Telstra Security Report 2018

Foreword

We are pleased to bring you the Telstra Security Report 2018.

It has been a notable year for security across the globe. With events such as the WannaCry ransomware, NotPetya malware, the Equifax breach, and the leaking of hacking tools by a group called the Shadow Brokers, the past year has seen large scale cyber events dominate the headlines.

In this dynamic and changing environment where connectivity underpins most businesses, this year's report highlighted that organisations are increasingly attuned to the importance of security and the need to protect their organisation.

Our 2018 Security Report is more comprehensive than ever before. This year we interviewed over 1,250 professionals with decision making responsibilities in their organisation for matters of security, three times more than our 2017 report. We expanded our geographic reach to 13 countries, once again including Australia and Asia, but also Europe and the UK. And, this year we also asked respondents specific questions about electronic security, including their challenges and budgets, not just traditional cyber security.

Our research insights and analysis are supported by findings from over 15 other organisations including our range of security partners too.

Some of the insights are surprising. Security professionals are overwhelmingly extending their remit from cyber security to electronic security, with over 99 percent of respondents responsible for cyber security indicating they are also responsible for electronic security. This suggests the market is at an early stage of addressing cyber and electronic together as one logical security domain.

Some of the findings are very encouraging. The industry is shifting its mindset, moving to a 'expectation of breach' mentality, and implementing a wide range of programs too, including security audits, risk assessments and compliance tools through to continuous end-user training. In many countries, there is also a strong focus on governance, risk management and compliance in the face of several new laws regarding privacy and breach reporting.

However, other findings are more concerning. Ransomware is on the rise and is becoming increasingly targeted. Respondents reported more ransomware attacks in this year's survey than any previous years and 31 percent of Australian respondents whose business has been interrupted due to a security breach in the past year are experiencing these attacks on a weekly or monthly basis. Also of note is that a quarter of respondents globally did not have, or did not know if their organisation had, a security incidence response plan in place.

Not all attacks require malware. Criminals are increasingly using social engineering to hijack accounts and trick organisations into wiring large amounts of money into their accounts. These Business Email Compromise (BEC) attacks are among the highest security risks for IT departments in Australia with nearly a quarter of respondents saying their business has been targeted at least once a month. Government figures suggest BEC attacks cost Australian businesses more than $20 million in 2016.

We hope you find the Telstra Security Report 2018 a useful tool to help you make decisions about the security of your organisation.

Neil Campbell
Director, Global Security Solutions
Telstra Corporation Limited

Berin Lautenbach
Chief Information Security Officer Asia Pacific
Telstra Corporation Limited

Table of Contents

Executive summary

Organisations across the globe recognise that getting security right from the outset is a critical success factor for large IT transformation projects, and is essential for the customer experience.[1]

Unfortunately, the risk of cyber-attack is all too real. In 2017 cyber-attacks not only resulted in the loss of intellectual property (IP), but impacted share prices and customer confidence, brought the threat of litigation, and caused businesses public embarrassment. The Equifax breach, for example, had a number of these elements, with the data loss hack impacting 145.5 million customer accounts.[2] It is one of the largest ever breaches reported to date.

In the face of these attacks, many in the security industry are changing their stance from whether an attack will take place; to how often these attacks might be occurring, are they able to detect them when they do, and the subsequent impact on their business.

Cybercrime is a lucrative business. Some industry sources have estimated that cybercrime damages will cost the world a staggering US$6 trillion dollars annually by 2021, up from US$3 trillion on in 2015.[3] There are many adversaries in the cybercrime arena, and a growing number of threat types. These range from distributed denial of service (DDoS), web and application vulnerabilities, to advanced persistent threats (APTs) carried out through zero day exploits which attack previously unknown vulnerabilities. Motives range from wanting to conduct an attack as publicly as possible, to the theft of intellectual property, corporate espionage or surveillance by quietly gaining entry and staying within a system as long as possible.

Threats can come from the inside too. Internal threats can range from the employee who made a simple mistake, for example losing a laptop or USB; to a targeted employee who loses credentials, through social engineering or other means. Most damaging on this spectrum is the 'malicious insider' intent on stealing or damaging corporate data.

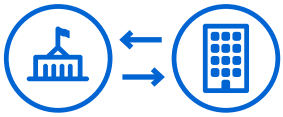
Established security threats, such as ransomware, are some of the fastest growing. In 2017, Carbon Black put the growth rate of underground ransomware economy at 2,500 percent.[4] The Australian government conservatively estimated the cost of ransomware to the Australian economy to be approximately A$1 billion per year.[5] This type of threat is supported by the growth of underground markets operating on the dark webs, and the ubiquity of cryptocurrencies such as bitcoin, allowing buyers and sellers to transact almost anonymously. Many attacks are no longer random, but a very deliberate targeting of businesses which are held hostage by cyber criminals demanding ransom in return for precious company data and files.

There are also new threats on the horizon. Attacks that have been native to IT systems, such as botnets and ransomware, are also a new threat to industrial IoT, wearables and many other connected devices. One of the largest DDoS attacks in 2017, the Mirai botnet, worked by taking control of unsecure IP cameras, home routers and other electronics. It reached capacities of 1Tbps and took down sites around the world. Malware attacks have also targeted industrial control systems and driverless cars. Criminals will also rely on latest technologies, such as cloud, mobility, social media and Artificial Intelligence (AI) as new ways to launch an attack.

[1] Telstra Annual Cyber and Electronic Survey, conducted by GlobalData, 2017.
[2] Fortune. Equifax Underestimated by 2.5 Million the Number of Potential Breach Victims. October 2, 2017
[3] Herjavec Group. 2017 Cybercrime Report. Retrieved from *https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf*
[4] Carbon Black (2017). The ransomware economy. Massachusetts, USA: Author. Retrieved from *https://www.carbonblack.com/resource/the-ransomware-economy*
[5] ABC News. Ransomware cyberattack hits Australia as EU warns victims worldwide may grow. Retrieved from *http://www.abc.net.au/news/2017-05-14/ransomware-cyberattack-threat-lingers-as-people-return-to-work/8525554*

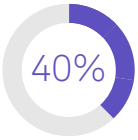
Security Trends

New Synergies



Goverments and Busineses are working together in the area of “intelligence sharing”

Increase of cyber awareness



of global respondents

have implemented cyber-awareness programmes

Regular security reporting

Majority of companies are reporting on cyber and electronic security to management and board at least once per quarter

The good news is that the security industry is well aware of these threats. Business and governments are collaborating in areas such as intelligence sharing and offering many forms of support and information services. Our research shows 40 percent of global respondents, including 36 percent of Australian respondents, have implemented cyber-awareness programmes as part of their cyber preparation strategy. As of February 2018, many businesses in Australia are now required to notify victims and the Privacy Commissioner of data breaches which will drive further awareness and accountability. Similar measures are coming in the European Union and many other countries. Our research shows that the majority of companies are reporting on both cyber and electronic security to their senior management and board members at least once per quarter. Many lines of business play a specific role in the event of a breach and are part of the incident response strategy.

Ultimately, security is critical to the success of any modern organisation and security risk must be managed to acceptable levels. Businesses will continue to use different technologies, such as cloud services and mobility. Employees will continue to access information using their own devices, in remote locations and will need to take precautions. Every organisation must determine for itself what constitutes an acceptable level of risk. As your organisation strives to make vital decisions about security and its operational impact, we hope that this report offers useful guidance on identifying and managing that risk.

Methodology

The Telstra Security Report 2018 provides insights into the current security landscape, to help arm organisations with research based information on managing and mitigating their risk. This year, we have extended the scope of our research to include electronic security. For the purpose of this report, electronic security refers to connected devices such as IP surveillance systems, through to building access and management systems, including industrial control systems. We have also extended the geographical coverage across Asia Pacific and Western Europe.

We engaged research and analyst firm GlobalData 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's infrastructure and security solutions, and over 15 third-party providers including our security partners.

Sample Size

GlobalData's online research in November and December 2017 provided 1,252 responses across 13 countries. Sixty percent of the surveys were conducted in Asia Pacific (APAC) and 40 percent in Europe. Within Asia Pacific, 23 percent of respondents were from Australia; with the remaining 37 percent from New Zealand, Singapore, Hong Kong, Indonesia, Philippines and Taiwan. European respondent were from Germany, France, the UK and the Benelux region.

Business Types

Respondents identified themselves as working in businesses of all sizes - from 50 employees to as large as 5,000 plus across 15 industry verticals. A large proportion of our survey results were based on large organisations; 59 percent of total respondents worked for organisations employing 500 or more employees globally (54 percent in Australia). Respondents were from a variety of business types including local organisations, public sector and government entities and multinational corporation (MNCs). 42 percent of the MNCs were APAC headquartered; 58 percent came from outside APAC.

Position Titles

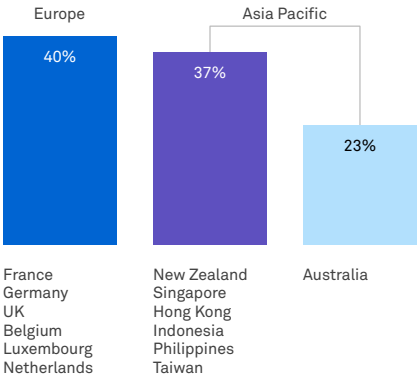
C-level executives including chief executive officers, chief financial officers, chief information officers, chief operating officers, chief technology officers, chief information security officers and chief security officers accounted for 21 percent of the respondents (19 percent in Australia). The remainder were in IT security management roles. All respondents have either some influence or complete control over the security investment within their organisations for their respective regions.

Locations of respondents

1,252
Responses

13
Countries

15
Industries



France
Germany
UK
Belgium
Luxembourg
Netherlands

New Zealand
Singapore
Hong Kong
Indonesia
Philippines
Taiwan

Australia

Convergence of cyber and electronic security

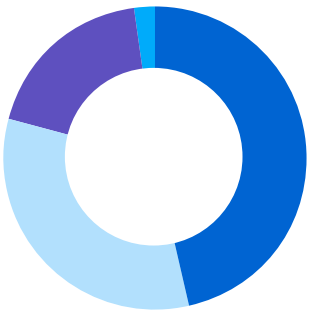
Our research shows that security professionals are extending their remit from cyber security to electronic security too. Over 99 percent of respondents who were responsible for cyber security indicated they are also responsible for electronic security.[6] Conversely, 97 percent of respondents who indicated they were responsible or influenced the electronic security agenda also had some responsibility or decision making on cyber security. In total, approximately 96 percent of respondents qualified to answer both survey sections: cyber and electronic. These figures suggest that the market is at an early stage of addressing cyber and electronic together as one logical security domain. This could either be in recognition of common threats for both areas, the need to improve situational awareness, or both. Interestingly, there is no statistical variation between organisation sizes or by industry vertical.

Respondents in Australia who are slightly 'less involved' with electronic security tended to come from banking, financial services, insurance and government. Budget holders who reported they have final decision on electronic security tended to come from businesses within the 200-499 employee range for APAC and Europe, and the same trend held for cyber security. In Australia, final decision makers for electronic and cyber security are high across the spectrum of company sizes from 50 to the over 1,000 employees range. Another interesting trend is that final decision makers for electronic security had the lowest response rate in businesses with 100-199 employee range (42 percent), where the opposite was true for cyber security. Some 60 percent of the respondents surveyed by this company size range were the final decision makers for cyber security.

Q: To Cyber Security Decision Makers: Do you have responsibility for decisions made for overall electronic security spend in your organisation?

Australia

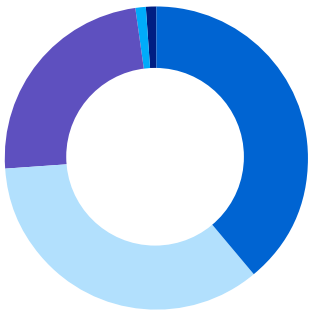
n=279



- **47%** Yes, I make the final decision
- **33%** Yes, I am one of the final decision makers
- **19%** Yes, I contribute to the final decision
- **2%** No, I am a key stakeholder consulted on the eletronic security issues
- **0%** No, I am not involved

Global

n=1,214



- **38%** Yes, I make the final decision in my organisation
- **35%** Yes, I am one of the final decision makers in my organisation
- **24%** Yes, I contribute to the final decision
- **1%** No, I am not involved in the final decision but I am a key stakeholder consulted on the eletronic security issues
- **1%** No, I am not involved

[6] Electronic security refers to security products and services which provide security surveillance, teleme-try, video analytics, biometric and other services. These are often used to protect business sites, staff and assets.
[6] Across APAC, Hong Kong, New Zealand and Singapore reported a 100 percent response rate to this question. In Europe, the UK and Benelux region also reported a 100 percent rate for security professionals driving or influencing the agenda on electronic security. Countries with the lowest re-sponse rates included Taiwan and Philippines in APAC. In Europe, the countries were France and Germany. Nevertheless, the response rates were greater than 90 percent.

Convergence of IT and OT

There are a number of trends which are driving the convergence of IT and OT, and the market for Industrial IoT. From a technology perspective, there is a migration from legacy analogue systems, e.g. Public Switched Telephone Network (PSTN) to Internet Protocol (IP). There is also the convergence of operational technology, such as industrial control systems with IT systems. For example, many newer systems like video surveillance, event monitoring, and alarming are being delivered over the Internet. There will also be numerous connected sensors and devices as a result of the growing number of use cases in smart cities (e.g. metering and telemetry), healthcare (e.g. patient monitoring), transportation (e.g. autonomous vehicles), and fleet and asset management.

Building automation systems (BAS) are also driving the market for smart buildings. These are the centralised systems that typically control heating, ventilation, cooling, lighting, access control and health and safety features within office buildings. For many businesses, smart buildings are a part of the creation of next-gen environments for activity-based working. Other benefits include improving energy efficiency, reducing office sizes and making better use of space through digitally driven designs. Some smart buildings provide personalisation for employees, such as environmental controls. Other GlobalData research in Australia found that facilities managers in particular are working to integrate building access management systems onto the central IT network, which suggests convergence is also being driven from initiatives led by other lines of business.[7]

In the longer term, there will be a number of industries, such as manufacturing, mining, construction and utilities looking to converge and connect operational technology – hardware and software that monitor and control physical equipment and processes – with IT systems. This is to help improve business process automation (e.g. assembly lines, plant monitoring), introduce or expand the use of robotics and drive new efficiencies in the supply chain that connects suppliers and customers. In many cases, this will be used for better visibility across all systems for improved operational efficiencies. With an estimated 18.1 billion connected IoT devices by 2022,[8] this will increase the number of ways a potential attack can breach a system and helps to explain why businesses in this survey are looking at cyber and electronic as one logical domain.

Some of the major threats that can impact cyber and electronic security in this converged landscape include:

Ransomware.

The emergence of IoT has led to a new strain of ransomware that can affect building automation systems or industrial control systems powering vehicles, industrial processes, production lines, and public systems such as water and power. This ransomware can work by locking an underlying boot system, rendering connected devices or sensors inoperable until they are restored either by a back-up system, if available, or a decision by the owner to pay the ransom in hopes of restoring operations. Many new attack surfaces are opening up such as thermostats, public transport systems, connected vehicles, and even hotels where guests were reported to have been locked out of their rooms until a ransom is paid.[9] Beyond the payment of the ransom, businesses can face downtime and related repercussions in operations. They may incur financial losses, environmental, damage to property or assets.[10]

IoT DDoS and botnet attacks.

This type of an attack can happen when an attacker gains access to a manufacturer's IoT device, such as an IP surveillance camera, and from this gains access to thousands of other units with relatively minimal effort. Mirai was one of the largest DDoS attacks through these means and has led to other strains *(See DDoS Section on page 44)*.

Combined attacks.

Other forms of malware attacks are starting to take place at regular intervals, some of which are listing sets of commands to disable machinery, control rooms, or industrial processes. The objective can be sabotage and, in this case, adversaries may be state-assisted. These types of attacks may be in conjunction with DDoS, APTs or other means. Several attacks on the Ukraine power grid are believed to be of this type.[11]

[7] GlobalData Australia Research. The top use cases was security and access control (75 percent); video sur-veillance (74 percent); building management (59 percent) and visitor management (58 percent). This included 147 decision makers from companies with 500 or more employees, across all major industries and Australian states. The survey was conducted in November 2016.

[8] Ericsson. Internet of Things Forecast. Retrieved from https://www.ericsson.com/en/mobility-report/internet-of-things-forecast

[9] Bilefsky, D. (2017, January 30). Hackers Use New Tactic at Austrian Hotel: Locking the Doors. New York Times. Reteieved from *https://www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html*

[10] Boddy, S., & Shattuck, J. (2017, August 9). The Hunt for IoT: The Rise of Thingbots. F5. Retrieved from *https://f5.com/labs/articles/threat-intelligence/ddos/the-hunt-for-iot-the-rise-of-thingbots*

[11] Wired. 'Crash Override': The Malware That Took Down a Power Grid. June, 2017

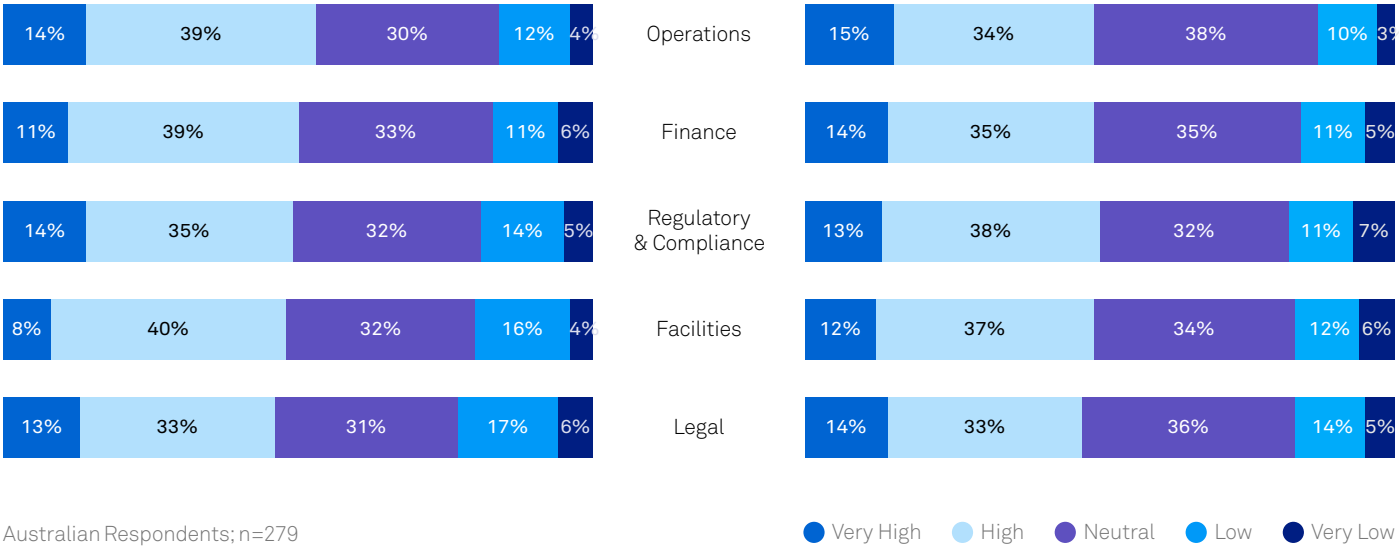
Cyber and Electronic Security Reporting, Accountability and Escalation

Our research shows that the top five lines of business for matters to do with either cyber security and/or electronic security are the same in both domains. While there are differences in the ranking of the line of business, the data shows consistency in the stakeholders for both domains overall. Security professionals are working with the same departments on matters related to security, whether cyber or electronic.

Q: Thinking about your organisation, what is the level of formal involvement with the following departments as it relates to Cyber Security and Electronic Security?

Top 5 Cyber Security Level of Involvement

Top 5 Electronic Security Level of Involvement



Australian Respondents; n=279

The IT department is still seen as the main business group involved in security initiatives for both cyber and electronic. Our research indicates an orchestration role, where IT is still the main group identified as understanding the importance of cyber security to carry out their functions effectively, but also works with multiple business lines. In the event of a security breach, our research also shows a consistency in attribution of responsibility to the C-Level. The major difference between the Australian and global results is the latter places more responsibility on individual employees involved, and in both domains the CEO moves down one place to fourth.

Q: In the event of a Breach, who is ultimately held responsible?

Ultimately held responsible for a breach – Australian Results

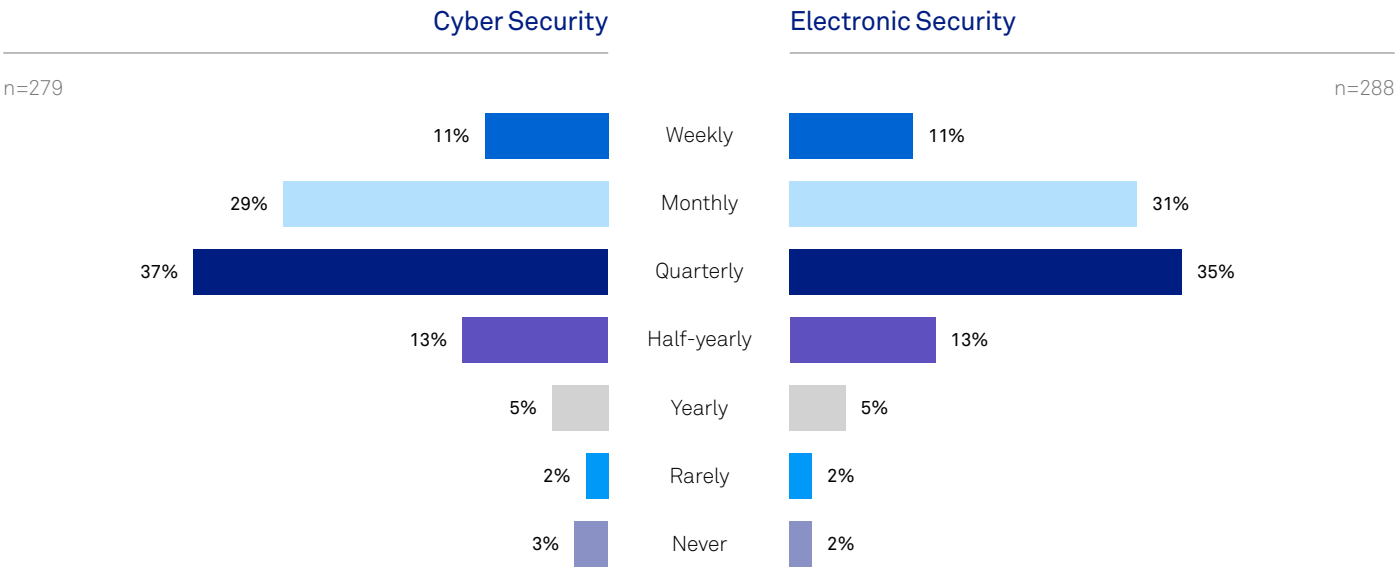
Cyber		Electronic	
IT Department	**40%**	IT Department	**36%**
CIO	**20%**	CIO	**21%**
CEO	**19%**	CEO	**19%**
n=279		n=288	

Ultimately held responsible for a breach - Global Results

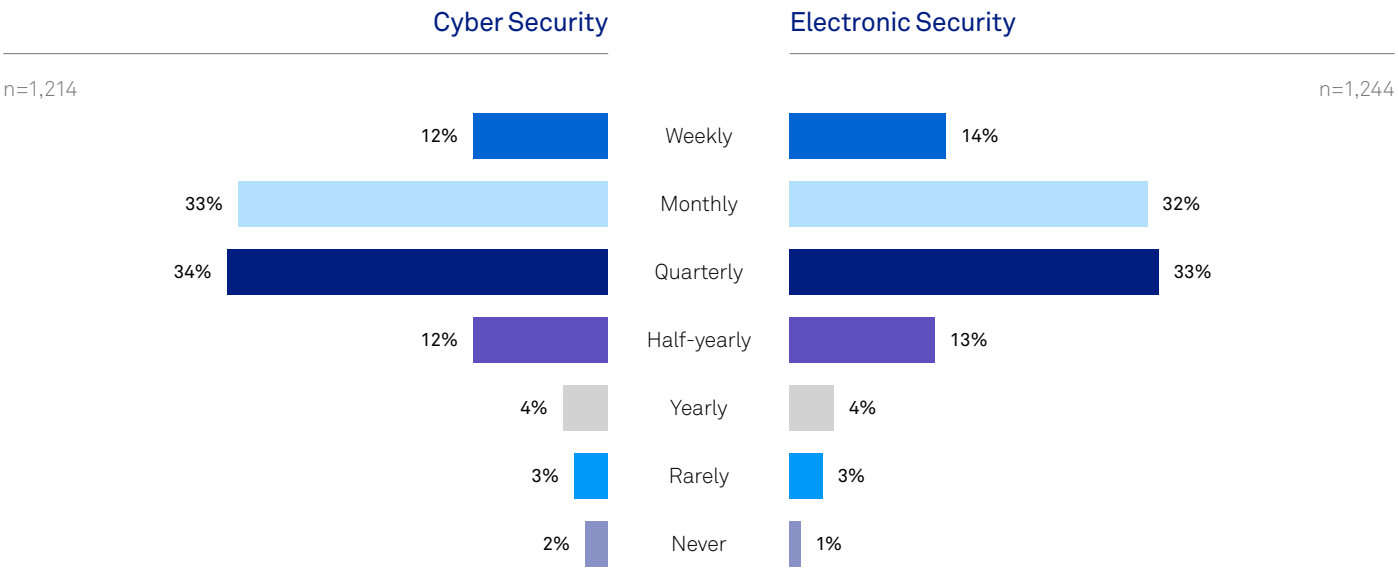
Cyber		Electronic	
IT Department	**44%**	IT Department	**40%**
CIO	**23%**	CIO	**21%**
Employees involved	**20%**	Employees involved	**19%**
n=1,214		n=1,244	

C-Level executives continue to take a more active role in cyber security by understanding the importance of cyber security initiatives, increasing their involvement in these initiatives and taking responsibility for security incidents when they occur. Our research also shows that the level of reporting seems to be increasing for both domains. As convergence continues between cyber and electronic security, reporting is likely to be more integrated.

Frequency of Security Reporting – Australian Results



Frequency of Security Reporting – Global Results



Outlook

Security Budgets will increase in absolute terms and in relative terms.

The cyber and electronic security domains are vastly different, as historically, electronic and IT systems have run on separate systems and share little resemblance to one another. Our research, and other industry data shows the two domains will start to converge. Some 83 percent of Australian respondents report that budgets for cyber and electronic security are increasing in 2018, similar to the 84 percent of the APAC and European respondents. Security, when measured as a line item relative to the overall ICT budget, will also increase for 58 percent of Australian business and 64 percent of APAC and European businesses surveyed. Security budgets will increase in absolute and in relative terms.

Our research suggests that budgets for cyber and electronic security are converging. Around 67 percent of Australian businesses have, or plan to have, a combined budget for cyber and electronic security. This is consistent with the European results (68 percent) but lower than APAC results of 77 percent. Both security domains will also be increasingly a shared responsibility across multiple lines of business, and the frequency of security reporting will also likely increase.

The convergence of electronic security and cyber will take time. Our research shows that 84 percent of Australian businesses are considering, trialling or have already implemented systems to manage the convergence of cyber security and electronic security, for example, tools to unify monitoring of premises and network activity. This is similar for European respondents. Asia Pacific respondents reported a higher rate of 90 percent. In terms of more immediate priorities, Australian businesses will look to electronic security solutions such as operational technology (65 percent), CCTV and external video sources (61 percent), biometric and physical access systems (58 percent), and BAS, uninterruptable power supply (UPS) and alarming systems (56 percent). These priorities are ranked in the same order by global respondents, but percentages are higher overall. Some 73 percent of global respondents will look into operational technology, and 63 percent into BAS.

Recommendations

Consider multi-factor authentication

An employee's access badge, video surveillance and facial recognition technologies, for example, can be integrated with login credentials to validate the physical location of an employee. This multi-factor authentication is of particular importance in sectors such as banking, financial services and government, where some employees may have access to highly sensitive and confidential data.

Protect data in motion

The use of additional encryption technologies can deliver secure tunnelling and transport of data. This encryption is important for thwarting any attempts in TLS/SSL attacks. This is usually used as an additional capability for industrial control systems, but can also protect video surveillance, BAS and other systems from potential attacks.

Integrate situational awareness

Combing disparate sets of data can also improve overall visibility, and command over cyber and electronic security. Combining and integrating data sources can often paint a more complete picture around a security event or data breach. Using multiple disparate data sources can help to find the "unknown unknowns", expose vulnerabilities, predict potential attacks or support post event mitigation.

Cyber preparation and incidence response

Security awareness continues to increase and our research indicates this is driving the adoption of certain frameworks, such as security audits, risk assessments and compliance tools through to continuous end-user training. In the last several years, security has shifted from being considered a value-added capability or premium service, to a critical element that needs to be integrated and hardwired into an underlying architecture. In 2018, security will continue be a topic addressed from the outset of an ICT project to help ensure success. Businesses that address security at a later phase will have a much higher chance of project postponement or even failure. Our research found that Australian, APAC and European companies tend to focus more on conducting security audits as their top priority, which is consistent with the results from our 2017 report. The 2018 data indicates a trend whereby businesses are undertaking a number of security initiatives. There is no area being excluded per se this year, there are only varying degrees of priority.

Cyber Preparation

We asked respondents in Australia, the APAC region as a whole and Europe if their organisations have been or are implementing cyber preparedness. The results are as follows:

Q: Cyber Preparedness: which of the following programmes are you undertaking at the present time? (Multiple Responses Allowed)

Australia	
High Priorities	
Security Audits	**38%**
Risk Assessments of internal systems	**36%**
Governance, Risk and Compliance Tests	**36%**
Cyber Security Awareness Programmes	**36%**
Procedures to protect IP	**35%**
Other Priorities	
Incident management and response process	**28%**
Risk assessment of third parties	**27%**
Programme to identify sensitive assets	**26%**
Data Classification	**25%**
Security Drill	**23%**

n=279; n=864

APAC Region	
High Priorities	
Security Audits	**44%**
Cyber security awareness programmes	**43%**
Risk Assessments of internal systems	**40%**
Governance, risk and compliance tools	**40%**
Procedures to protecting IP	**40%**
Other Priorities	
Risk assessment of third parties; Incident management and response process	**33%**
Program to identify sensitive assets	**32%**
Security drill	**29%**
Data Classification	**28%**

n=739; n=2,685

Europe	
High Priorities	
Security Audits	**39%**
Risk Assessments of internal systems	**36%**
Cyber security awareness programmes	**34%**
Other Priorities	
Procedures to protecting IP	**31%**
Data Classification	**28%**
Incident management and response process; Risk assessment of third parties	**27%**
Program to identify sensitive assets; Governance, risk and compliance tools	**27%**
Security Drill	**25%**

n=475; n=1,427

Australia and APAC

After security audits, Australia and Asia Pacific respondents tend to focus on risk assessments and improving security awareness, perhaps in recognition of the growing interest in security overall. There is also a strong focus on governance, risk management and compliance (GRC) likely due to new laws in Australia regarding data breach disclosure. Singapore tends to have a strong focus on critical national infrastructure, and in February its Parliament passed a Cybersecurity Bill that proposes personal accountability in the event of data breaches, while many ASEAN countries have rules regarding data sovereignty. Protection of intellectual property (IP) is also high on this list of programmes and this is likely due to a relatively high level of awareness of cybercrime.

European results

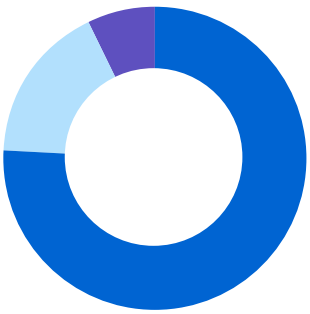
After security audits, risk assessments and cyber awareness are the two programmes that featured as a priority one initiative with a response rate of 35 percent or higher. However, similar to the Australian and APAC results, there are a large number of programmes being undertaken. Interestingly, governance, risk and compliance tools are programmes only being undertaken by 27 percent of European respondents. This is despite with General Data Protection Regulation (GDPR) set to come into force in May 2018. This regulation, which we discuss later in this report, applies to the management and protection of personal data.

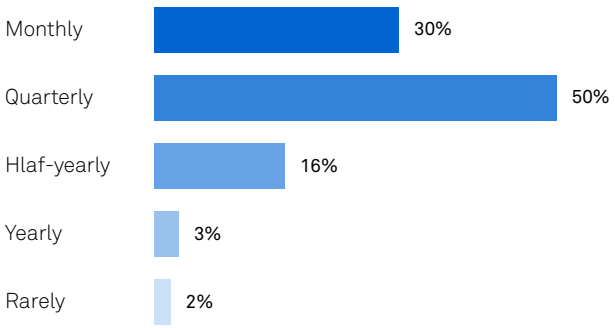
Incidence Response Plans

Our research highlights that approximately three of four respondents have an incidence response (IR) plan which is a strong starting point. Within this group that have IR, over 70 percent of organisations are testing them at least once a quarter. Unfortunately, there is still a sizeable proportion (25 percent globally) who either did not know if their organisation had such a plan, or could confirm no plan exists, which is indicative of cyber maturity.

Q: Does your organisation have an incident response plan in place? If yes, how frequent is the testing and reviews of your incident response plan?

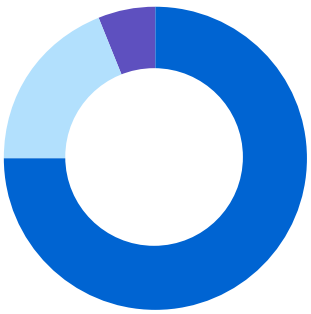
Australia

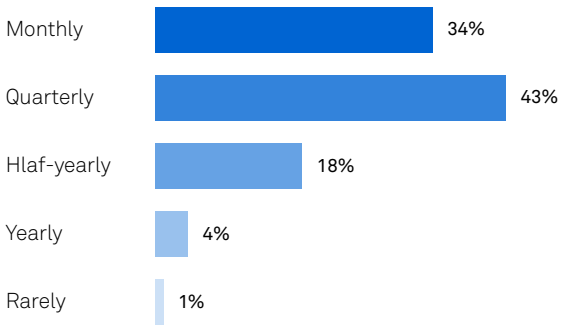




n=279; Yes n=212

Global

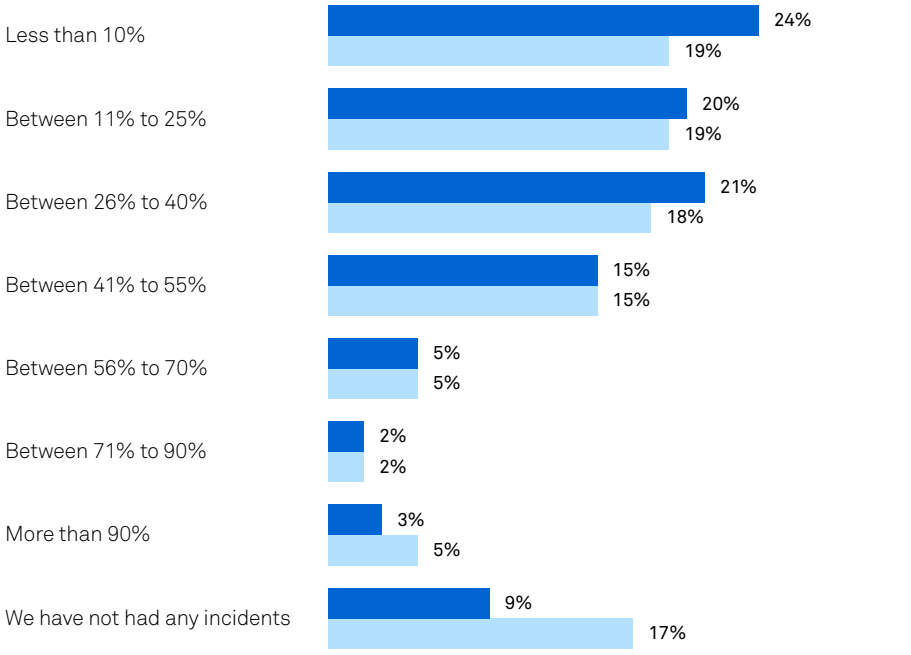




n=1,214; Yes n=911

While this trend is encouraging, our data shows incident response has room for improvement. Businesses by and large take cyber security very seriously; moving from a defensive posture to a presumption of breach, and have a plan in place which is tested regularly. However many attacks and data breaches are not detected, falling below the radar. Another challenge is that businesses can find themselves besieged by alerts and false positives which can drain analyst resources. Sometimes one attack (e.g. DDoS) can mask another (e.g. malware) and distract analysts from the attacker's real target. Polymorphic malware, once in a system, will replicate itself in slightly different forms making it more difficult to track. The graph below shows an estimate of incidents that respondent organisations responded to in the past year. The data highlights the sentiment of IT security professionals regarding the challenges of incident response, especially with regard to end to end visibility. This also reflects the volume of alerts and threat intelligence being continuously experienced.

Q: In your best estimates, what is the percentage of incidents that your organisation responded to in the past year?



Global n=1,214; Australia n=279

While Australian respondents are reporting a higher rate of no incidence, only three to five percent of respondents believe their organisation is able to respond to over 90 percent of incidents. Unfortunately, it is often the case that breaches take place within minutes or days and can go unnoticed for months or years.

How Often Do Breaches Occur?

Our research highlighted the following:

Unknown, unknowns.

AU	EU	APAC
67%	75%	75%

Estimated up to 55% of breaches go undetected

Sixty seven per cent of Australian businesses (and 75% of the APAC and European respondents) estimated that the number of breaches that had gone undetected in the past year was up to 55%. Within this figure, 28% of Australia respondents estimated this to be less than 10% which is consistent with the European results of 29%. In APAC, 35% of respondents estimated the number of successful undetected breaches to be less than 10%.

Known, unknowns.

AU	EU	APAC
9%	7%	6%

Did not know the number of undetected breaches

The study also shows that 9% of Australian business, 6% of APAC and 7% of European organisations indicated they did not know the number of successful, undetected data breaches.

Known, knowns.

AU	EU	APAC
75%	83%	81%

Estimated up to 55% of incident alerts had gone unanswered

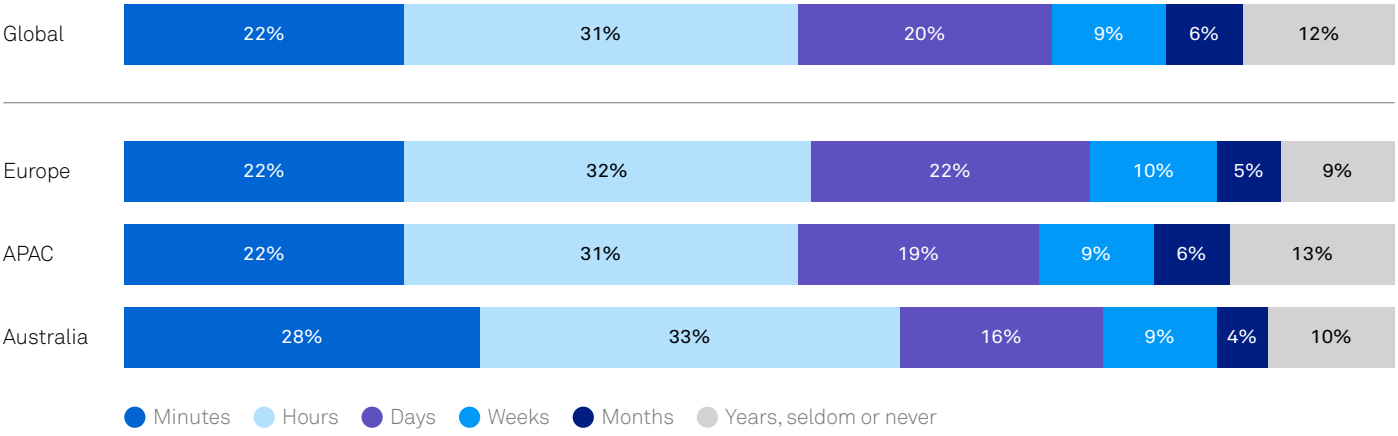
Approximately 75% of Australian businesses (and 81% of the APAC and 83% of European respondents) estimated that up to 55% of incident alerts in the past year had gone unanswered. Within this figure 27% of Australian businesses, 33% of APAC and 31% of European respondents estimated that less than 10% of incident alerts had gone unanswered in the past year. Despite improvements some businesses have made in automation, this data suggest a lot of alerts are still going unanswered.

Incident Response and Dwell Times

Encouragingly, 61 percent of data breaches were discovered in minutes or hours by Australian respondents. This compares to 53 percent in APAC and 54 percent in Europe. However some 29 percent of the security breaches in Australia were detected in days, weeks, or months, compared to 34 percent in APAC and 37 percent in Europe. Ten percent of the security breaches in Australia were not detected for years, seldom or never. which was consistent with the European results. The results in APAC were slightly higher at 13 percent and slightly lower in Europe at nine percent. The two outliers for this question were Hong Kong and Taiwan, with respondents indicating that 29 percent and 25 percent of breaches respectively fall into this latter category.

These statistics highlight that many organisations are still under invested in cyber security or at least have considerable room for improvement. A study conducted by FireEye in 2017 shows that the global median dwell time – the time between an initial security breach to the discovery – remains high at 99 days and significantly higher in APAC at 172 days.[12] CrowdStrike has seen dwell times of between 800 and 1,000 days in outlier cases.[13] These results highlight that even though more organisations have established better testing methodologies, the changing nature of attacks can have a significant effect on organisations ability to detect the attacks.

Average time to detect a security breach



Global n=1,214; Europe n=475; APAC n=739 (includes Australia); Australia n=279

In terms of recovery time from cyber-attacks, there has been an improvement in Australia across various forms of attacks. Our research found that on average, 74 percent of the cases in 2017 were recovered in less than two hours versus 56 percent in 2016. Australia is, at present, slightly ahead of APAC and Europe in achieving faster recovery from attacks. On average, 67 percent and 66 percent of the attacks in 2017 were recovered in less than two hours in APAC and Europe respectively.

The improvement in response time in Australia is in line with the greater number of organisations putting in place an incident response plan (76 percent vs. 66 percent in 2016) as well as the frequency of which organisations are testing and reviewing their incident response plan. In comparison, organisations in Europe had a slightly lower take up rate for incident response plan (68 percent). In general, there is a correlation between dwell times and cost per breach. A recent report from CrowdStrike highlights that the longer an attacker can dwell in the environment, the more opportunity they have to find, exfiltrate or destroy valuable data or disrupt business operations.[14] This would also likely increase the cost of a breach. An effective incidence response solution can help to reduce dwell times. Putting this into perspective, the Australian Cyber Security Centre (ACSC) report notes that "defending a network from compromise is far less costly than dealing with the costs of compromise".[15]

[12] FireEye. (2017). M-Trends 2017: Trends behind Today's Breaches & Cyber Attacks (FireEye report). Milpitas, California: Author.
[13] CrowdStrike. Cyber Intrusion Casebook, 2017. (CrowdStrike also reports the average dwell time to be 86 days globally).
[14] CrowdStrike. Cyber Intrusion Casebook, 2017.
[15] Australian Cyber Security Centre. (2017). ACSC 2017 threat report (ACSC report). Canberra: Author.

Outlook

"If you are not finding data breaches, you are not looking hard enough." – CISO, US healthcare provider

The security industry will continue to move towards a presumption of breach approach, and the focus for many will be on the ability to reduce dwell times. This is in recognition of industry trends as well as the stealth of APTs in their ability to infiltrate a system. The goal of some attacks is to go undetected for as long as possible. In some cases, organisations will never truly know the answer to questions such as whether an attack has happened, how long it has happened for and how much it is costing the business. The number and size of attacks and cost per attack will likely increase into 2018.The costs associated with a breach will range from damage to physical infrastructure, loss of intellectual property and downtime.

Given the number of threats and the motivations behind each, security will have multiple layers of control. In the event one control fails or another vulnerability is exploited, systems will continue to be designed to protect data and maximise service uptime and availability. Not all security issues will be addressed at once. Our research suggests businesses will have high priority requirements, such as security audits, education and training; and other priority needs, such as cyber drills. Nevertheless, businesses will continue to put plans in place for cyber preparation, response and mitigation and will need a view on what to do before, during and after an attack.

Recommendations

IR can reduce dwell times

Our research indicates that businesses who have an incidence response plan that are actively tested are best placed to reduce the time between when a breach happens and its subsequent remediation. This IR plan is important for identifying, isolating and containing damage an attack can cause. The sooner this process can happen, the better.

Consider cyber AI

Businesses should continue to invest in real-time analytics capabilities and artificial intelligence (AI) to help identify the so-called "unknown unknowns", to better improve cyber defence posture. Some threats are increasingly difficult to detect through conventional means. Continual advancements in machine learning, including the integration of multiple threat feeds, combined with cloud scale computing will continue to make big improvements in automation and overall incidence response.

Rehearse the IR plan

A cyber response should not only be defined, but also rehearsed. The plan should consider multiple threat vectors, underlying motives (e.g., insider threat, politically or financially motivated cyber criminals) and consider the corresponding actions in advance. Our research shows that not all incidents are being responded to and this is an area that needs to improve. Cyber security response plans should be revisited, rehearsed and updated regularly.

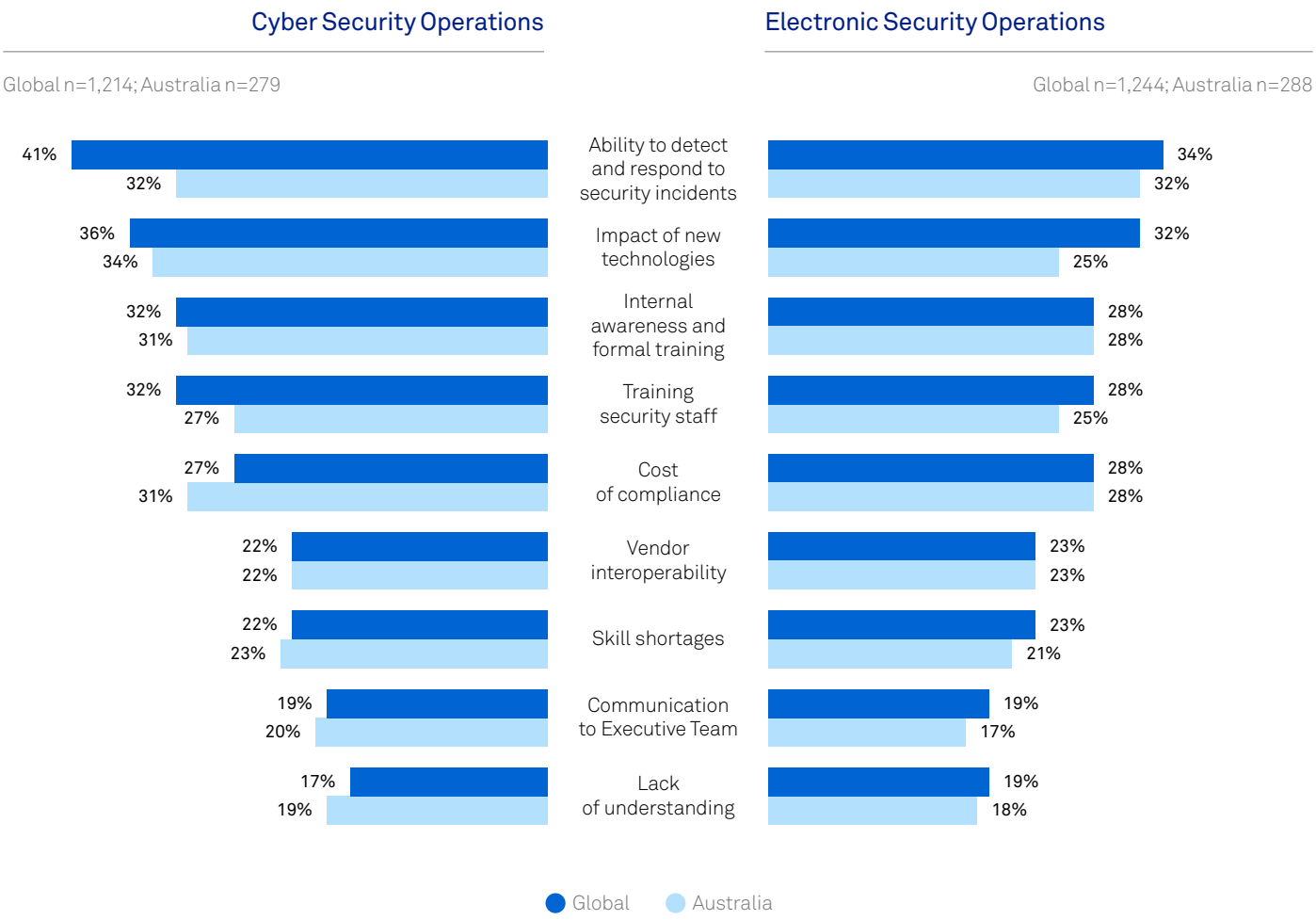
Security challenges and business impact

Challenges of Security Operations

Security threats are now getting the attention of board members and senior management across different industries due to their overall importance. Business and IT leaders are concerned about security because of the difficulties in managing the IT environment and protecting it against threats.

Our research shows that the top two challenges globally with regard to security operations are the ability to timely detect and effectively respond to security incidents; and the impact of new technologies such as cloud, mobile and software-defined networking (SDN). In Australia, the cost of compliance and internal awareness are also highlighted as major challenges by 31 percent of the responses. The challenges identified are similar when respondents are asked about their electronic security operations.

Challenges with regard to:



With more security threats and breaches being reported, the perception is that cyber security is becoming more difficult to manage due to the frequency as well as sophistication of attacks. This perception also leads to questions about whether companies have the right measures and solutions in place to detect and respond to cyber threats. For example, a study conducted by Carbon Black highlights the emergence of creative, non-malware attacks such as impersonating the Chief Information Security Officer (CISO) while attempting to access corporate IP; spoofing login systems to appear authentic; masquerading as 'Human Resources' and asking employees for personal details; and utilising task automation and configuration management frameworks, such as PowerShell. In dealing with these new forms of attacks as well as commodity malware, the study also suggests that there is a lack of visibility with legacy anti-virus (AV) solutions.[16]

This complex and rapidly changing threat landscape makes it harder for security staff to keep up with emerging threats as well as new cyber security solutions or methodologies. Thirty two percent of our respondents indicated training of security staff was a major challenge as they needed to be constantly kept up to date.

Making the situation more difficult is the need for businesses to adopt new technologies to achieve operational efficiency and enable new business models. For example, IT departments are looking to cloud technologies to reduce the cost of IT infrastructure and improve agility in meeting business needs. Organisations are also adopting a mobile first approach to engage their customers through ubiquitous smartphones as well as to enable employees to become more mobile for productivity gains.

The use of these technologies means that traditional security solutions are no longer adequate. IT departments must now protect corporate data that resides outside the company premises and secure a wider range of endpoints. The use of mobile devices for work is prevalent and there is also widespread use of social media in the workplace; as well as online collaboration tools for sharing files with co-workers and external stakeholders. While employees are using more consumer technologies at work, they may not be aware of the potential consequences. A study by Citrix/Ponemon Institute shows that the greatest risks identified by IT/IT security practitioners are associated with the use of social media in the workplace.[17] Another study conducted by Checkpoint highlights the expansion of mobile malware. In particular, Checkpoint highlighted the growing number of mobile adware botnets such as HummingWhale and HummingBad affecting millions of devices. Both strains were prominent in third-party app marketplaces in 2016. In 2017 Checkpoint also unravelled Judy, an auto-clicking adware that might be the largest mobile malware infection to date.[18] Hence, there is a need to ensure employees are aware of security risks and provide them with training so that they do not become easy targets for cyber criminals.

[16] Carbon Black. (2017). Beyond the Hype: *Security experts weigh in on artificial intelligence, machine learning and non – malware attacks.* (Carbon Black Report). Massachusetts, USA: Author.
[17] Ponemon Institute LLC. (2017). The Need for a New IT Security Architecture: Global Study on the Risk of Out-dated Technologies. (Ponemon Institute report). USA: Author.
[18] Checkpoint. (2017). *Mid-year report: Cyber attack trends.* USA: Author. Retrieved from https://research.checkpoint.com/cyber-attack-trends-mid-year-report/

Security Incidents

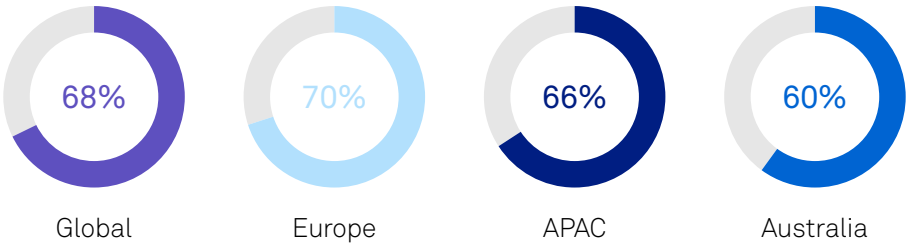
There were several high profile security breaches reported in 2017, but many more incidents around the world went unreported. Our research shows that there is a high chance of an organisation being impacted by a security breach. In Australia, 60 percent of respondents experienced business interruption due to a security breach at least once over the past year. This was slightly higher in Asia Pacific and Europe at 66 percent and 70 percent respectively.

The two most common types of security incidents in Australia are Business Email Compromise (BEC) and phishing attacks. In Asia, the two most common are virus/malware outbreak and employee error; and in Europe they are phishing attacks and employee errors. These types of security threats highlight that cyber criminals are targeting employees who can be seen as the weakest link. Phishing and deceptive email remains prevalent. In a study conducted by COFENSE Inc. (formerly PhishMe), 89 percent of Australian IT professionals surveyed have dealt with security threats originating from deceptive emails.[19] FirstWave Cloud Technology, which scanned over 1.3 billion emails in Australia in 2017, highlighted an increase of 1,178 percent in the volume of email with phishing risks; and an increase of 243 percent in the volume of email with C-Level impersonation (BEC) risks.[20]

While there are security solutions that can filter or block malicious emails, they are not infallible, and these figures again point to the need for employee awareness of security risks and training on how to detect and respond to deceptive email.

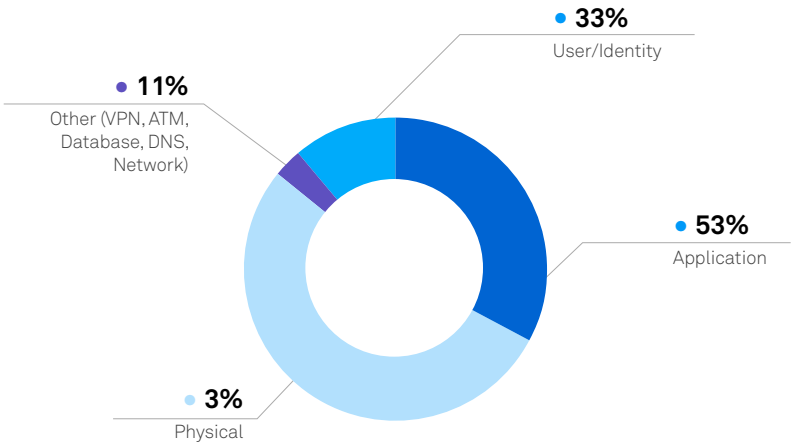
A study by F5 analysing 338 breach records also shows that applications were the initial targets in 53 percent of breaches; and together with identity make up 86 percent of the breaches.[21]

Business interrupted due to a security breach in the past year



Australia n=279; APAC n=739 (including Australia); Europe n=475; Global n=1,214

Cases by initial attack target



"Of the cases for which we were able to determine the initial attack target, applications were the first target in 53% of the cases. Identities were the first target in 33% of the cases. Collectively, attackers started their attack either directly at the web application, or attacked a user for their identity in 86% of the cases."

Source: F5

[19] Anti-Phishing Working Group. (2017). *Australia phishing response trends: Losing the war.* Retrieved from https://phishme.com/phishing-response-trends-australia/
[20] FirstWave Cloud Technology. (2017). *Cloud Technology's Threat Insights Report: 2017 Review.* Retrieved from https://www.firstwavecloud.com/news/category/company-announcements
[21] Boddy, S., & Pompon, R. (2017, November). *F5 Threat Intelligence Report: Lessons Learned from a Decade of Data Breaches.* Retrieved from https://f5.com/Portals/1/PDF/labs/F5_Labs_Lessons_Learned_from_a_Decade_of_Data_Breaches_rev.pdf?ver=2017-12-11-093704-320

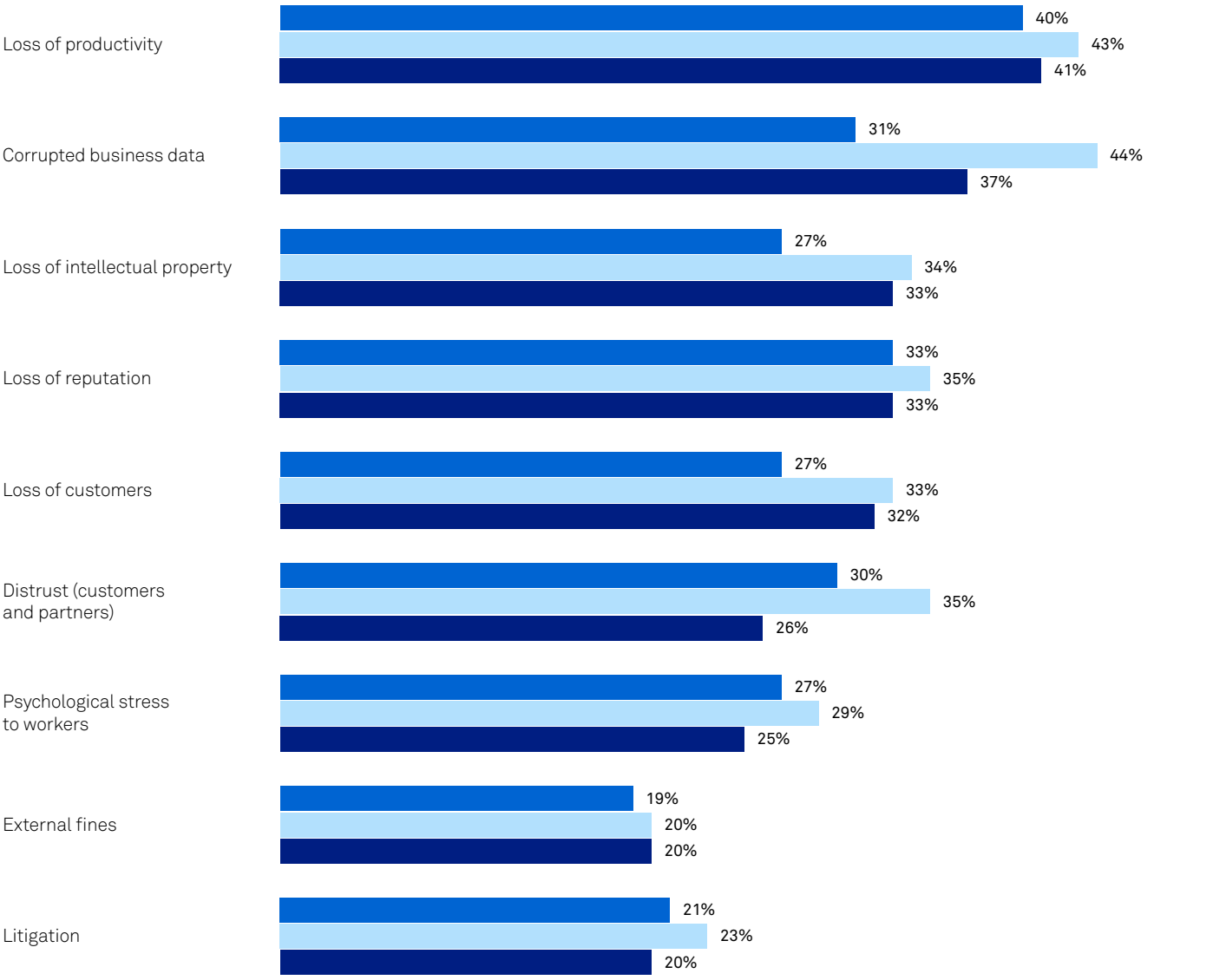
Business Impact

Our research shows that loss of productivity was rated as having the most detrimental impact to businesses in Australia, Europe and in Singapore, and the second most serious impact in APAC. Lost productivity can be expensive.

Organisations have to bear costs such as wages, rents, utilities, etc. while operations have been disrupted, and also face the potential loss of revenue, for example when buyers are not able to complete purchases online. In

Australia, lost productivity was rated fourth in our 2016 survey, which shows an increasing concern regarding this possible impact as cyberattacks become more prevalent.

Impact of a major security breach



Europe n=475; APAC n=739; Australia n=279

Europe APAC Australia

Loss of reputation was also ranked as one of the top three business impacts in Australia, APAC and Europe, and fourth in Australia. The financial impact of loss of reputation or negative impact to a brand can be significant, and it takes time and a huge amount of resources to rebuild this reputation. Corrupted data was the top impact for organisations surveyed in APAC and third in Europe. Organisations are becoming more data-driven, and they see data as a critical asset to drive differentiation. At the same time, detecting the corruption or alteration of data during a security breach can be harder to detect. This will become a greater concern going forward as companies increasingly rely on big data and analytics for business insights. In Australia, the third major business impact was loss of intellectual property, which was ranked the highest in our 2016 survey. The loss of IP continues to be a major impact and understandably so since it can result in the loss of competitive advantage to rivals. Companies that rely on innovation to stay ahead have the most to worry about, particularly since it is often costly to fund research and development (R&D) and build IP.

There is also evidence of rising costs due to cyber security breaches. For example, the ACSC Threat Report 2017 indicates that the number of BEC reports to the Australian Cybercrime Online Reporting Network (ACORN) had shown a significant increase. The financial losses in FY2016/17 amounted to A$20 million, an increase of over 230 percent from A$8.6 million in FY2015/16. Since only a small percentage of BEC incidents were reported, the total losses would be significantly larger. Symantec highlighted a steady increase in mega breaches – breaches in which more than 10 million identities were stolen – from 11 mega breaches in 2014, to 13 in 2015, and 15 in 2016.[22]

[22] Symantec. (2017). *Internet Security Threat Report:* Volume 22. California, USA: Author. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

Outlook

Businesses measure the impact of a security breach in their own ways, which are significant in their own right. 2018 brings more transparency to security breaches through public disclosure as part of a wave of compliance measures being introduced globally. This will add considerable pressure on businesses. Public disclosure of breaches can impact customer confidence, in an era when businesses are trying to differentiate on the basis of customer experience; and public embarrassment in having to testify before lawmakers. With the convergence of cyber and electronic security, the impact of a breach will extend to physical damage to property, infrastructure or assets.

Recommendations

Proportionality

While breaches can adversely impact the bottom line, businesses, in turn, should assess their digital assets to determine their worth. From here, businesses should look to provide a level of security commensurate with the true value of these digital assets. Data classification helps to identify the most critical digital assets.[23] Unfortunately, many businesses have not conducted such an assessment and have found this process to be challenging.[24]

Establish data ownership

Many organisations are far down the path of digital transformation and have several initiatives around the use of big data. However, the vast majority of businesses do not have a centralised strategy around their data. In practice, data collection and analysis is project specific and over–seen at a department level. To better protect digital assets, it is imperative for organisations to assign ownership and responsibility of data. Marketing is often leading the charge for big da-ta and can often be a strong partner with IT.

[23] Ponemon Institute estimates the average global cost of data breach per lost or stolen record was US$ 141 per record in 2017. In Australia, the cost per compromised record is AUD$ 139. This number increases some industries such as financial services and health care.
[24] GlobalData End User Research

Compliance

The Year of New Compliance

2018 will see more focus on compliance than ever before, with many laws coming into effect across the world that will have far reaching implications beyond national borders; implications that are not yet fully understood. Our research shows that some 87 percent of Australian businesses say they are actively adhering to the Australian Privacy Act. This is important to note because, from February onwards, there are new notification procedures in the event of a data breach. This notification to the affected individuals must include details of the data breach and recommendations on the steps they should take in response to the breach. Disclosure has to be prompt and the Australian Information Commissioner must also be notified.[25]

From May onwards, the GDPR will also come into play, requiring organisations around the world that hold data belonging to EU citizens to provide a high level of protection and explicitly know where data is stored. In the case of the GDPR, organisations that fail to comply with the regulation requirements could be penalised up to €20 million in fines, or up to four percent of their total worldwide annual turnover of the preceding financial year, whichever is higher. Our research shows that nearly 87 percent of APAC businesses; and 84 percent of European businesses are following national legislation on cyber security, such as GDPR.

Beyond compliance, businesses are also relying on various security standards or frameworks as guiding principles for corporate security policy. Australian respondents tend to work with government and industry bodies such as the Australian Prudential Regulation Authority (APRA) and Australian Signals Directorate (ASD), but are also considering many other international guidelines from CERT, ISO and COBIT. This approach in Australia is consistent with the APAC and European results.

[25] Office of the Australian Information Commissioner. (n.d.). Notifiable Data Breaches scheme. Retrieved from *https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme*

Outlook

Security frameworks and compliance reporting will continue to become more complex. Businesses will continue to draw on multiple sources of information and will need to spend more time understanding the implications. The convergence of cyber and electronic, for example, will likely mean more requirements around the protection of national critical infrastructure and in the coordination and rehearsal of national cyber security strategies. Australian businesses are likely to continue their focus on the implementation the Notifiable Data Breach (NDB) scheme. There will also be some focus on the compliance with GDPR. Some compliance regulations are also industry specific and/or may require self-regulation. Businesses who accept and process payments via credit or debit cards will also need to adhere to PCI. Likewise, industries that are more regulated also have reporting around areas of data sovereignty, archive and retrieval, as well as legal discovery.

Our research shows that 70 percent of Australian business have already implemented compliance services (49 percent) or were trialling them (21 percent). This is consistent with the international results where 47 percent implemented compliance services and 25 percent were trialling them. Compliance spending will continue unabated into 2018. Our data also shows businesses to be the most complete in terms of implementation relative to other services such as cloud-based security or incidence response – remediation services. However new regulations such as GDPR and NDB will add even more pressures to businesses. A global survey conducted by Citrix in 2017 found that while 67 percent of respondents were aware of GDPR, only about half of organisations represented in the research had allocated budgets and started to prepare for new regulations.[26] In May 2018, there are additional directives coming into force, such as the NIS Directive which sets out additional requirements for member states, cross-border collaboration, and guidelines for critical sectors (e.g. energy, transport, water, financial services, health, telecom, etc.).

Recommendations

Look to Co-ordinated Approaches

Both national and cross-border compliance standards and reporting can be confusing. Many national governments are introducing new laws on data sovereignty. Businesses are best advised to work with legal teams and compliance officers to keep themselves up to date. They should look for coordinated approaches for collecting, monitoring and reporting data.

Expect more reporting requirements

While Australian businesses are looking at the impacts of the NDB scheme, EU-based companies face GDPR compliance and this will continue to be an ongoing challenge. Businesses who are trading in the EU and the UK should also consider the implications of the Data Protection Bill to the EU's GDPR. As yet, the implications are unclear, but early drafts suggest that consumer protection and reporting could be even more stringent. A national compliance law often has global implications too. Some EU countries, such as Germany, Austria and the Netherlands, have additional compliance obligations in addition to the GDPR that could be regarded as being more stringent.

Employee training and compliance awareness

While the C-Level executives and board members are taking on a fiduciary responsibility for cyber security, compliance must be improved through formal and consistent end-user training at all levels. This can help ensure employees handle customer data appropriately and adhere to corporate policies. Employees should have better means to identify potential cyber-attacks such as phishing attacks. There should be clear guidelines on BYOD, use of applications not formally sanctioned by IT and use of social media. User behaviour analytics can often identify potential threats from the inside.

[26] Ponemon Institute. (2017). *The Need for a New IT Security Architecture: Global Study on Compliance Challenges & Security Effectiveness in the Workplace*. Retrieved from https://www.citrix.com/content/dam/citrix/en_us/documents/analyst-report/ponemon-security-study-compliance-challenges.pdf

Security threats and trends

Email Threats and Phishing Campaigns

Email remains the primary mode of business and personal communications, despite the rise of messaging apps and other social media platforms. The volume of email is rising and, with this, the proportion of spam emails is rising too. Symantec estimated 53 percent of emails in 2017 were spam.[27] A growing proportion of those spam emails are now certain to contain malware.[28] In the first eight months of 2017, COFENSE Inc. identified 15 percent of all emails from a sample of 216,000 contained malware. In Australia specifically, FirstWave Cloud Technology scanned over 1.3 billion inbound and outbound emails across its customers' mail servers and blocked over 750,000 risky inbound emails. FirstWave Cloud Technology also saw a 1,178 percent increase in phishing and 1,056 percent increase in malicious URLs by volume.[29]

Email continues to be one of the major attack vectors, with malicious emails the weapon of choice in 2017. To execute a successful email based attack, the attacker doesn't have to rely on vulnerabilities but simple deception of the victim into volunteering their personal and company related information. The better the deception, the higher the chances of the victim sharing valuable data.

Common Forms of Malware and Phishing Attacks

Spam emails

Refers to unsolicited email, very often sent in bulk. Spam email continues to be the primary method of extracting sensitive data from victims, with malware carrying spam emails rising significantly in volume.[30] The sheer volume of spam emails can overwhelm many people and employees who are not necessarily aware of the implications of opening spam emails or who don't have the requisite tools to help them screen spam emails. Victims typically click on links that initiate the installation of malware, or are taken to impostor sites that are used for collection of sensitive information.

Phishing

This is a form of attack that looks to steal user data including login credentials and credit card numbers. Phishing attacks are typically based on some level of social engineering, whereby attackers track online usage and habits and try to insert themselves into the daily routine of victims, targeting websites they typically use or through emails and social media messages. The victim is deceived into opening a malicious link that then proceeds to install malware for sensitive data theft or even instigates a system shutdown as a precursor of a ransom demand *(see Ransomware on page 32)*. Phishing can also be used to gain access to corporate networks, with employees deceived so that attackers are able to bypass security parameters, distribute malware in targeted environments or even gain access to highly confidential information.

Spear-phishing emails

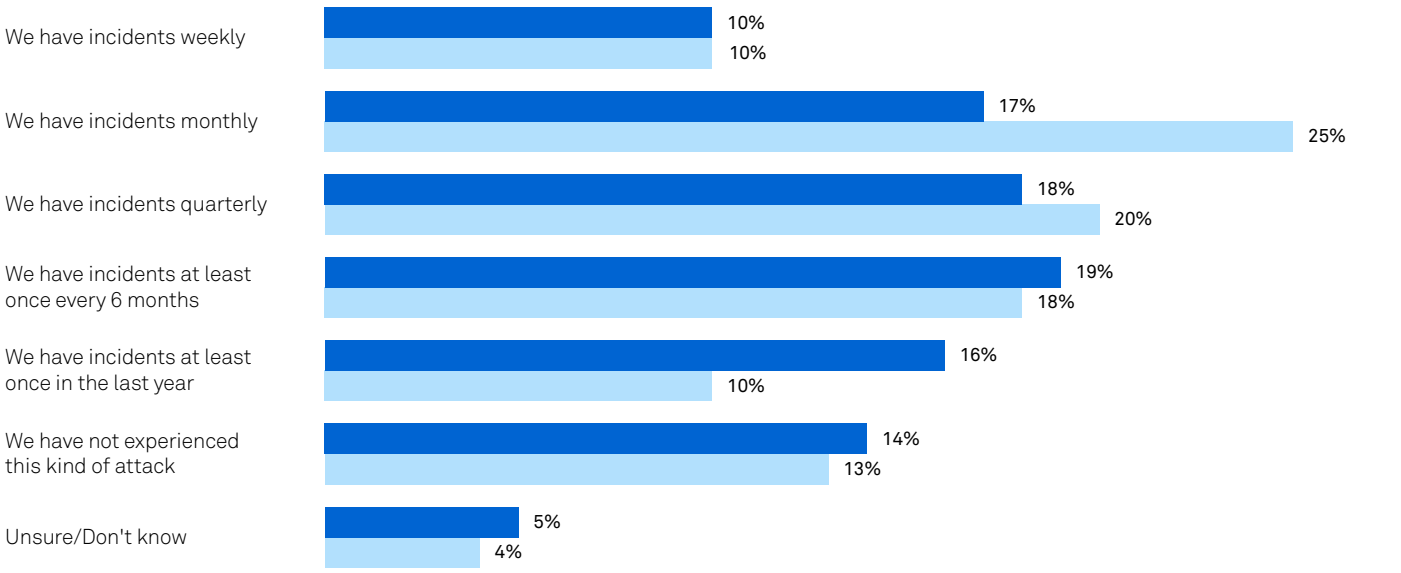
This is a particular form of phishing attacks that typically targets either specific individuals or organisations with high ranking executives or officials to gain access to sensitive data and information. This practice is called whaling.

[27] Symantec. (2017). *Internet Security Threat Report*: Volume 22. (Symantec Corporation Report). California, USA: Author. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf
[28] COFENSE Inc. (formerly PhishMe) (2017). *Enterprise Phishing Resiliency and Defence Report*. USA: Author. Retrieved from https://phishme.com/phishing-resiliency-report-2017/
[29] Please note: these numbers are approximated by using statistical methods on representative data samples.
[30] Symantec. (2017). *Internet Security Threat Report*: Volume 22. (Symantec Corporation Report). California, USA: Author. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

In our research, 68% of global respondents and 60% of Australian respondents report that their business has been interrupted due to a security breach in the past year. In Australia, the number of attacks via phishing and malicious emails is steadily rising. Among the subset of organisations (those that have been interrupted due to a security breach), our research shows that 11 percent of Australian enterprises reported incidents on a weekly basis in 2017, with 25 percent reporting incidents on a monthly basis. Compared to the global results, Australia tends to have greater instances of monthly and quarterly attacks.

Q: How frequently has your organisation experienced phishing attacks in the past year?

A subset of organisations which have had business interrupted by a security breach in last 12 months



Australia n=166; Global n=1,214

Global Australia

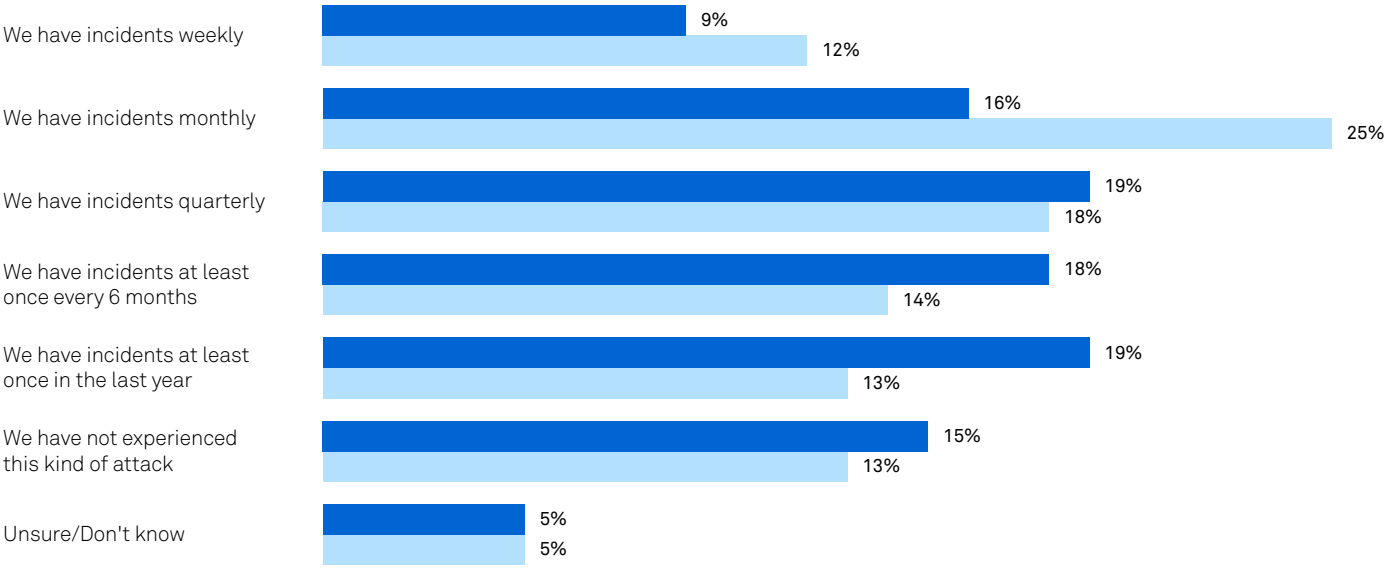
Business Email Compromise (BEC)

BEC involves attackers using credential grabbing techniques to steal sensitive personal or corporate information. Some are email attacks designed to gain access to the accounts of high level executives or public officials. When the objective is to observe traffic, collect data and remain below the radar, these can be associated with APTs.

Others may use a compromised email, for example, to coax employees or business partners to make a fraudulent payment. This can often happen while the executive is travelling. Hackers can set up a rule to redirect or delete a certain thread of emails to avoid detection. In Australia, according to the Australia Cyber Security Centre Threat Report 2017, an attack was launched on a local company wherein the attackers managed to pose as the CEO and COO, sending sequential emails requesting a large transfer of money. The company, not realising that the emails were fraudulent, made transfers in excess of US$500,000 to accounts in overseas jurisdictions.[31] In a global study conducted between October 2013 and December 2016, the FBI estimated this scam to cost businesses in excess of US$5.3 billion dollars.[32]

Frequency of Business Email Compromise (BEC) Attacks

A subset of organisations which have had business interrupted by a security breach in last 12 months



Australia n=166; Global n=825

Global Australia

[31] Australian Cyber Security Centre. (2017). Australian Cyber Security 2017 Threat Report. Canberra, Australia: Author Retrieved from *https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf*
[32] Federal Bureau of Investigation. (2017, May 4). *Public service announcement*. Retrieved from *https://www.ic3.gov/media/2017/170504.aspx*

Outlook

Our data shows that email based attacks are amongst the highest security risks for IT departments in Australia. Nearly a quarter of respondents whose business has been interrupted due to a security breach in the past year indicated that their business had experienced a BEC or phishing attack at least once a month. The costs of such attacks can be significant, with either direct financial costs as a result of a breach, or lost customer revenues and brand equity due to downtime or fraudulent transactions. It is imperative that Australian enterprises and individuals take active steps to protect themselves against these increasingly prevalent attack vectors.

Recommendations

Implement corporate policies

Besides taking preparatory measures, education and training is crucial. Some IT departments undergo fake phishing attack drills to see how well employees are prepared. Businesses should also consider other corporate policies on money transfers or other critical information exchange to reduce the likelihood of falling victim to phishing attacks or BEC.

Consider multi-factor authentication

Implementing multi-factor authentication for specific corporate email and corporate network access would mitigate the potential for an attacker gaining access through stolen credentials, such as a username and password. More sensitive sectors should consider integrating authentication with building access management systems, biometrics or facial recognition. Of course, the level of caution would need to be commensurate with the value of the data and the impact of a loss.

Strict password management policies

In addition to implementing multi-factor authentication, organisations should also look at strict policies for password management. Frequent password changes with the inability to reuse previous passwords are fast becoming the norm, along with other measures. Security enforcement will also have to be balanced with user experience to avoid IT workarounds and increase chances of adherence to policy.

Ransomware

Ransomware is another form of malicious software targeting both human and technical weaknesses in an effort to deny the availability of critical data and/or systems. Ransomware is frequently delivered through various methods. Phishing is one of the most common tactics, where a user is enticed to click on an email attachment labelled as 'invoice', 'receipt' or 'delivery'. Once the victim opens the file, malware is installed onto the computer through a hidden downloader. This attack spreads quickly and often goes unnoticed. When the victim determines they are no longer able to access their data, the cyber adversary demands the payment of a ransom. The common form of payment is with cryptocurrencies such as Bitcoin. The adversary will often promise the victim will regain access to their data once the amount is paid by a set deadline e.g. 48 or 72 hours. If the ransom is not paid however, the encrypted files will be destroyed.

Some of the major methods for ransomware include:

Exploit kits

This can happen when users, for example, click on a malicious advertisement (malvertisement) and are redirected through a compromised website. In many cases malicious code is embedded into web pages hosted on compromised servers. Some recent examples include Cerber and CryptXXX.

Server vulnerabilities

This type of attack is carried out by gaining access to the network by targeting server vulnerabilities. Examples like WannaCry and NotPetya became some of the most damaging ransomware attacks in 2017. These attacks targeted a vulnerability in Microsoft's implementation of the Server Message Block (SMB) protocol. These strains travelled quickly through other infected, unpatched machines across a network without any human intervention. Within a short period of time, both became worldwide affecting 300,000 computers in over 150 countries.

Brute force on remote desktop protocol (RDP)

Another tactic for ransomware is cracking passwords through RDP. A study by Sophos found this to be problematic for small businesses as they tend to outsource their IT to third-party contractors who typically accessed and connected to these businesses systems through RDP.[33] Once this system is hacked, a criminal holds their key to the impacted business IT systems.

Third–party app stores

Ransomware can also be downloaded from non-trusted third-party app marketplaces where malware is embedded inside the software to be downloaded, typically on a mobile device.

Connected devices

With the emergence of IoT, new strains of ransomware are targeting control systems, assembly lines and power systems. These work by locking the underlying boot system, thus rendering the devices inoperable without an option to restore them from backups or a decision by the victim to pay the ransom.

[33] Stockley, M. (2017, November 15). Ransomware-spreading hackers sneak in through RDP. Retrieved from *https://nakedsecurity.sophos.com/2017/11/15/ransomware-spreading-hackers-sneak-in-through-rdp/*

The not-so-randomness of Ransomware

Ransomware was a major problem in 2017. Symantec found many businesses can be overwhelmed with the sheer volume of emails they were receiving laden with ransomware. In one attack in 2017, a campaign unleased 23 million emails within 24 hours.[34]

Symantec found that, increasingly, the ransomware market is moving away from spray and pray tactics targeting the average consumer through phishing campaigns, to more sophisticated attacks. In the latter, cyber criminals conduct more reconnaissance first, resulting in the purposeful targeting of specific companies or industry verticals, like a health care provider securing patient records. Through social media searches, they may even look for details of individual employees or departments working within these companies before launching their attack.

Some strains of malware will also look for ways to attack back-up systems first, as a means to increase the price of the ransom. Other variants such as Zepto will target more valuable files first such as virtual wallets and documents over other forms of files, believing they would be able to reap larger sums. In this way, ransomware attacks are proving to be not so spontaneous, but more methodical, targeted and pre-planned. Many companies in verticals such as government, healthcare, telecommunication, transport, banks, retail companies, utilities and manufacturing have found themselves targets of such attacks. One possibility is many industries, particularly those that are heavily regulated or rely heavily on IT, may be more willing to pay a ransom.

Shipping container company Maersk was attacked in June 2017 and disclosed their estimated damages to be in the range of $300 million. The infection hit its global network and impacted shipping across 76 ports.[35]

[34] Mathews, L. (2017, August, 8). Massive Ransomware Attack Unleashes 23 Million Emails In 24 Hours. Retrieved from *https://www.forbes.com/sites/leemathews/2017/08/31/massive-ransomware-attack-unleashes-23-million-emails-in-24-hours/#3cefd57a394b*

[35] Thomson, I. (2017, August 8). NotPetya ransomware attack cost us $300m – shipping giant Maersk. Retrieved from *https://www.theregister.co.uk/2017/08/16/notpetya_ransomware_attack_cost_us_300m_says_shipping_giant_maersk/*

Our research on ransomware revealed the following insights:

Attacks are inevitable

Thirty one percent of Australian respondents whose business has been interrupted due to a security breach in the past year are experiencing ransomware attacks on a weekly or monthly basis, the highest among all countries surveyed. In the APAC and European region, this figure was only 22 percent. The UK figure is 25 percent, second to Belgium at 29 percent for the European markets. Over the course of 2017, Australia had the highest rate of ransomware attacks at 76 percent, followed by Europe and Asia Pacific, both at 74 percent. Respondents reported more ransomware attacks in this years' survey than previous years.

Around half of business victims pay the ransom

Some 47 percent of Australian businesses who found themselves victims of ransomware paid the ransom, which was consistent across APAC. Some 60 percent of ransomware victims in New Zealand and 55 percent in Indonesia paid the ransom, making it the highest for Asia. In Europe, 41 percent of respondent ransomware victims paid up.

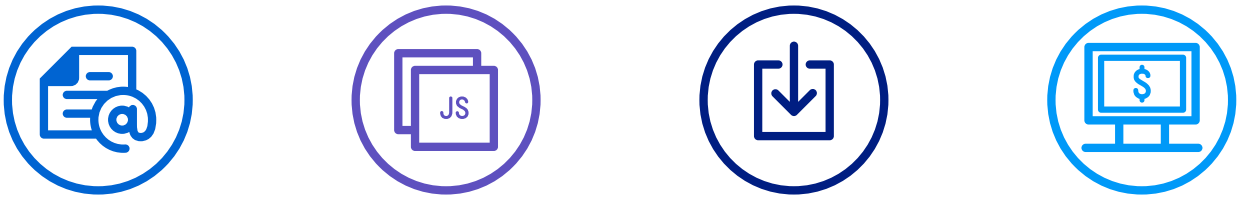
Most are able to retrieve data after payment

Eighty six percent of Australian businesses who paid a ransom were able to retrieve their data after the payment. In Asia, this figure was slightly higher at 87 percent, and slightly lower for Europe at 82 percent. Our research suggests that ransomware that specifically targets businesses tends to be more sophisticated, with attackers having the ability to release files, typically through central command and control systems, once the amount has been paid.

Many would pay again

In Australia, 83 percent of respondents would pay the ransom again if there were no back-up files available. Across Asia, 76 percent would also consider paying again as would 80 percent of European businesses. It should be noted that an increased number of ransomware variants will attempt to attack some files, such as a back-up systems, as a first priority. This is often in an effort to increase the price of the ransom.

Typical emailed malware infection process



01
Email received disguised as routine notification, most commonly an INVOICE or RECEIPT

02
Includes attachment, typically JavaScript file or Office file containing malicious macro

03
Opened attachment executes PowerShell script to download malware

04
Malware downloaded is typically ransomware

Source: Symantec

Ransomware as a Service (RaaS)

Ransomware will continue to be one of the most prevalent attacks. Perpetrators are being greatly assisted by the emerging Ransomware as a Service (RaaS) market where malware authors have developed user-friendly interfaces and offer them to others to become distributors. Customers can buy RaaS or have an author custom build a ransomware capability to take to market.

Anonymous communications and are making it easy for buyers and sellers to connect in underground markets, and cryptocurrencies have made it easier to transact. These two factors have essentially lowered the risk and reduced the barriers to entry.

RaaS 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.

There are approximately 6,300 marketplaces selling ransomware in the dark web with 45,000 product listings.[36]

Each RaaS instance offers different features to recruit distributors, typically based on claims of detection avoidance options and different profit models. RaaS features may include different encryption options, worm features to infect more users, multiple language options, documentation and the promise of lifetime access and future releases. The prices for do-it-yourself (DIY) kits range from US$0.50 to US$3,000. The median price is US$10.50. Some RaaS offerings are initially free, with approximately 15 percent to 40 percent of the profit share from the attack going back to the author.[37]

Some companies are brazen in their offer of ransomware on the public Internet. Rainmaker Labs launched a RaaS called Philadelphia in 2017. This was marketed through YouTube and other channels as a complete crimeware package. Their launch was supported with a brochure and video advertisements promoting configurations and features, such as campaign colour schemes, PDF reports and charts tracking the effectiveness of ransomware campaigns. There was also a degree of automation for managing and planning attacks as well as for the collection payments. Similar to how many cloud providers would market their services, Philadelphia offered options for hosting (e.g. dedicated, shared) without having to invest in dedicated infrastructure (e.g. command and control servers).

[36] Carbon Black (2017). The ransomware economy. Massachusetts, USA: Author. Retrieved from *https://www.carbonblack.com/resource/the-ransomware-economy*
[37] Ibid

Outlook

The global ransomware market is growing at an explosive pace. Carbon Black estimates the ransomware market grew by 2,502 percent in 2016 to 2017, costing businesses US$1 billion dollars.[38] As ransomware becomes more targeted, the ROI will increase for attackers. Businesses by and large will pay a premium to recover encrypted files. Symantec found the average ransom demand in 2016 rose to US$1,077, up from US$294 just a year earlier. At the same time, the number of ransomware families identified in 2016 was 101 compared to only 30 in 2015.[39] This suggests ransomware is profitable and becoming mainstream. New strains of ransomware in 2018 will focus on exfiltration of data before encryption to reap additional commercial rewards for stealing corporate intellectual property. There will also be some more focus on attacking connected devices and the greater use of AI and machine learning to discover more vulnerabilities.

Recommendations

Preparation is key

With a growing number of businesses reporting a ransomware attack in the past year, organisations should identify critical data and ensure regular offline backups and versioning are performed. Some variants of ransomware are also targeting backup systems. Backup systems should also be encrypted so that data does not fall into the wrong hands.

Patch early and often

Conduct regular security patching/ updates for operating systems and applications to mitigate risks associated with exploit kits and malware. This is particularly important for Java, Adobe Reader, Flash, Silverlight and other applications regularly targeted by exploit kits.

Have a plan for ransomware

Ensure that incident response plans and business continuity plans are in place. This includes regular disaster recovery drills are performed to ensure that backup data can be used to return the business back to normal operation within acceptable time frames.

Consider external resources

The worldwide 'No More Ransom Project' offers prevention advice and you can check to see whether they have the tools for decrypting some files via recovered keys. 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. Other advice is available from CERT Australia to assist with managing ransomware risks, reputable security vendors and security service providers.

[38] Ibid
[39] Symantec, Internet Security Threat Report, April 2017. *https://www.symantec.com/security-center/threat-report*

Mobile Security

The proliferation of sophisticated smartphones and consumer IoT devices such as wearables continues. Many countries populations are skewing towards mobile broadband adoption versus fixed. This adoption has in turn spawned new attack methods and increased frequency of attacks.

Common Attack Methods

There are a number of methods for the delivery of malware and other security hazards to mobile devices, such as phishing. Another challenge in mobility security is data leakages, which can occur when users give sweeping permissions to apps and services without realising the implications. Typically, these tend to be free apps which sometimes go beyond the advertised features and functionality by sending sensitive information to remote servers.

Another increasingly prevalent scenario is when mobile users try to root their devices to get around enterprise mobile device management (MDM) solutions, thereby exposing their devices to attack.

Other known mobile device vulnerabilities

Unsecured WiFi and network spoofing

It is very common for users, especially consumers, to seek out WiFi hotspots for connectivity in various situations. These WiFi access points are frequently unsecured and can be used to compromise connected mobile device users. In other scenarios, network spoofing is where adversaries set up fake access points to impersonate legitimate public locations at high traffic locations like coffee shops and airports. These spoofed access points then encourage users to log in or create an account, with potentially damaging consequences. For example, key reinstallation attacks (KRACKS) leverage vulnerabilities in the WPA2 protocols of WiFi networks in order to steal sensitive information including login credentials as well as files. Exploits such as Broadpwn, which targets vulnerabilities in Broadcom chipsets, allow attackers to hack into phones.[40]

Malware in app stores

The biggest emerging threat in mobile security relates to the rise of trojanised applications on app marketplaces. Malware can be carried in apps marketed as open source, free, music player and file explorer applications. McAfee discovered malware it called Grabos, versions of which were found in a number of applications, all designed to deceive the victim into a download, following which they are prompted to install more apps which stay open in the background, collecting information. Grabos was able to evade security tools by updating its settings every 24 hours.[41]

Mobile botnets

These are botnets that, once on a mobile device, proceed to infect applications already installed. In August 2017, WireX targeted vulnerable devices by infecting them and creating a botnet that generated DDoS attacks. These are similar attacks to Mirai, but focus on mobile devices.

[40] Greenberg, A. (2017, July 7). How a Bug in an Obscure Chip Exposed a Billion Smartphones to Hackers. *Wired*. Retrieved from https://www.wired.com/story/broadpwn-wi-fi-vulnerability-ios-android/
[41] Hackett, R. (2017, September 14). Massive Android Malware Outbreak Invades Google Play Store. *Fortune*. http://fortune.com/2017/09/14/google-play-android-malware/

Outlook

Businesses will continue to support employees using personal or work devices remotely. This is often a requirement for attracting top talent. While bring your own device (BYOD) was popular a few years ago, some businesses have moved to alternate models of choose your own device (CYOD); company-owned, personally expensed (COPE); and company owned, business only (COBO). Some business will use several models, and each have a varying degrees of risk. Our research shows a relatively even distribution of concerns around the security of mobile devices from malware, loss of corporate data, setting the right identity and access management, to balancing employee monitoring with privacy.

Recommendations

Consider MDM and IPS solutions

Enterprise mobility management (EMM) solutions such as device management can help to protect employees. They can provide additional security when employees are accessing corporate data from their personal device and carry out commands such as remote lock, wipe and delete when devices are lost or stolen. These solutions have been very effective in supporting businesses with policies such as BYOD.

Secure the end–user experience

There are a number of solutions available for security managers, such as the ability to deploy whitelisting, restricting access to application downloads, and continuous security scanning. In many cases, such measures need to be balanced with the real life experience of using the devices, increasingly in remote locations and outside the corporate office. There have been cases where remote wiping of business data mistakenly deleted employee personal data. Any mobile device management policy, especially outside of COBO, should seek the input of employees, human resources and legal teams as a starting point.

Factor in IoT convergence

Enterprise mobility solutions are also moving into the IoT and budgets are starting to converge. There are a growing number of use cases where IoT is being integrated with Artificial Intelligence (AI), for example, and staggering growth in data collection. It is imperative that any security posture factors in the use of cloud and the pervasiveness of IoT enabled devices. The problem it is difficult to create transparent visibility and management across all devices and why a security fabric should perhaps be considered.[42]

Secure mobile channels

Mobile apps are becoming more customer oriented and being integrated as part of the delivery of an omni-channel experience. In some cases, these apps interface with other channels like a contact centre, and even accept payments. It is imperative that ownership is established for customer data, especially where analytics is used, and the data is adequately secured. There are often no clear rules on how data should be passed from one channel to the next while keeping the conversation in session and context.

[42] Fortinet, Rethinking the Approach to Cybersecurity, February 2017. *https://www.fortinet.com/demand/gated/WP-Rethinking-The-Approach-To-Cybersecurity.html*

Advanced Persistent Threats (APTs)

APTs can be very dangerous, especially from the perspective of theft of intellectual property (IP). APTs use multiple phases to watch and eventually break into a network while avoiding detection. The primary objective is to harvest valuable information over the long term. Unlike DDoS or ransomware attacks which are public and out in the open, APTs aim to evade detection, blend in with other traffic, communicate infrequently if necessary and circumvent security measures designed to defend against them.

APTs are typically carried out in several phases:

Step 1. Reconnaissance.

APT threat adversaries 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.

Step 2. Gaining initial entry.

The initial compromise is typically achieved through spear phishing or a malicious payload delivered from a compromised website. Some APT attacks utilise zero day vulnerabilities to evade detection. A zero day exploit may execute on the target device, implant malware and open a backdoor to communicate back to command and control (C&C) servers.

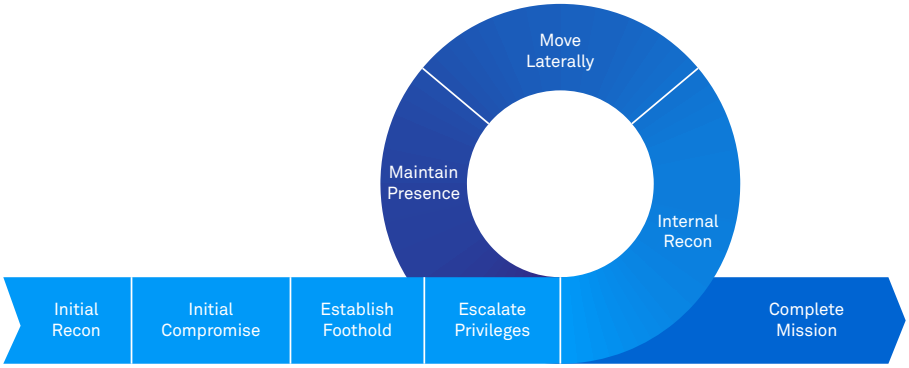
Step 3. Discovery and exfiltration.

The attacker then harvests access credentials from users to obtain escalated privileges. The persistent nature of an APT attack is achieved through establishing a presence by deploying backdoors on multiple computers that are used to communicate back to C&C servers. These are used for remote discovery activities, moving laterally through the targeted systems to exfiltrate the desired data back to the attack team for further analysis.

Techniques

APT attacks use a number of ways to gain entry such as spear phishing, direct hacking systems, delivery of attack code through USB devices, and penetration through partner networks. Once in place, APTs can move laterally through data centre networks and blend in with normal network traffic to achieve their objectives. According to our research, among the respondents in Australia whose business has been interrupted due to a security breach in the past year, 30 percent of them experienced an APT attack on at least a monthly basis. This is up 8 percent from the previous year. In APAC, this figure was 22 percent, which is slightly higher than in Europe, where one in five respondents reported APT attacks at least once per month.

APT Phases of an Attack[43]



Source: Infosec Institute

[43] Infosec Institute. (2017). Anatomy of an APT Attack: Step by Step Approach. Retrieved from *http://resources.infosecinstitute.com/anatomy-of-an-apt-attack-step-by-step-approach/#gre*

Outlook

The focus of APT will remain on the theft of commercial secrets and the main industries targeted will continue to be banks, consulting and IT companies, manufacturing and government. Major events are also likely to be APT targets, and there may also be some headline grabbing incidents of using APTs to achieve cyber-attack objectives.

Recommendations

Threat hunting

APTs and zero day attacks are often designed to steal the most sensitive data and corporate secrets. APTs can combatted through threat hunting practices. In many cases, organisations employ third parties look for system vulnerabilities and abnormal activities.

Consult third-party resources

MITRE, a non-profit research organisation, has developed a methodology, called ATT&CK, for threat hunting. This methodology is specifically focused on understanding the potential attacker, motives, possible moves and evasion strategies. This helps organisations better prepare and defend against these threats.

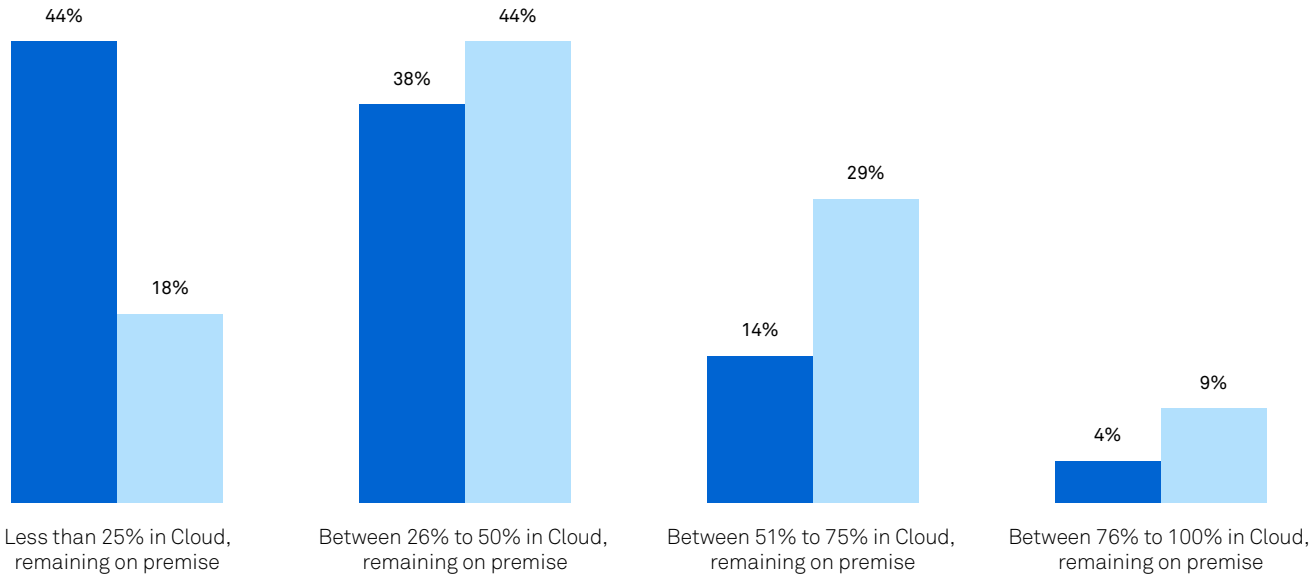
Consult independent advice

CISOs are looking at ways to reduce dwell times. When breaches occur, they can often rest dormant in the system for weeks, months or longer. When these breaches are discovered, it has often been by third-party experts. Businesses with sensitive data should make system scans, audits and threat hunting routine.

Cloud Security

The migration and deployment of applications across public, private and hybrid cloud environments will likely continue into 2018. Our research indicates that respondents see less than 20% percent of workloads in Australia are anticipated to remain on traditional on-premiseo infrastructure ver the next two years. This is consistent with results in APAC at 19 percent and Europe at 17 percent. However, businesses will continue to have some workloads on-site. Less than 10 percent of respondents foresee more than 75 percent of their workloads moving to a cloud environment in the next 24 months.

Q: What percentage of the workload do you have in the cloud today? What percentage do you anticipate in two years?



Australia Results; n=279

The typical business can support up to 10 different cloud environments and sometimes even more. Hybrid cloud – defined as running clouds across multiple environments – is fast becoming the de facto industry standard. The security implications of running applications in these more complex cloud environments is that traffic is also shifting from the north-south direction (typical for perimeter security) to an east-west flow. Many data centres are also software-defined and are increasingly interconnecting with one another. This can help businesses access cloud services, and improve business continuity, content distribution disaster recovery and back-up solutions. 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.

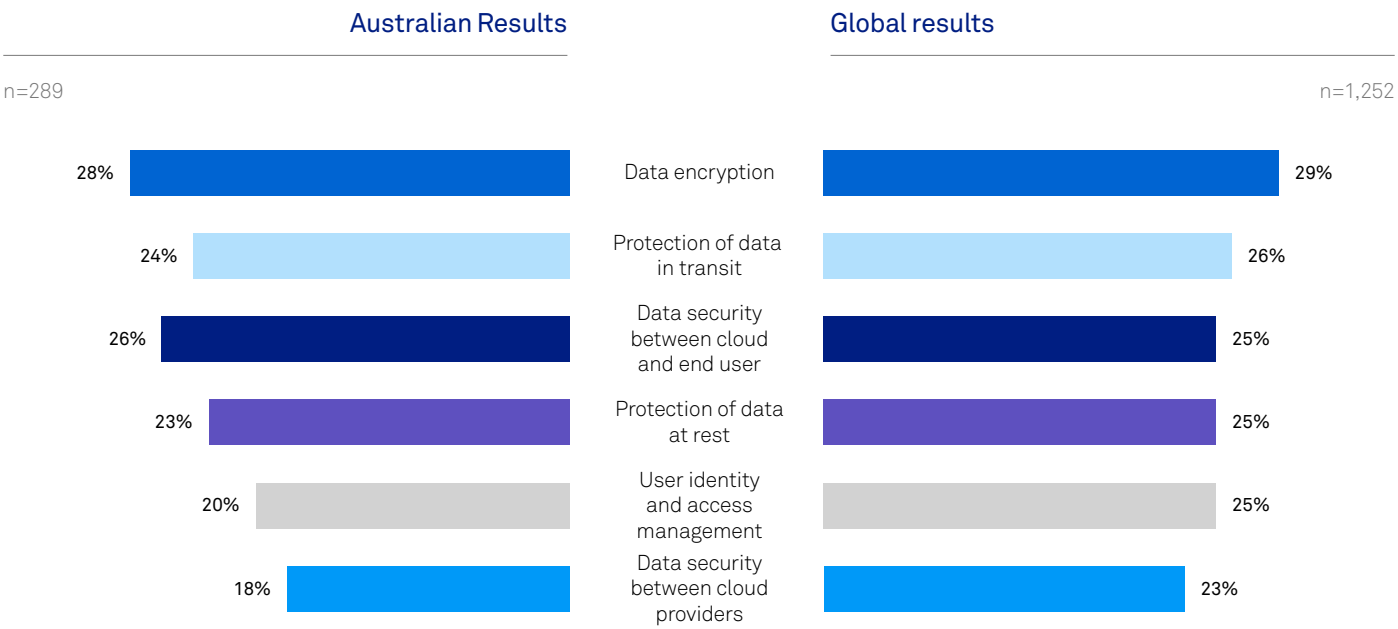
Security management is further complicated by the dynamic nature of these virtualised applications, able to be moved between host servers as resource demands change. The rise of mobile applications and cloud-based environments means that there is a heightened risk of malware spreading laterally throughout IT environments.

Top Perceived Threats

Our research shows that some of the top concerns for both Australian and global respondents for cloud security are data encryption, data security between cloud and end user, and protection of data in transit.

Some common concerns are around file integrity monitoring, data classification and detection of shadow IT systems. Others are around the ability to map workloads to the appropriate cloud environments. Our research also show that cloud services are the most frequently highlighted security concern in Australia, APAC and Europe in the context of all other possible threat vectors such as mobile devices, operating systems and databases.

Q: In cases where applications / data are stored and accessed from the cloud, what are the top security considerations? (Top 6)



Outlook

Cloud continues to be a perfect storm in IT. The requirement for cost efficiency, agility and scale needs to be balanced with security, managing risk and achieving compliance. Our survey results confirm cloud adoption plans continue into 2018. Within the next year, up to half of all enterprise environments will integrate cognitive AI technologies into unified communications and collaboration (UC&C) environments. By 2020, up to half of all large IoT implementations will be deployed from the cloud.[44] As businesses deploy more workloads to the cloud, they will also need to mitigate all potential threats. These can range from authentication, proxy attacks (e.g. man in the middle), malware (e.g. ransomware), the growing number of injection attacks (e.g. LDAP, SIP, SQL, SIP, XML), cross side scripting, through to DDoS attacks.

Businesses will also have to consider the trade-offs between managing data though private, public or hybrid clouds. There are limitations on what cloud providers are liable for in the event of a breach that also need to be considered when choosing between platforms. There will also be risks in shadow IT which will need to be mitigated with end-users.

Recommendations

Embrace Zero Trust for Network segmentation

To maintain IT security in virtualised public and private clouds, business can look to mitigate the threat of breaches by segmenting network, users and applications by using a virtual secure gateway at the switch layer. This can help to obtain visibility and control of any malicious traffic moving laterally in cloud environments. Palo Alto Networks, for example, extends the Zero Trust concept – never trust, always verify – to network segmentation. Access, for example, should be granted for specific applications based on credentials. There is also control over what content can be sent at each segmentation point.[45]

Conduct continuity planning

Uptime can be improved through effective business continuity and disaster recovery (BCDR) planning. This planning should consider back-up and recovery systems that align to recovery time objectives (RTO) and recovery point objectives (RPO). These should also be tested regularly.

Coordinate cloud and mobility policies together

Identity and Access Management (IAM) needs should also look at the trade-offs of single sign on and federated sign-on. These policies should also be roles-based, policy enforced and ideally context-aware. Cloud access management should align with the enterprise mobility policies practiced by the organisation.

Consider cloud access security brokers

Cloud access security brokers (CASBs) are a visibility and policy control point for security services. They can be a proxy-gateway, hosted agent and an API-based service. They will often integrate with log files, identity and access controls to improve cloud security. This can be measured by greater visibility, reducing the threat of shadow IT, compliance, threat prevention and data loss prevention. For the second year in a row, our research shows a strong interest for these types of solutions to support cloud security issues.

[44] Estimates provided by GlobalData for this report

[45] Palo Alto Networks. Whitepaper: *Securing Traditional and Cloud-Based Data Centers with Next-Generation Firewalls*. https://www.paloaltonetworks.com/resources/whitepapers/securing-your-virtualized-data-center-with-next-generation-firewalls#

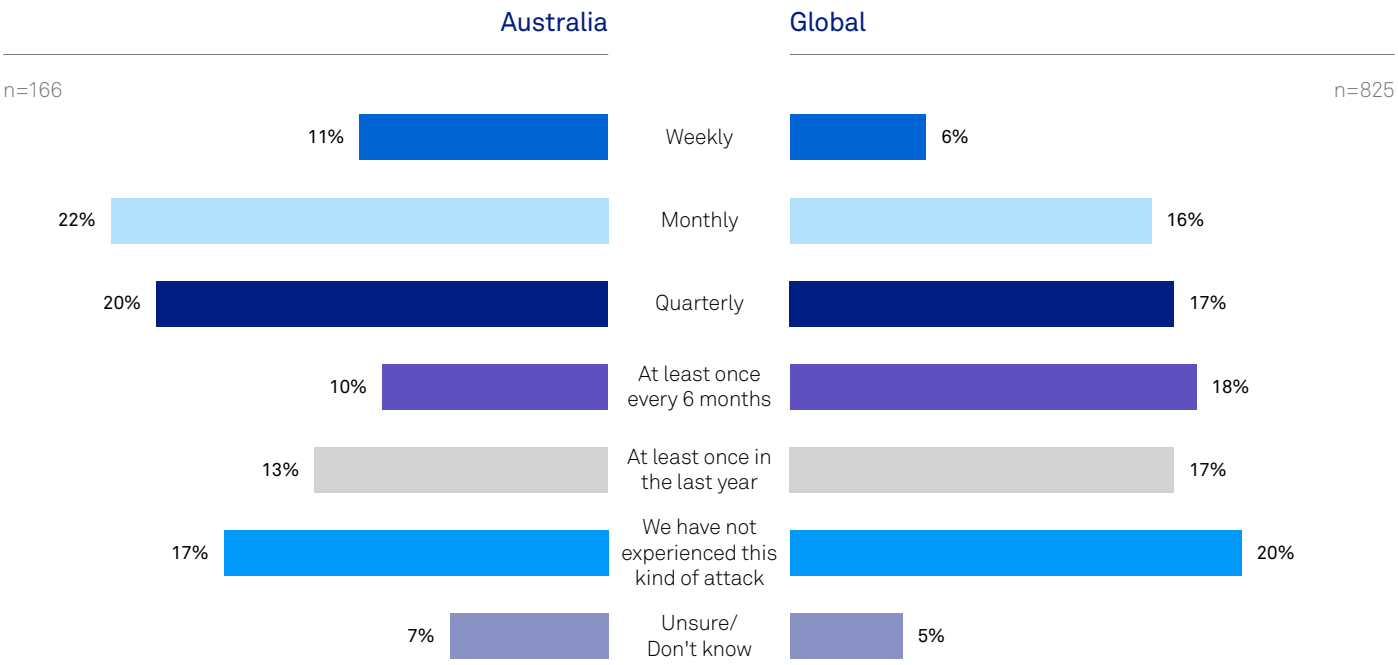
Distributed Denial of Service (DDoS)

Distributed Denial of Service (DDoS) threats typically render online websites and services unavailable by overwhelming them with surges in traffic from multiple sources. The two most discussed are application and network layer attacks. DDoS attacks are becoming increasingly more sophisticated, generating much higher volumes of traffic. Targets for these attacks are various industries and resources, from banking and financial institutions to e-commerce companies and news and online content services. According to Akamai, Q3 2017 saw an eight percent rise in total DDoS attacks over the previous quarter, even though the total was down three percent from the previous year. The vast majority of these attacks were volumetric attacks.[46]

In Australia, among the respondents whose business has been interrupted due to a security breach in the past year, our research indicated that 11 percent of organisations experienced a DDoS attack weekly, while 22 percent experienced attacks every month. 29 percent of organisations, suffered outages ranging from 30 minutes to two hours before they were able to get back online. Most of these attacks were detected within minutes or hours. Surprisingly, the Australian numbers indicate 54 percent experience business impacting DDoS attacks weekly, monthly or quarterly, which is significantly higher than Asia-Pacific (41 percent), European countries (37 percent) and even the UK (39 percent) which has been a perennial target for large scale DDoS attacks over the years.

Q: How frequently has your organisation experienced the following business impacting cyber security incidents in the past year? Distributed Denial of Service DDoS Attack

A subset of organisations which have had business interrupted by a security breach in last 12 months



[46] Akamai. Q3 2017 State of the Internet / Security Report *https://www.akamai.com/us/en/about/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.jsp*

There are different types of DDoS attacks.

Volumetric attacks

The most common type of DDoS attacks, these attacks are also known as 'floods' and typically account for the majority of total DDoS incidents. Akamai estimates that 99 percent of the total DDoS traffic through its networks in Q3 2017 was volumetric in nature.[47]

Fragmentation attacks

These send a flood of fragments, either TCP or UDP fragments, to a victim's site or service. The victim's servers are unable to reassemble the fragments and this results in severely degraded performance.

TCP connection attacks

These focus on infrastructure components like firewalls, web servers and load balancers. By maxing out the available connections to these devices, these attacks can severely disrupt connections.

Application attacks

These occur when attackers target the application layer of the OSI model with a view to disabling certain features or functionality. These attacks don't target the whole network, but instead target specific application packets. This often distracts already stretched internal resources from monitoring and detecting security breaches.

Zero day DDoS attacks

These happen when external adversaries exploit a previous unknown vulnerability or flaw.

IoT and the Evolving DDoS Landscape

The ability to launch a DDoS attack has become significantly easier, with entry barriers coming down, both in terms of cost as well as attack kits. This is particularly true for volumetric DDoS attacks aimed at the infrastructure layer. Moreover, DDoS attacks are increasingly available "as a service" making them even easier to initiate. Attackers are also taking advantage of the boom in cryptocurrency to demand payment for attack resolution from the victim, or even as a payment to launch an attack.

Moreover, the scale of individual DDoS attacks is also rising with the advent of IoT. Connected devices, especially consumer devices, such as digital cameras, are being installed across the world and many of them have not been secured - left with factory default settings and passwords. The implication of this is that attackers could install malware on the devices, program them for future use, or enlist them in a global army of bots with minimal investments.

[47] Akamai. Q3 2017 State of the Internet / Security Report *https://www.akamai.com/us/en/about/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.jsp*

APT Phases of an Attack[43]

1. Recon

Scan for Telnet
(remote admin port 23)

Brute force admin

Use same credentials on all
same make/model devices

2. Build

Install malware

Auto build "Thingbot"

3. Attack

Attack!

Plethora of options
depending on the device

Source: F5 report

The best example of the potential damage and havoc created by these botnets was the attack on one of the key hubs of the Internet hosting the bulk of the web's domain name server (DNS) infrastructure. The sustained attack in October 2016 brought down several major websites and services, as well disrupting trans-Atlantic Internet traffic. The source of the attacks was the Mirai botnet, and it was estimated that the attack had involved over 100,000 malicious endpoints which issued a DDoS that peaked at 990 Gbps.[48]

[48] Gaining control to access credentials to IoT devices is one the most frequent ways an attack is launched. F5 conducted a study of top 50 most commonly attacked administration credentials and found in 94 percent of the cases.

Outlook

DDoS attacks are among the main drivers explaining the gradual convergence of cyber and electronic security. The Mirai botnet taught the industry about the effectiveness of taking control of IP cameras, home routers and other connected devices to deliver seismic attacks. This was one of the largest attacks ever seen, to date. DDoS attacks are becoming increasingly sophisticated and varied, with many targeting the application layers (WireX) as well as targeting unsecured IoT devices to disrupt networks. The threat from IoT botnets is increasingly dangerous. It will also become easier for anyone to access botnet kits. While we have seen some evidence of the havoc botnet attacks can cause, there are still unknowns, such as the number of botnets lying dormant until they receive new commands to launch an attack. There have been targeted attacks on utilities, manufacturing and other industries designed to create physical damage to machinery, property or control systems. In 2018, we expect DDoS attacks to increase focus on IoT devices, especially if security controls continue to be lax. DDoS will also start to be part of broader battle plans.

Recommendations

Secure IoT devices

Network administrators should bring the same vigilance with protecting ICT environments as they would with connected devices. Several security vendors have found lax password enforcement and use of default passwords to be some of the major issues.[49] A DDoS attack on a benign peripheral device could be a backdoor for something more sinister.

Prepare for a broader attack surface

One of the underlying reasons cyber and electronic are starting to converge is they are becoming interconnected in regards to facing emerging threats. DDoS planning should also consider industrial controls including SCADA, environmental controls, beacons, sensors or other connected devices. The motive of an attack may be an attempt to disable machinery and could potentially target any industry.

Consider multi-layered DDoS systems

Businesses should consider the many ways to detect and respond to DDoS attacks. This can be premise-based solutions and cloud overlays. This can include scanning for misconfigured ports. There is network-based technology that can help mitigate the impact of an attack. Again, any solution should be tested regularly.

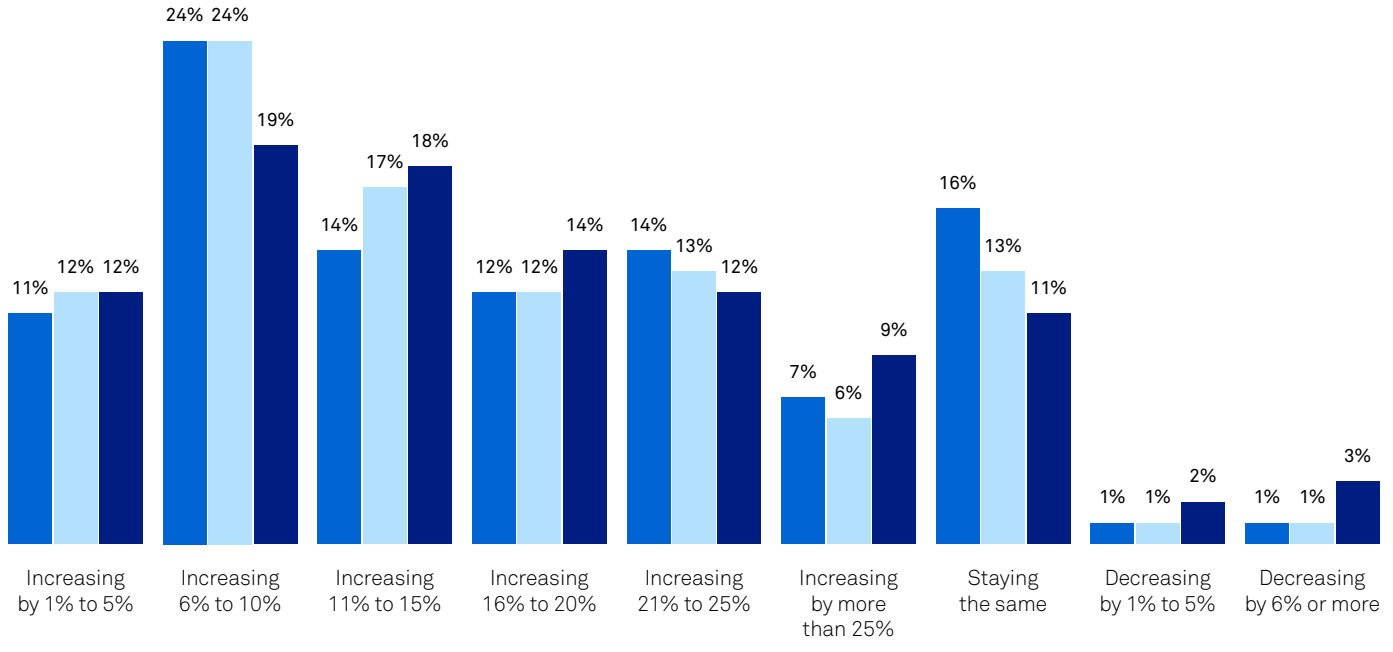
[49] Usernames and passwords were exactly the same. Symantec concluded in a recent report that default passwords are still the biggest security weakness for IoT devices. The password most commonly tried by attackers is "admin".

Security trends and future investments

IT and Security Investments

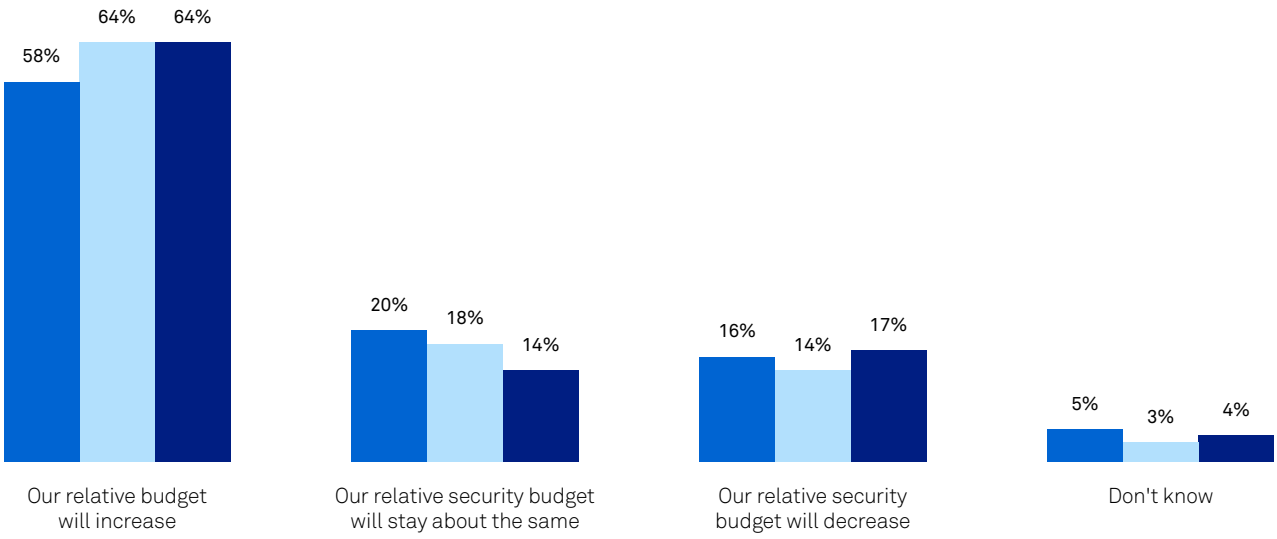
As indicated previously in this report, the majority of businesses indicate they are planning to combine their cyber and electronic security budgets. We also note consistencies in notification, frequency of reporting and involvement with multiple lines of business. For example, the top five departments, operations, finance, regulation and compliance, legal and facilities are the same, but with a different ordering in the Australian and global results. In terms of spending, our research highlighted security spending is also projected to increase in absolute terms in the next 12 to 24 months, but also relative to the percentage of total ICT budget. The table below shows the results for Australia, APAC and Europe.

Q: Absolute Budget: With the next 12 to 24 months, is your overall security (cyber and electronic) budget increasing, decreasing or staying the same?



Australia n=289; APAC n=755; Europe n=497

Q: Relative Budget: Taken as an individual line item, is your overall security (cyber and electronic) budget increasing, decreasing or staying the same as a percentage of your total ICT budget?



Australia n=289; APAC n=755; Europe n=497

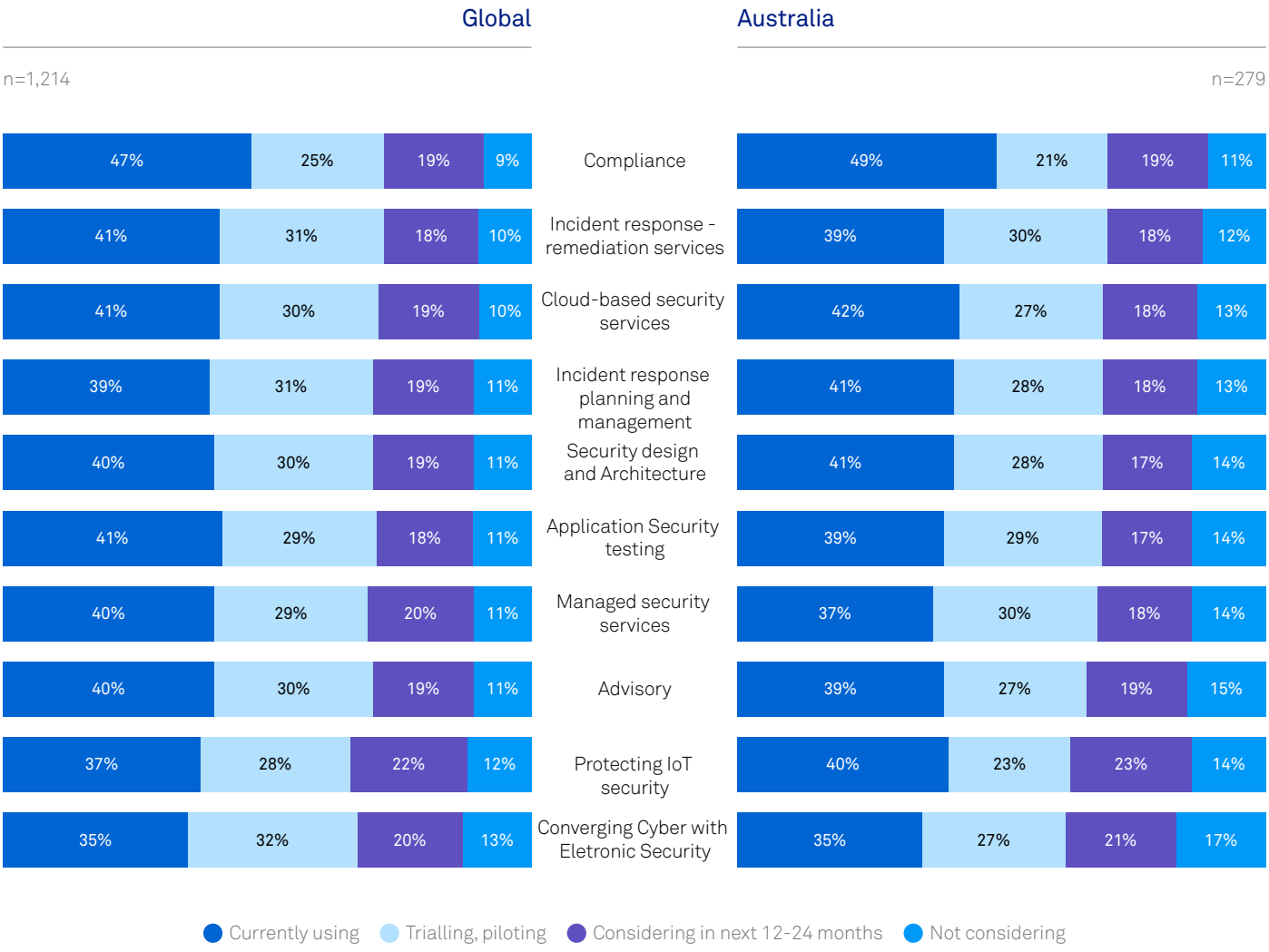
Australia APAC Europe

Spending Priorities

In terms of security initiatives, compliance is the single largest implementation priority in Australia, Asia Pacific and Europe. This focus on compliance reflects many new laws coming into place in 2018 across all regions. Incidence Response (IR) remediation services, followed by cloud-based security services, were at the most advanced stages of implementation into 2018. APAC respondents also tended to place a high priority on implementing application security testing, more so than European or Australian respondents.

Technologies being implemented

Q: What stage of implementation are you at with the following security service initiatives?



Technologies being trialled or considered

In terms of technology being trialled now or under consideration in the next one to two years, next generation endpoint security ranked the highest among respondents at 60 percent, followed by new capabilities to manage the convergence of cyber and electronic security at 59 percent; and application testing at 57 percent. In Australia, there was also a strong interest in user and entity behaviour analytics (UEBA) and CASB solutions. This is consistent with last year's results.

Emerging Technologies Being Trialed Now or Under Consideration

Australia Results	
Next–Gen Endpoint Security	**60%**
Convergence of Cyber and Electronic Security	**60%**
Application Testing	**57%**

APAC Results	
Next–Gen Endpoint Security	**61%**
Convergence of Cyber and Electronic Security	**59%**
Threat Hunting	**58%**

European Results	
Convergence of Cyber and Electronic Security	**58%**
UEBA	**57%**
Next–Gen Endpoint Security	**56%**

Australia n=279, APAC n=739, Europe n=475

APAC

APAC respondents also registered a strong interest in user and entity behaviour analytics (UEBA) at 57 percent; followed by threat intelligence platforms, DevOps for Security IoT Security and Application tied at 56 percent. The lowest ranked priority was cyber preparedness with a score of 48 percent. All other emerging technologies received a score of 50 percent or higher underscoring their perceived importance.

EUROPE

European respondents also registered a strong interest in DevOps for security, and security for IoT, tied at 55 percent. The lowest ranking priority was threat intelligence platforms with a score of 49 percent, with all other emerging technologies as a category receiving a score of 50 percent or higher.

Outlook

Organisational spending on security services will continue into 2018. Cyber and electronic security is converging which is also driving new requirements into emerging technologies such as next-gen endpoint security. Endpoint security, for its part, will morph into other areas such as CCTV, building management and automation systems. One explanation for this is the need to protect IoT devices from common threats such as DDoS and ransomware.

In terms of current projects, compliance spending will continue to be a priority for Australian, European and APAC organisations. This too is driving other requirements such as incident remediation, cloud-based services, advisory services, security and design testing. The rise of UEBA in Australia and APAC is indicative of businesses using more analytics and automation to understand normal activity before raising alerts when deviations from users' normal patterns pose heightened risk. This can be for example, an alert to an employee leaving the company, to users showing dangerous activity online. Cyber awareness and training will be important, and security managers will also become dependent on other tools to better detect and respond to potential threats from inside and outside the company.

Recommendations

Interoperability and integration

As spending in security increases, businesses should be looking for tighter integration of vendor platforms. A recent report from Cisco found that 55 percent of businesses used more than five security vendors and 65 percent used more than five products.[47] Multi-vendor solutions will be the norm for most, but ensuring systems are compatible is important as is increasing the number of external threat feeds. This multi-vendor approach can bring more context to events and, as a result, help businesses be more targeted and effective with incident response.

Data classification and loss prevention

Businesses should also look to invest in classification and loss prevention systems as these systems can help prevent data from leaving a private network to an unauthorised destination, such as the public Internet, personal email addresses or USB storage devices. There can be additional policies tagged to the data once a breach has been detected and the policy can automatically apply the appropriate response when an incident occurs (e.g. block, report, quarantine, notify, warn, etc.). These systems will also be more important for compliance purposes.

Security audits

Security should be reviewed continuously and audits are a strong starting point. This includes IT vulnerability scans, penetration testing of applications, operating system, access controls and determining the location and value of data. This is a strong starting point to determine current security posture and next steps.

Involve lines of business in the plan

A security plan should also support many lines of business, depending on the nature and extent of a breach. For example, the theft of intellectual property from an employee leaving the organisation should involve human resources, while one impacting the brand, reputation and share price should actively involve public relations, investor relations and marketing, among other departments. Similarly, facilities managers and operations will need to be involved in electronic breaches. As the C-Level becomes more involved in security, it is imperative for businesses to be working together.

[47] Cisco 2017. Annual Cybersecurity Report. Page 63

In summary

As cyber and electronic converge and the industry prepares for a greater range and variety of attacks, organisations should start with the basics. This includes ascertaining the location and value of data; who has access to the data; and the overall level of protection. There should also be clear ownership of this data. From here, data classification can help an organisation understand the value, while data loss prevention can help ensure the data is not lost. Likewise, IAM is among the tools available that can govern which employees have access to what, and from where. The location of data, for example, will be particularly important for compliance purposes.

There are also some general best practices business should consider.

Multi-layered defences

With the number of threats that can penetrate IT systems, this approach, also known as defence in depth, relies on multiple layers of security controls throughout ICT and now electronic security environments. Its intent is to provide redundancy in the event that one point fails or is exploited. This could be using web security gateways to block malicious code being downloaded. Whitelisting should also be considered for keeping unknown executable files from running. Deploying advanced endpoint protection on laptops, mobiles and servers is also recommended. In addition, continue to run and update anti-malware, managed firewalls and VPNs to improve security across corporate networks. Passwords should also be alphanumeric, entirely unique and memorable.

Architecture reviews

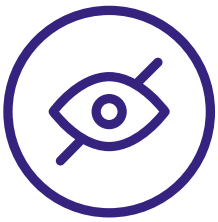
Architectural reviews should be a constant whether for planning for a system refresh or considering ways to interconnect physical with electronic. This should also include system and vulnerability scans, penetration testing and other tests to understand environments, discover vulnerabilities and prioritise fixes.

Incident response

With businesses moving to a presumption of breach approach, it is critical to have a plan in place before, during and after an attack. This plan should be documented and rehearsed. Depending on the type of attack (e.g. theft of property by an employee, loss of customer data through an external attack etc.), organisations should have notification and escalation procedures. There should be designated department heads who may need to be involved (e.g. investor, corporate communications, legal, finance, compliance officers, etc.) This is important for compliance as well as good governance.

Education and training

Employee outreach will be an effective way to reduce the number of potential attacks. Employees are your greatest asset, but can also be the weakest link into your corporate network. Helping employees know what to look for, advising them on ways to prevent themselves being targets, and establishing good practices (e.g. setting unique passwords, not writing passwords on devices) can go a long way. Security is also a balance between managing risks and end-user experience. Having a feedback loop or a way to engage the end-user community is important for building trust and mutual understanding.



Future of security and IT

With many new regulations coming into law in 2018, the level of C-Level involvement in matter of security will increase. Organisations should prepare for a future of security – cyber and electronic – being in the hands of multiple stakeholders. Businesses should also be working with peers in their industry, as well as government, on more intelligence sharing on security threats.

Acknowledgements

Telstra contributions

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

About Telstra Security Services

Telstra's Managed Security Services can help you navigate the security landscape and manage risk across your cyber, electronic & IoT ecosystems. Underpinned by our powerful open source Managed Security Service platform, our solutions leverage our purpose built Security Operations Centres (SOCs) in Sydney and Melbourne. These SOCs provide the visibility, expertise, intelligence and tools our customers need to secure their business in an evolving threat environment.

Cyber Security services

Our cyber security services are highly flexible and new services are regularly added.

Our current capability include:

Security Monitoring

Our Security Monitoring service feeds event data from a variety of sources across your on-premises, IoT and cloud infrastructure. With 24/7 visibility and actionable reports, you can gain deeper understanding of your risk status and clearer resolution paths for mitigation.

Incident Response

Receive priority access to Telstra's highly-skilled Computer Emergency Response Team (CERT) who respond quickly to any suspected incident, such as unauthorised access to your systems, electronic data loss or theft, viruses, suspicious network activity and ransomware attacks.

Electronic Security

Organisations in every sector have security and monitoring challenges, but we understand that your business has unique needs. We have always provided network services to the electronic security industry, and now we've partnered with leading security companies to combine their expertise with our high performance network. Together, we provide a suite of electronic security solutions that go beyond safety and loss prevention, offering reliable, convenient and effective ways to protect your business and enhance business outcomes – now and into the future.

Consulting Services

Our team of security consultants can help you align your security and risk environment with your business drivers, innovate with industry leading protection, navigate complex security challenges, or take a holistic approach to cyber security risk management. Our capabilities include security consulting, security compliance, incident preparedness, intelligence and analytics, network and cloud security, end-point, mobile and application protection, as well as managed security services.

For More Information

We can assist your organisation to manage risk and meet your security requirements.
For more information about our services, contact your Telstra Account Executive or visit *telstra.com/enterprisesecurity*

Thank you to our Partners for their contributions to this report

Akamai FASTER FORWARD · Carbon Black. · Check Point SOFTWARE TECHNOLOGIES LTD ONE STEP AHEAD · CISCO · CITRIX · COFENSE · CROWDSTRIKE · ERICSSON · f5 · FireEye · FIRSTWAVE CLOUD SECURITY TECHNOLOGY · FORTINET · Gorilla · IBM · JUNIPER NETWORKS · McAfee Together is power. · paloalto NETWORKS · Qualys. · Symantec. · TeleSign · ZIMPERIUM MOBILE THREAT DEFENSE · zscaler

Contact your Telstra Account Executive
Or call 1300 835 787

Visit telstra.com/enterprisesecurity