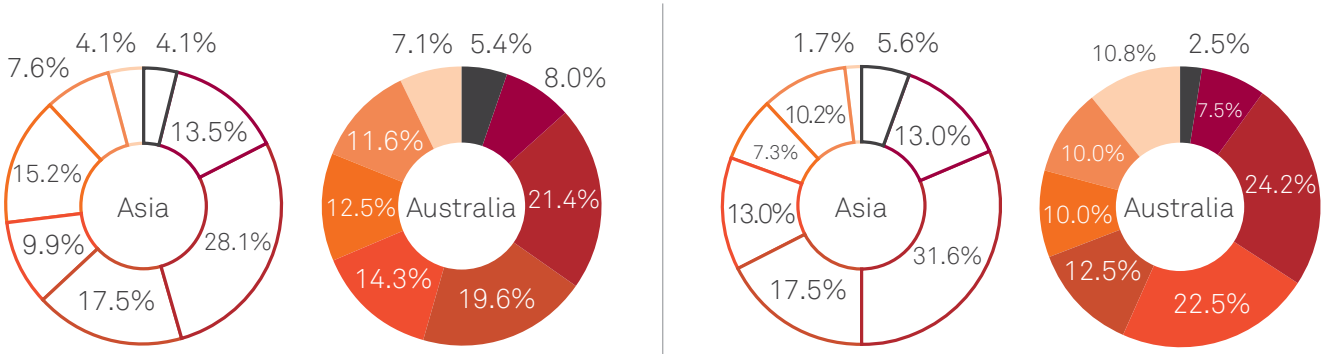


# Business Impacts

Among Asian respondents, the time taken to recover from APT attacks has become significantly slower when compared to 2015. Enterprises in Asia are facing challenges in recovering from any attack, with an increase in the numbers of attacks that require a recovery time of more than 24 hours across all types of attacks in 2016. These results indicate that the time to remediate and recover from an APT attack is getting more complex. The research from Mandiant indicates the extent of the remediation activity required to remove these threats, with the average number of compromised machines of 78 and the average time the compromises went undiscovered was 17 months.[52]

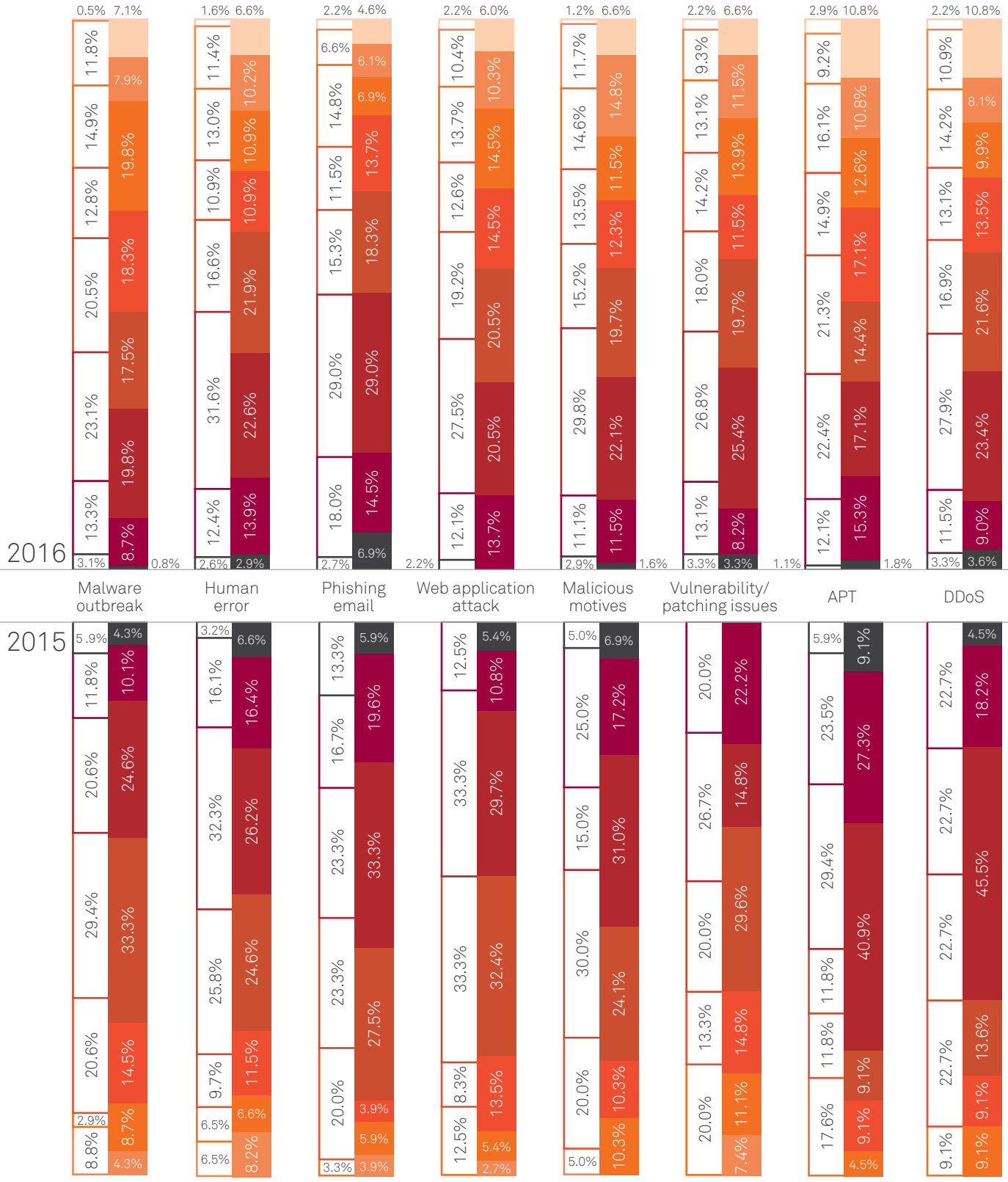
Australian respondents have indicated that both APT and DDoS recovery times in 2016 have slowed when compared to 2015. This may be attributed to the increased sophistication of APTs in Australia and the increased volume of network based DDoS attacks, and the multiple instances of application based DDoS attacks on targeted businesses in the APAC region. According to Imperva, 46 per cent of all targeted APAC businesses were attacked more than once by application layer attacks.

## Recovery time for business-affecting new security incidents in 2016 – Asia and Australia




52. https://www2.fireeye.com/m-trends-2016-asia-pacific.html

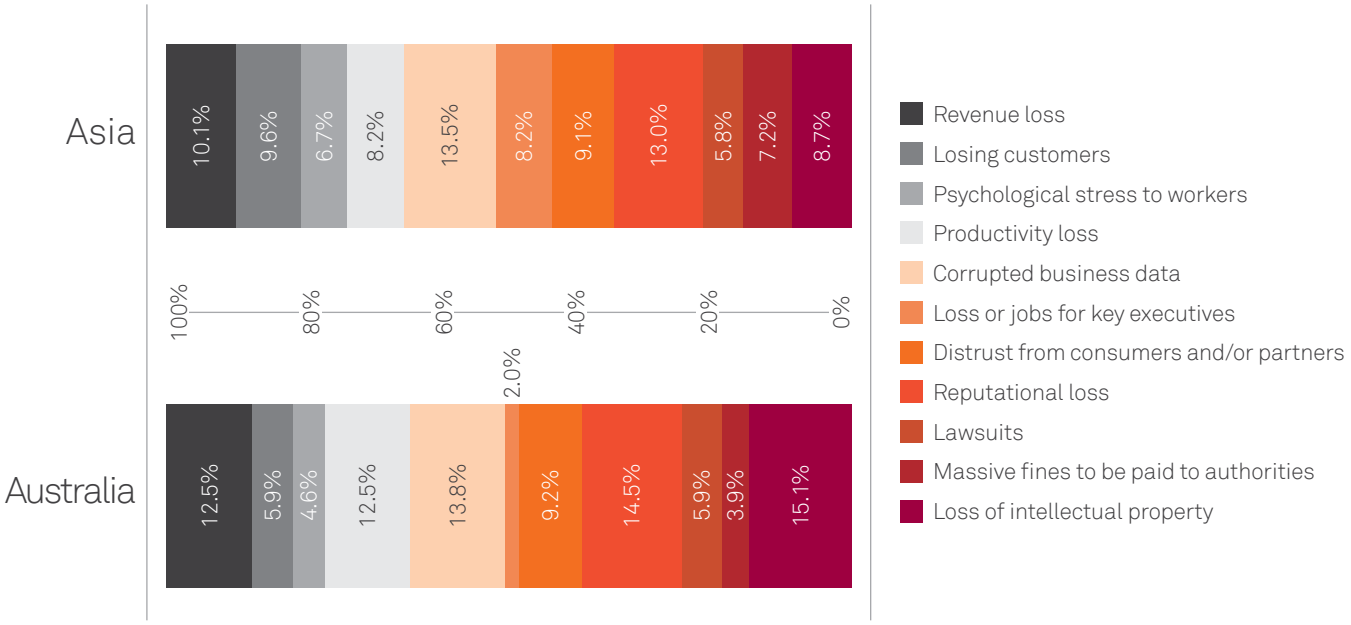
## Recovery time for business-affecting security incidents in 2016 compared to 2015 – Asia and Australia



Whilst 15 per cent of respondents from Australia indicate 'loss of intellectual property' as the most detrimental outcome of a security incident, 14 per cent of Asian respondents highlight 'corrupted business data' and 13 per cent highlight 'reputational loss' as the most detrimental outcome of a security incident.

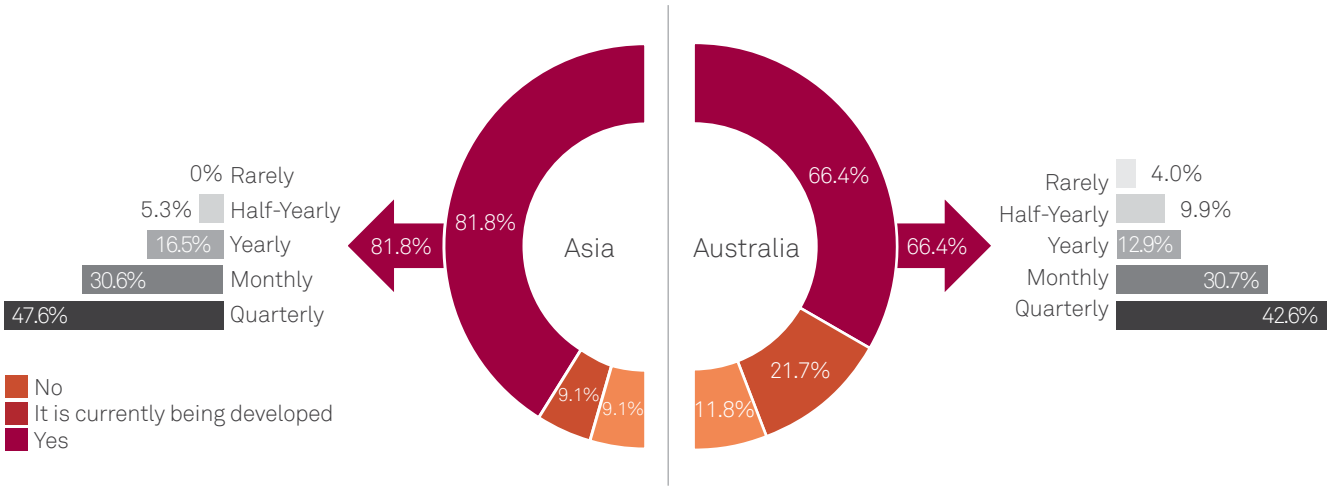
Compared to Asia, Australian organisations surveyed tend to pay more attention to the protection of IP. In general, organisations in both Australia and Asia have to pay greater attention to the series of events that may result in reputational loss when there is a data breach – i.e. web defacements, discovery of leaked company files and customer data dumps, lawsuits with negative press coverage, etc. It is vital that companies put in place incident response plans tailored to address each potential incident. Examples seen recently are enterprises investing in cyber insurance and associated incident response services to mitigate bad publicity in the event of a data breach.

## Top business impacts of security incidents – Asia and Australia




According to our survey, 88 per cent of respondents in Australia and 91 per cent in Asia either have, or are in the process of developing, an incident response plan. Most of these respondents have indicated that they conduct a review and test of their plans on a regular basis, the most common being quarterly. Regular testing and reviews of incident response plans for all the business impacting security incident types is recommended to reduce recovery times, to reduce the impacts to your business processes and to ensure business continuity. The incident response plan also needs to manage communications for key stakeholders and manage notifications to affected parties where private data is compromised.

## Incident response plan in place and frequency of testing and review – Asia and Australia



# Security incidents in Australia

## Australian Government

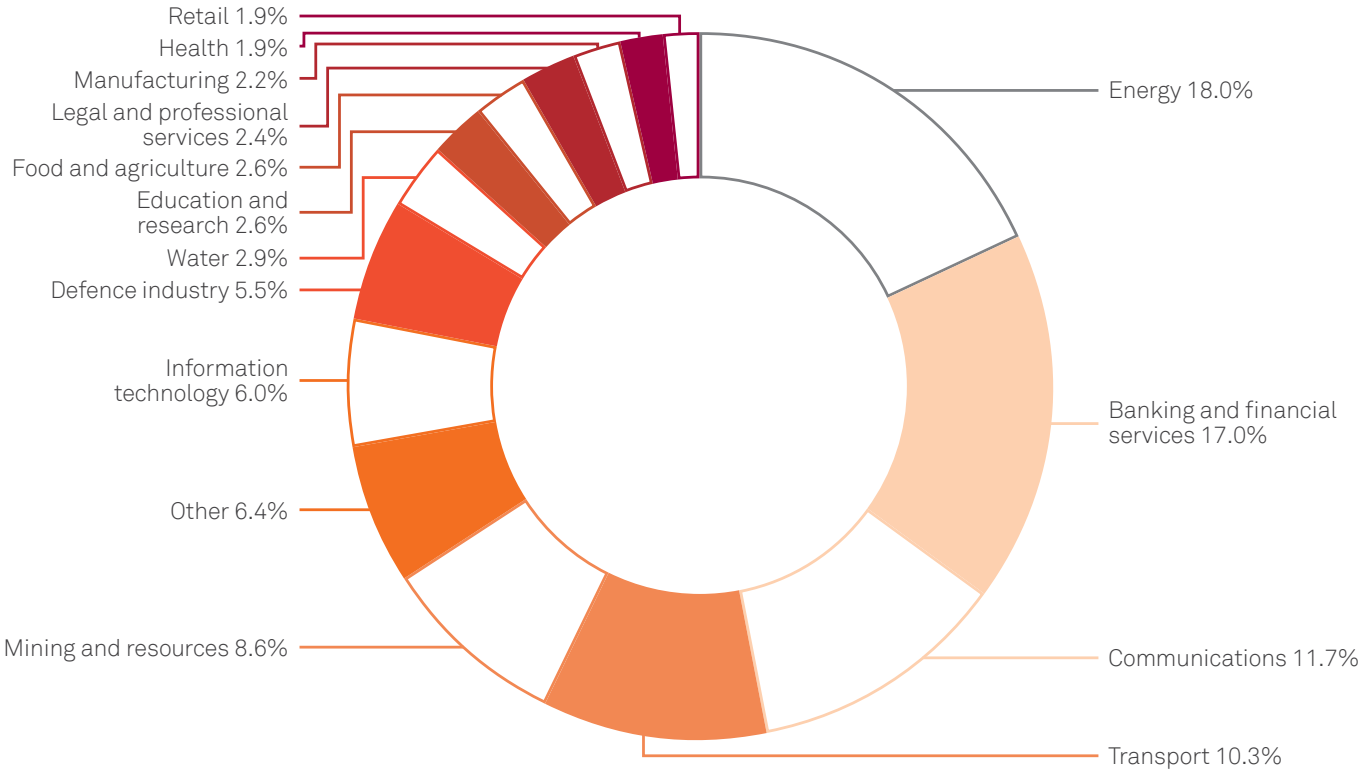
Between 1 January 2015 and 30 June 2016, the Australian Signals Directorate (ASD), as part of the Australian Cyber Security Centre (ACSC) responded to 1,095 cyber security incidents on government systems that were serious enough to warrant operational responses. The good news is that the number of incidents are reducing due to improved security awareness and government organisation improvements in managing low level cyber security incidents. Australian Government organisations are required to report incidents to improve ACSC's understanding of the threat and to gain experience to assist other organisations facing similar threats.[53]

## Australian Industries

Between 1 January 2015 and 30 June 2016, CERT (Computer Emergency Response Team) Australia responded to 14,804 cyber security incidents affecting Australian businesses, 418 of which involved systems of national interest (SNI) and critical infrastructure (CI). CERT relies on the voluntary self-reporting of cyber security incidents from a wide variety of sources both in Australia and internationally. This assists ACSC to develop a better understanding of the threat environment and will be used to assist other organisations who are at also at risk.[54]

According to CERT Australia, the energy and communications sectors had the highest number of reported compromised systems. The banking and financial services and communications sectors had the highest incidence of DDoS activity and the energy and mining/ resources sectors had the highest number of malicious emails being received.

## Incidents affecting Systems of National Interest (SNI) and Critial Infrastructure (CI) by Industry Sector[55]




53. https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf
54. https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf
55. https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf

# Financial impacts due to privacy data breaches

The financial impacts for all the different types of cyber security incidents is difficult to quantify as the extent of an incident and the business impacts can reach far and wide and require an in-depth analysis and investigation of both the incident and associated costs. The full costs of an incident may include brand and reputation damages, PR costs, investigation, incident response services, IT infrastructure repairs, defence and legal fees, regulatory penalties and fines, ransom demands, business interruption and loss of revenue, loss of customers, loss of IP, public apologies and incident notifications to impacted customers/staff/organisations and privacy commissioner.

The Cost of Data Breach Study in Australia by Ponemon provides an insight into the costs and impacts due to the loss or theft of protected personal data. The study examined the costs incurred by 26 Australian companies after the loss or theft of protected personal data. These costs are based on estimates due to actual data loss incidents over a 10-month period. A$2.64 million is the average total cost of the data breach within Australia, which is good news when compared to the average cost in 2015 of A$2.82 million and the Global average total cost of a data breach of US$4 million. The number of breached records per incident ranged from 4,000 to 68,700 records. The average number of breached records in 2016 was 19,663. The average size of a data breach increased slightly compared to the previous years results with two per cent more records lost or stolen but Australian companies were more successful in retaining customers following a data breach.[56]

Lost business costs were significantly higher in the US at US$3.97 million compared with Australia at US$0.78 million, which included the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. Post data breach response costs were higher in the US at US$1.72 million compared to Australia at US$0.59 million, which included investigative activities, remediation, legal expenditures, product discounts, identity protection services and regulatory interventions. The detection and escalation costs were lower for the US compared to Australia at US$0.73 million compared to US$0.86 million respectively for forensic and investigative activities, assessment and audit services, crisis team management and communications to executive management and board of directors.[57]

Notification costs in Australia (US$0.06 million) were much lower when compared to the United States (US$0.59 million).[58] This may be due to the mandatory breach notification legislation in the US compared to Australia that did not have this legislation in place when this report was compiled.

Improvements in prevention activities like cyber security governance programs, appointment of a CISO, employee training and security awareness programs, business continuity management, data loss prevention solutions, encryption and deployment of advanced end point security solutions and incident response plans go a long way to reduce the likelyhood of breaches occurring and the subsequent costs. A number of organisations are looking into purchasing cyber security insurance to mitigate cost impacts if a breach occurs. Research from Telstra's cyber security report in 2016[59], found that 11 per cent of Australian organisations indicated that they were interested in purchasing cyber insurance, but were unsure how to go about it.

# New data breach notification legislation

On the 13th February 2017, the Australian senate passed new laws that will require businesses and government agencies governed by the Privacy Act to notify the Privacy Commissioner and affected customers individuals if they have experienced a data breach.[60]

In particular, the notification requirements apply to data breaches where unauthorised access, disclosure and loss of personal information is likely to result in serious harm to the individual.

As these data breach notification laws take effect and are implemented into the business processes and cyber security practices of Australian businesses and government agencies, it will be interesting to monitor their impact on cyber security awareness, accountability, incident response, and the cost and reputational impact of security incidents in future.

56. http://www-03.ibm.com/security/au/data-breach/index.html
57. http://www-03.ibm.com/security/au/data-breach/index.html
58. http://www-03.ibm.com/security/au/data-breach/index.html
59. https://www.telstra.com.au/business-enterprise/campaigns/cyber-security-report
60. Privacy Amendment (Notifiable Data Breaches) Act 2016 (Cth), amending the Privacy Act 1988 (Cth).

# Security drivers and investment decisions

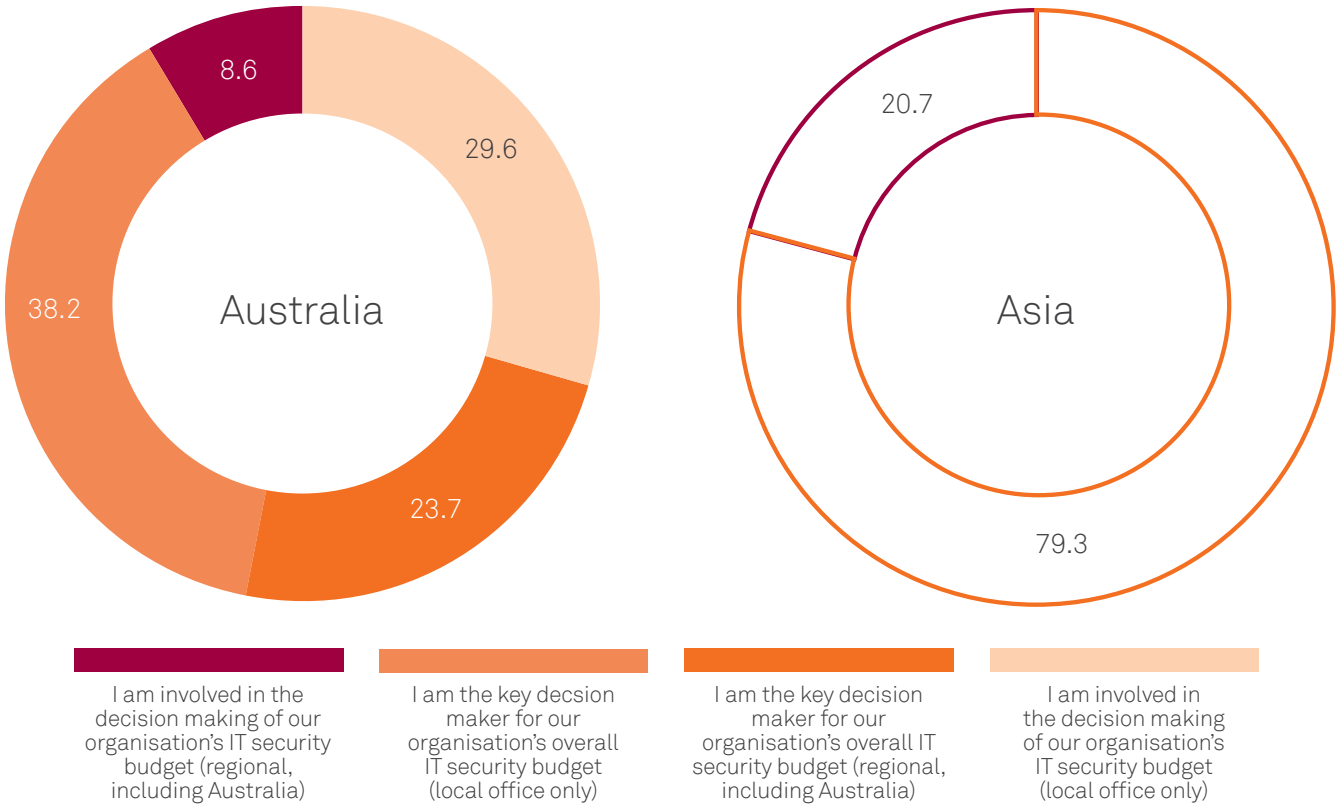
Increases in IT security budgets are driven by the increased stakeholder engagement on security initiatives and security incidents by C-level executives.

### IT Security Investment

To participate in our survey, respondents were required to have either some involvement in or be primarily responsible for IT security budget decisions. 62 per cent of Australian respondents and 79 per cent of Asian respondents indicated that they are the 'key decision maker' for the IT security budget. The majority of surveyed respondents in both Australia and Asia have indicated that they will increase their IT security spending within the next 12 months.

- Our survey results indicate, 48 per cent of Australian and 68 per cent of Asian organisations will increase IT security spending by more than 10 per cent in 2017.
- The majority of Asian respondents in 2016 indicate that they are looking to increase their IT security spending, most commonly by 11 per cent to 15 per cent.
- According to our survey, 24 per cent of organisations in Australia have indicated that they will increase their IT spending by six per cent to 10 per cent.
- The percentage of Australian respondents expecting to decrease their IT security spending has fallen significantly from six per cent in 2015 to one per cent in 2016.
- Only four per cent of organisations in Asia have the same IT security budget as 2015, which is significantly lower compared to the 17 per cent of organisations in Australia with the same budget constraints.
- According to our research, 41 per cent of organisations surveyed in Australia and 36 per cent in Asia set aside four per cent to five per cent of their total IT expenditure for IT security.

## Ownership of security budgets from respondents in Australia and Asia (%)



## Forecast IT security budget for next 12 months (2016 vs 2015) – Asia and Australia (%)

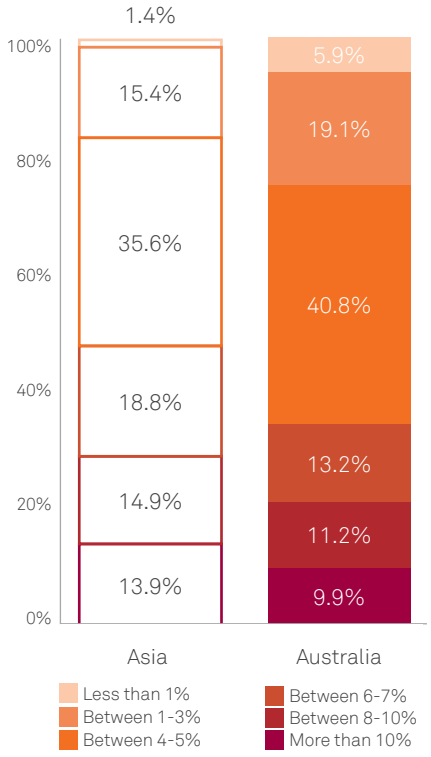

## The increased adoption of incident response drives the growth of the after breach market.

In Australia, the highest usage for emerging security solutions is in 'incident response', and Cloud Access Security Brokers (CASB) are used the most in Asia. 47 per cent of organisations surveyed in Australia and 55 per cent in Asia have adopted 'incident response' toolsets or services. The adoption of incident response services is likely to increase in Australia with the recent announcement of legislation around mandatory data breach notification by the Australian Government. There is an increasing number of incident response tools and incident response services on offer to organisations and government departments that may be due to the high profile announcements of a number of data breaches and the negative impacts to reputation and customer confidence. This may have increased the adoption and investments in incident response tools and services due to the heightened awareness with C-level executives towards managing these security breaches. In terms of technologies under consideration for purchase 'threat intelligence services' take the lead in Australia and 'Next Generation Endpoint security' is popular in Asia.

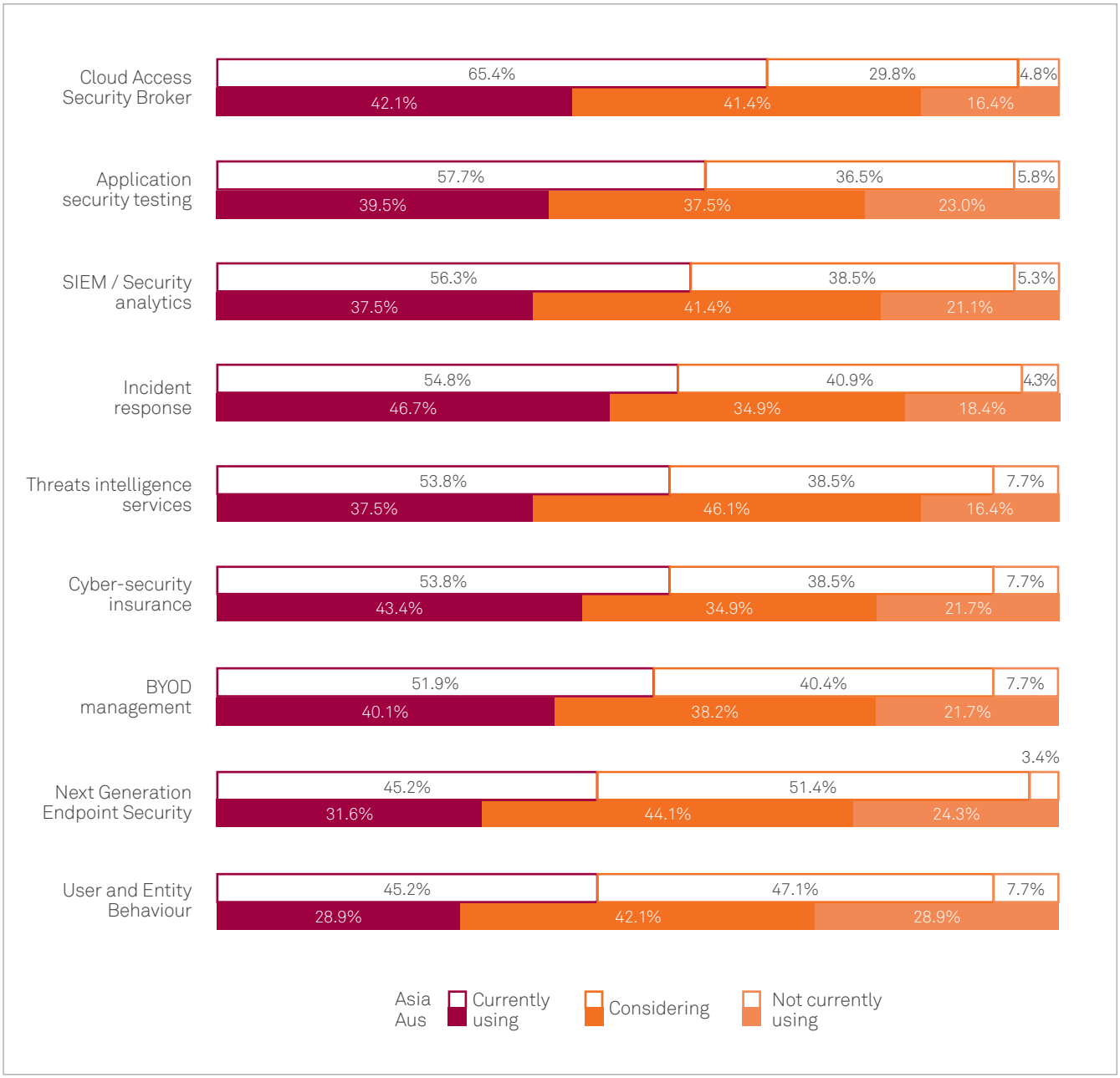
## User and Entity Behaviour Analytics (UEBA) is the tool of choice for mitigating the rising issue of internal threats.

When comparing UEBA to other emerging areas such as CASB, the adoption level is lower, possibly due to the fact that certain service providers offer Security Incident and Event Managers (SIEMs) with built-in UEBA functionalities. However, the fact that 'human error' ranks as the second highest cloud adoption concern amongst Australian enterprises is indicative of the risks due to insider threats. Thus, weak adoption of UEBA is possibly seen as a lack of awareness towards effective tools that can mitigate this risk but may also be due the assumption that UEBA is being delivered as part of their SIEM service. It is also worth noting there is an opportunity to use electronic security device data to enable more inherence-based authentication processes, as well as advancing analytics capabilities in video surveillance, including facial recognition applications.

## IT security budget / Total IT expenditure – Australia and Asia (%)



## Investments in emerging security solutions – Asia and Australia

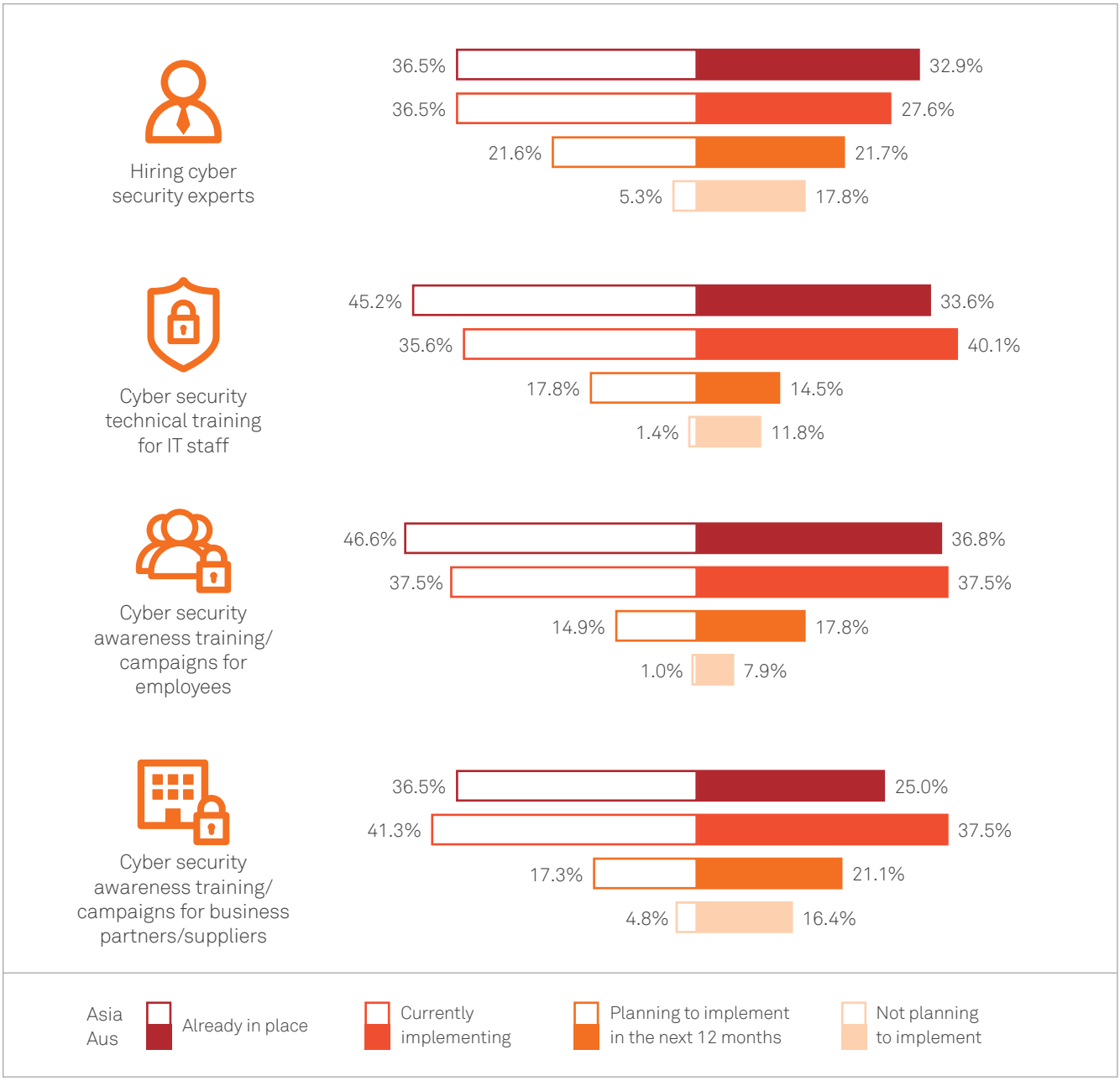



The majority of respondents from Australia and Asia indicate that they already have or are currently implementing cyber security initiatives related to training and resourcing. Cyber security technical training for IT staff and cyber security awareness training for employees were chosen as the top initiatives by respondents from both Australia and Asia. A number of organisations may not have plans to hire cyber security experts as they may be sourcing this function from Managed Security Service Providers (MSSPs). The organisations who are not planning to invest in cyber security training for business partners/suppliers may be utilising other security initiatives to control these risks; such as the use of access controls for systems and data, contractual controls or security audits for business partners/suppliers.

### Cyber security awareness training is moving beyond the enterprise and into the supply chain.

The survey reveals that both Australian and Asian respondents are looking to provide cyber security training and

## Implementation stage of the following resource and training cyber security initiatives – Asia and Australia



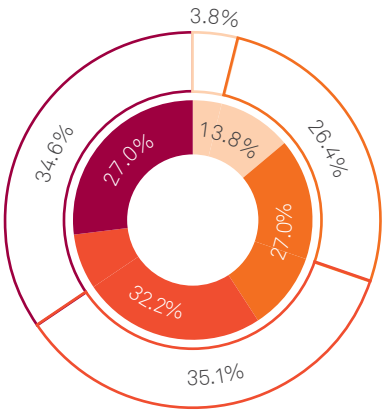

campaigns to their business partners and suppliers. Organisations may want to weigh up the costs and benefits of different approaches to mitigate cyber security risks with their business partners/suppliers and whether other security initiatives may be more suitable or a combination of initiatives like the use of access controls for systems and data, contractual controls, security audits and/or cyber security awareness training.

### Cloud-based and managed security services are expected to grow due to the strong interest indicated in the Asia Pacific study.

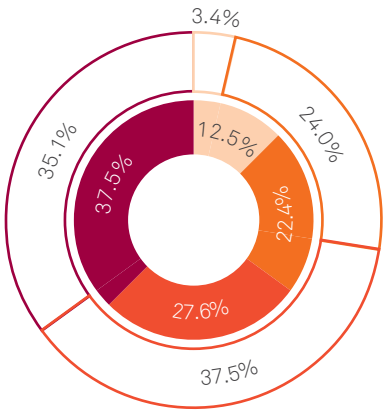
There is a strong uptake of cloud-based and managed security services by organisations in Asia and Australia, which indicates their popularity and an understanding of the value offered by these services. The majority of Australian and Asian respondents indicate that their organisations have either already implemented, or are currently implementing, all of the listed security services. Australian organisations indicated a higher percentage in 'not planning to implement' compared to Asian organisations for all security services surveyed that may be due to tighter budget constraints.

## Implementation stage of the following security service initiatives – Responses from Asia and Australia

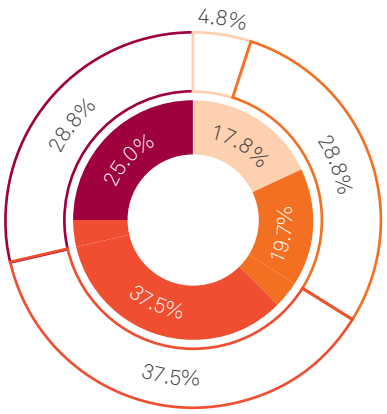
## Implementation stage of the following security solutions – Responses from Asia and Australia



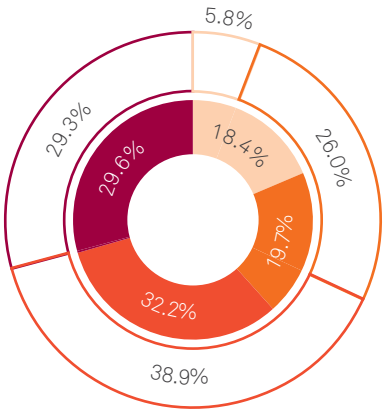

Cyber security technologies



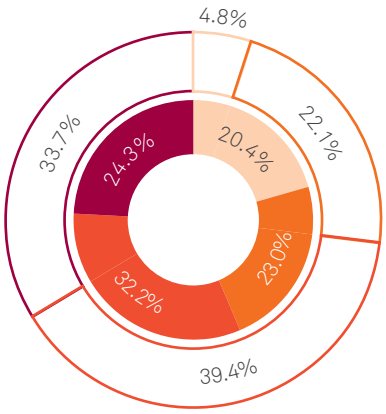

Endpoint security



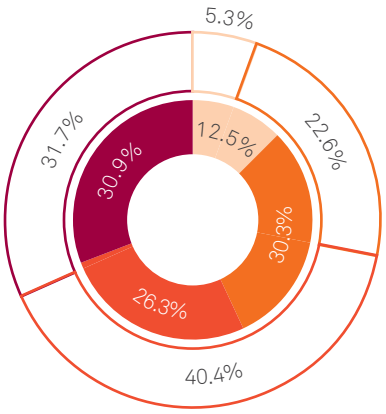

User behaviour analytics




Security forensics/SIEM and analysis tools




Cloud Access Security Broker




BYOD management

Asia
Aus

Already in place

Currently implementing

Planning to implement in the next 12 months

Not planning to implement

# Summary

As the data collected in this year's survey indicates, more organisations are being successfully targeted by cyber security attacks than ever before, but it is not all bad news.

One of the interesting findings in this year's survey was the very large jump in C-level executives taking responsibility for security breaches in Australia. The jump from 19 per cent to 61 per cent is one of the largest year-on-year changes we have seen and is repeated for the rest of Asia, increasing from 35 per cent to 65 per cent.

There is a correlation in Australia regarding this increase and several key changes in the local regulatory and legislative environments. For example, in 2016 the Australian Government released a draft of the serious data breach notification legislation, which has since been ratified by both houses of parliament. Several key industry groups including ASIC and the AICD have been actively discussing this topic and the need for company directors and boards to take more responsibility for cyber security.

Whilst this is good news for organisations and individuals alike, as recently as September 2016 ASIC were publicly stating that boards are underprepared for cyber threats.[62] The message here is that there is still room for improvement in addressing data breaches in organisations but the majority of executives are at last taking responsibility for this problem.

As organisations evolve so do their adversaries. We are seeing cyber-criminal adversaries operating more regular business models. For example, malware/exploit kit developers have black market sales campaigns, licensing and maintenance programs to continue to evolve their products to evade detection by security defenders, to achieve successful infection rates, and increase their illegal profits. They have also evolved to deliver service models like Ransomware-as-a-service and DDoS-for-hire services that can be used by affiliates or distributors to extract extortion payments from their victims. This is yet another reason why organisations must regularly review the efficacy of their cyber security strategies to ensure they still provide the organisation with appropriate cyber resiliency (which is the effective management of cyber risk).

There have been improvements in the resources companies can access to help guide their journey to higher resilience. More organisations are using cyber security frameworks, guidelines and standards such as the ISM, ISO27001 and NIST. These resources are being updated regularly and contain excellent advice that most organisations can apply to real world scenarios, such as which security controls to implement when using public cloud services.

When conducting business in the digitised world, integrating cyber-resilience into all aspects of the organisation and connected third parties is imperative. The data we have collected indicates that more organisations understand this. However, it is still early days for most in terms of transforming their operations and activities to ensure that cyber security is embedded into all their people, processes and technologies to ensure their data and their customers' data, which is the oil of the digital age, is protected. Cyber security is everyone's responsibility and it needs to be built into the DNA of the organisation. How well organisations respond to this challenge may well be an indicator of how successful they will be in the future.

We hope you found this report informative and of value to you and your organisation and look forward to working with many of you to secure your business.

With well over 500 cyber security professionals across the Asia Pacific region, Telstra is well positioned to help organisations improve their cyber resiliency. To find out more about how we can help secure your business, please visit:

www.telstra.com/enterprisesecurity

62. http://www.afr.com/technology/asic-says-boards-underprepared-for-cyber-threat-20160913-grfaoc

# Acknowledgements

## Telstra Contributions

- Global Security Solutions.
- Security Operations.
- Corporate Affairs Communications.
- Telstra Legal Services.
- Enterprise Solutions Marketing.
- Transport and Routing Engineering.

## 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. Our managed Security services continue to evolve in response to the demand for new solution sets to secure against a continually evolving set of cyber security risks.
- 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.

## Consulting Services

Telstra's teams of security consultants 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 manage risk and meet your security requirements. For more information contact your Telstra Account Executive or visit: www.telstra.com/enterprisesecurity for additional information about our security services.

## Telstra Partner Contributions

Akamai, Check Point Software Technologies Ltd., Cisco, CrowdStrike, F5, FireEye, FirstWave Cloud Technology, Fortinet, IBM, Imperva Incapsula, Intel Security, Juniper Networks, paloalto Networks, Qualys Continuous Security, Symantec.

Contact your Telstra Account Executive
Visit telstra.com/enterprisesecurity