Telstra Security Report 2019

Foreword

As our lives become more and more connected, cyber security has emerged as a top-of-mind issue for business leaders and governments right across the globe.

With cybercrime increasing, organisations of all kinds are regularly experiencing breaches that interrupt operations, compromise customer privacy and in the very worst cases irretrievably damage reputations or steal your intellectual property.

The introduction of new compliance regulations and growing public interest in data privacy, means C-level participation in cyber security management is now critical for all businesses.

Organisations must better understand the dynamic and changing world of cyber security, to help reduce the occurance and impact of cyber-attacks.

The Telstra Security Report 2019 reviews the current security landscape and how security professionals are managing risks around the world. Interviews with around 1,300 professionals across 13 countries, that have decision making responsibilities for cyber security, highlights the emerging technologies that will help detect and counter the impact of current and new security threats in the year ahead.

Encouragingly, this year's report shows the majority of organisations are working on being better prepared for when, not if, an attack occurs, but being able to detect and respond to incidents in a timely manner is still the number one challenge for security professionals for 2019.

The report also found that a majority of respondents in countries with data privacy legislation have been fined for data breaches indicating companies still have a way to go to understand and comply with local legislation.

What is clear is that security has moved far beyond the maintenance of firewalls and is now a whole-of-business concern for C-level executives and boards.

We hope this report is a useful tool to help you better think through your organisation's cyber security risk and make better decisions about your organisation's approach to cyber security.

Michael Ebeid AM
Group Executive
Telstra Enterprise

"My team and I once again welcome the publication of Telstra's fourth annual Security Report. The insights gleaned from the global security community captured in this report helps us to test our thinking and challenge our approach to protecting the privacy and security of our customers, Telstra and the services we provide. I hope you find the insights provided in the report of value and help you better protect your business and, most importantly, customers."

Berin Lautenbach
Chief Information Security Officer, Asia Pacific
Telstra Corporation Limited

Contents

Executive Summary

Over the last 12 months we've seen a material shift in the priorities of both defenders and attackers. Some aspects of security, like malware, are better-known. However, other emerging security technologies, though not as well understood, are high on the list of considerations to improve cyber defences. For example, 93 per cent of the global respondents are considering, trialling or have implemented next gen endpoint detection and response. Organisations are also increasing both security awareness and preparation programs. This is perhaps in recognition of security being a complex topic and the importance of having a plan before, during and after a potential attack. This is likely to encompass measures to mitigate risk to improving response and recovery objectives.

Media reporting of state-sponsored cyber-attacks continues to grow.[1] Shifts in global – and regional – politics and economics can play an influential part in changing the security landscape. A recent report from FireEye notes there is an increased level of activity among nation-state actors and predicts the development of more offensive capabilities. FireEye reports that rules of engagement are virtually non-existent and, as a result, many businesses are vulnerable.[2] A report from Cylance identified that the financial sector was 'top of the hit list for attackers spanning the full range of sophistication and capability'.[3]

Last year we discussed the threat of ransomware in detail and we covered its creation, distribution, and revenue models. While ransomware is still pervasive and profitable for cyber criminals, most potential victims have adopted policies and safeguards against such attacks. Many adversaries are now turning to cryptocurrency related products, which can often be bolted onto traditional malware and easily activated. The rise in popularity of these currencies makes this market attractive for crypto mining and cryptojacking.

Other types of attacks have included formjacking, which is the injection of malicious JavaScript code that is written to steal credit card data and other information. Typically, this sort of attack occurs on untrustworthy e-commerce websites.[4] Companies are also increasing their security defence spending in absolute and relative terms. A report from Oliver Wyman, (which was also quoted in the Harvard Business Review)[5], predicts that spending will approach US$1 trillion annually on a global basis by 2022.[6]

Breaches, defined as incidents that result in the confirmed disclosure of sensitive data to an unauthorised party, are on the rise. Our survey shows nearly two thirds of respondents have fallen victim to a security breach, showing these events are happening more frequently and continue to be more varied. 2018 saw the largest known Distributed Denial of Service (DDoS) attack recorded, which peaked at 1.35 Tbps.[7] Within a week of this attack, an undisclosed US service provider experienced an attack which peaked at 1.7 Tbps.[8]

In 2018, Marriott International experienced a large-scale security breach, with up to 383 million customers impacted (current estimate).[9] The Singapore Health System experienced a breach where 1.5 million patient records were compromised.[10] Cathay Pacific also experienced a major breach where personal data relating to 9.4 million passengers was compromised.[11]

This year, an interesting trend is emerging where defenders are striking back. Awareness and understanding of the strategic importance of security is improving. In all regions we surveyed this year, businesses reported investing more resources in security awareness and training, more so than what we saw in our 2018 Security Report. This includes delivering formal education focusing on information management and incident response. As security moves from

[1] Mullen, J. (2019, February 20). Chinese hackers are ramping up attacks on US companies. CNN. Retrieved from https://edition.cnn.com/2019/02/20/tech/crowdstrike-china-hackers-us/index.html
[2] FireEye (2019). Facing Forward Cyber Security in 2019 and Beyond. Retrieved from https://content.fireeye.com/predictions/rpt-security-predictions-2019
[3] Financial Threat Trends - Cylance research for Telstra Security Report 2019
[4] Symantec Security Response (2018, September 25). Formjacking: Major Increase in Attacks on Online Retailers. Symantec Blog. Retrieved from https://www.symantec.com/blogs/threat-intelligence/formjacking-attacks-retailers
[5] Harvard Business Review (2018, September 14). How a Cyber Attack Could Cause the Next Financial Crisis. Retrieved from https://hbr.org/2018/09/how-a-cyber-attack-could-cause-the-next-financial-crisis
[6] DeBrusk, C. and Mee, P. (2018). Cyber Risks that Hide in Plain Sight. Oliver Wyman. Retrieved from https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2018/june/Cyber-Risks-That-Hide-In-Plain-Sight.pdf
[7] Newman, L. (2018, March 1). GitHub Survived the Biggest DDoS Attack Recoded. Retrieved from: https://www.wired.com/story/github-ddos-memcached/
[8] Morale, C. (2018, March 5). NETSCOUT Arbor Confirms 1.7 Tbps DDoS Attack; The Terabit Attack Era Is Upon Us. NETSCOUT. Retrieved from https://asert.arbornetworks.com/netscout-arbor-confirms-1-7-tbps-ddos-attack-terabit-attack-era-upon-us/
[9] Marriot International (2018, January 4). Marriott Provides Update on Starwood Database Security Incident. Retrieved from https://marriott.gcs-web.com/news-releases/news-release-details/marriott-provides-update-starwood-database-security-incident
[10] Kwang K. (2018, July 20). Singapore health system hit by 'most serious breach of personal data' in cyberattack; PM Lee's data targeted. Channel NewsAsia. Retrieved from https://www.channelnewsasia.com/news/singapore/singhealth-health-system-hit-serious-cyberattack-pm-lee-target-10548318
[11] Cook, J. (2018, October 24). Cathay Pacific says data of 9.4 million passengers stolen in hack. The Telegraph. Retrieved from https://www.telegraph.co.uk/technology/2018/10/24/cathay-pacific-says-data-94-million-passengers-stolen-hack/

being an IT issue to one that is company-wide with every employee playing a role, the gap between adversaries and defenders has narrowed. When attacks do occur, response and remediation times are improving.

This year, all respondents surveyed identified that within their role they are responsible for both cyber and electronic security within their organisation. There are also early signs of increased C-level participation. This year we saw more focus from businesses on protecting customer privacy, with 46 per cent of global respondents and 38 per cent of Australian respondents reporting an increased concern. Additionally, about one third of businesses told us that because of new regulations, the frequency of C-level and senior management meetings on security in Australia, APAC, and Europe is increasing. Furthermore, there are improvements in the observation of local and regional compliance measures compared to last year's results. Many established security frameworks, such as ISO/IEC and COBIT, plus resources like CERT, continue to be utilised.

Our research found that getting security right from the outset is a 'critical success factor for large IT transformation projects'. The overall linkage between security and customer experience is just as important to survey respondents year on year. The number one challenge for security professionals for 2019 remains the ability to detect and effectively respond to incidents in a timely way, both in the cyber and electronic domains. This is closely followed by managing the impact of new technologies such as software defined networks and IoT, which is consistent with our 2018 findings.

This year there is considerable interest in emerging technologies. In Australia, this includes the integration of video analytics and telemetry into IT security. In other regions, there is a focus on the use of artificial intelligence (AI) to improve cyber defences, and new sandboxing techniques to stem the flow of attacks by allowing them to run in enclosed environments. There is a focus on extending a consistent security posture to the supply chain in recognition of adversaries targeting partners and suppliers – with potentially weaker defences – as a backdoor to a primary target.

We called 2018 the "Year of Compliance" due to the number of regulations that came into effect during that calendar year. This contributed to one of the most surprising findings in this year's survey: more than half of the respondents surveyed believe their organisation has received fines for being in breach of legislation enacted in the past two years. This reminds us that while the security profession has made many advances in just 12 months, we can't be complacent and need to continue striving to meet the challenges ahead.

Methodology

Our 2019 Telstra Security Report provides research-based insights into the current security landscape to support you in mitigating and managing security risk. Whether you're a senior security professional in a large multinational organisation, or an IT Manager in a 50 person domestic business, this report is designed to assist you in understanding current security trends and to frame strategies for preparedness and incident response.

We engaged research and analyst firm GlobalData to interview professionals responsible for making IT security decisions within their organisation to obtain several key insights on a range of security topics. Our report also draws on the analysis of security information and data gathered from Telstra's infrastructure and security solutions, plus that of over 15 third-party providers, including our security partners.

With continued convergence within the security field, this year we once again examined cyber security and have expanded our research even further into electronic security. For the purposes 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.

Sample Size and Geography

GlobalData interviewed 1,298 security professionals across 13 countries during November and December 2018. Sixty one per cent of the surveys were conducted in Asia-Pacific (APAC) and 39 per cent in Europe. Within APAC, 40 per cent of respondents were from Australia, with the remaining 60 per cent from New Zealand, Singapore, Hong Kong, Indonesia, Philippines, and Taiwan. European respondents were from Germany, France, United Kingdom, Belgium, Netherlands, and Luxembourg. This year, the UK was the largest sample size from Europe, representing 30 per cent of all European respondents.

Australia	320	25%
New Zealand	68	5%
Hong Kong	72	6%
Singapore	76	6%
United Kingdom	154	12%
Germany	129	10%
France	129	10%
Taiwan	86	7%
Philippines	82	6%
Indonesia	91	7%
BENELUX Region (Belgium, Netherlands, and Luxembourg)	91	7%
Total	1298	100%

Business Types

Respondents identified themselves as working in businesses of all sizes; from 50 employees in a single country, to as large as 5,000 plus employees spanning the globe. They work across 15 industry verticals including broadcast and media; banking, financial services and insurance (BFSI); mining and resources, and the government and public sector. The government and public sector were also split by local, state, and federal jurisdictions.

This year, 47 per cent of all respondents were from organisations that reported 500 or more employees. In Australia, 49 per cent represented businesses with fewer than 500 employees, up from 46 per cent last year; and 51 per cent came from organisations with more than 500 employees, versus 54 per cent last year.

Respondents came from a variety of business types including local organisations, public sector and government entities, and multinational corporations (MNCs). Nearly 40 per cent of all respondents came from private companies with no overseas offices. There were 577 MNCs surveyed, which represented 44 per cent of the total. Within the MNC segment, 38 per cent were APAC-headquartered (42 per cent last year); and 62 per cent were headquartered from outside APAC (58 per cent last year).

Position Titles

C-suite executives including CEO, CFO, CIO, COO, CTO, CISO and CSO accounted for 20 per cent of the global respondents, and 21 per cent in Australia - consistent with our 2018 Security Report. The remainder were in IT and security management roles. The single biggest role represented in the survey was the IT manager, at 36 per cent of the respondents globally, and 27 per cent in Australia. This year, all 1,298 respondents reported knowing their organisation's annual security budget and having either some influence or complete control over the security investment.

Location of Respondents

1,298 Respondents

13 Countries

15 Industries

- **Europe**
  France, Germany, United Kingdom, Belgium, Luxembourg, Netherlands
- **Asia Pacific**
  Australia, New Zealand, Singapore, Hong Kong, Indonesia, Philippines, Taiwan
- **Australia**

The Broadening Security Landscape

In our 2018 Security Report, we found that security professionals were in the process of extending their remit from cyber security into electronic security, with over 95 per cent of respondents indicating they were responsible for both domains. This year, 100 per cent of our respondents identified that within their role they were responsible for both cyber and electronic security within their organisation.

For the purposes 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.

Q: To cyber security decision makers: Do you have responsibility for decisions made for overall electronic security spend in your organisation?

Global

n=1,298

- **26%** Yes, I make the final decision in my organisation
- **41%** Yes, I am one of the final decision makers in my organisation
- **32%** Yes, I contribute significantly to the final decision
- **0%** No, I am not involved

Australia

n=320

- **19%** Yes, I make the final decision in my organisation
- **41%** Yes, I am one of the final decision makers in my organisation
- **39%** Yes, I contribute significantly to the final decision
- **0%** No, I am not involved

Convergence of Information Technology and Operational Technology

Underpinning the broadening security landscape is the convergence of information technology (IT), (including systems for data-centric computing); with operational technology (OT), (including systems used to monitor events, devices, and processes). This includes industrial control systems and supervisory control and data acquisition (SCADA) systems, which are embedded in critical infrastructure such as process control. Some of the major industries using these systems include manufacturing, energy, power grids, mining, and utilities. Some businesses are ingesting data sets from both IT and OT systems for better visibility and context. Over time as these systems continue to converge, there will be many new use cases in areas such as building automation systems, video surveillance, heating, ventilation, and air conditioning (HVAC) systems, smart lighting, energy management, and improvements in building health and safety systems. Smart buildings, which thrive on the interconnectedness of IT and OT systems, will also need to be secured.

With the prospect of 29 billion connected devices by 2022, there will also be a range of additional components, such as sensors, connected to the internet which will help to drive transformation in a number of major industries.[12]

As a natural progression from smart buildings, we will see even more use cases across smart cities (e.g. metering and telemetry), healthcare (e.g. patient monitoring, remote diagnosis, and real-time imaging), through to transportation and logistics (e.g. autonomous vehicles, fleet and asset management). Connecting OT to the internet is increasingly important for transforming the manufacturing sector with connected factories. This speaks to the integration of cyber and physical systems, sector-wide automation, and real time data exchange. Furthermore, many security use cases are emerging in areas such as predictive maintenance. Other possibilities include the wider use of artificial intelligence (AI) for human-robotic interaction (HRI) models to improve productivity and operational efficiencies in factory automation.

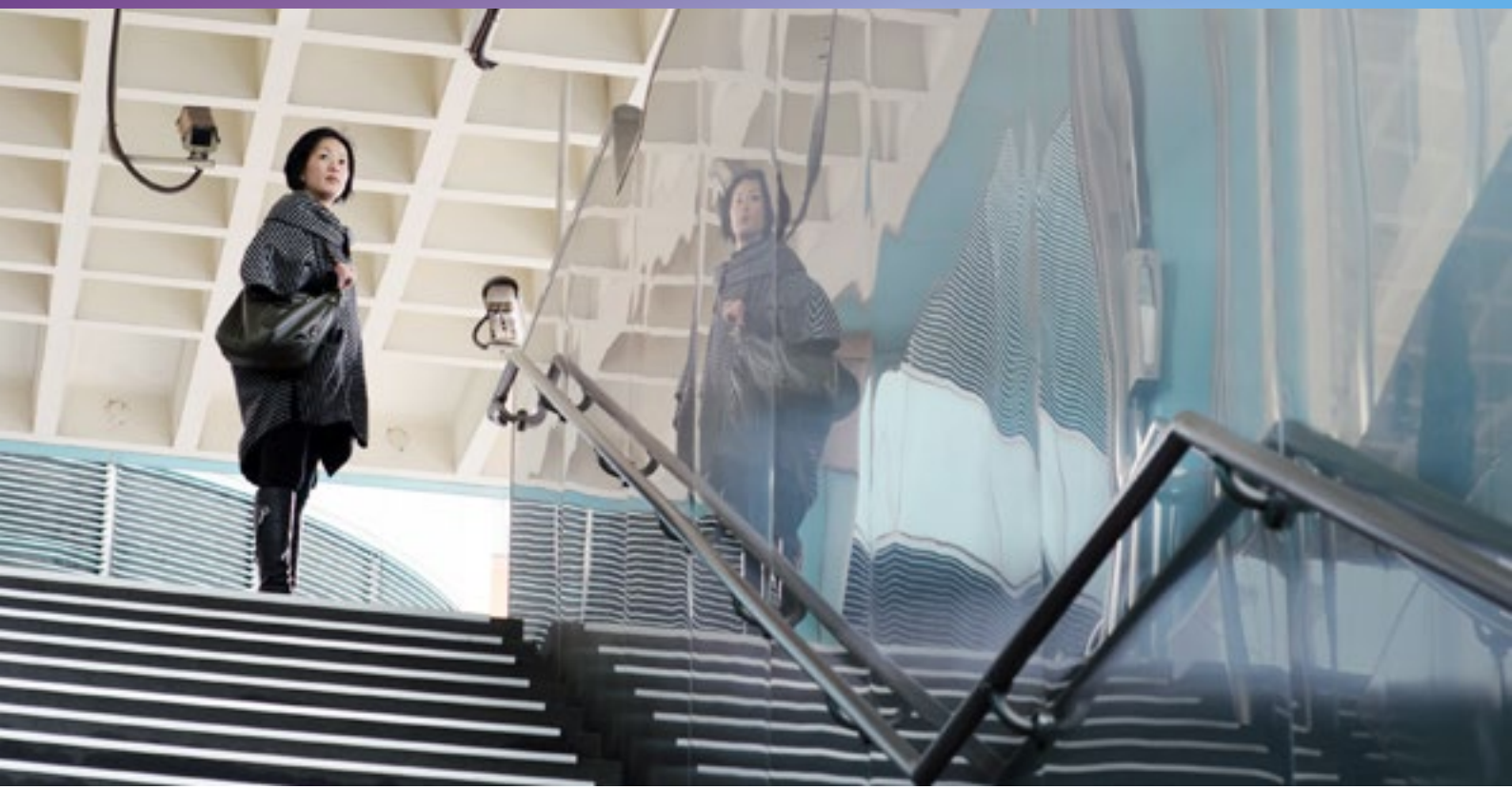
Insecure Systems

While there are many benefits from the convergence and connectivity of OT with IT systems, security risks need to be considered and managed. The integration of cyber and physical systems is exposing new attack vectors for hackers. While traditional IT systems can often have strong security features, hackers may look at softer targets within areas of OT to break into an IT system. This could range from minor security incidents to a mega-breach. In 2017, the IT system of a US casino was breached through a connected fish tank and sensitive data was infiltrated.[13] In our 2018 Security Report, we discussed the breach in an HVAC system that led to the loss of 40 million credit cards.[14]

More recently, researchers at the Cyber Security Research Centre at the Ben-Gurion University in Israel have shown that event air-gapped networks – physically isolated networks – can be also be breached.[15] Through the use of light, frequencies and electromagnetic signals, researchers have been able to pull small data streams from offline computers to nearby smartphones and even drones.[16] Other projects gave targeted video surveillance with infrared signals[17] to show that, through exfiltration and infiltration, hackers have been able to set up bi-directional communications with internal networks. In this case, the network was separated from the internet without any physical or logical connections.[18] Among the experiments, sensitive data such as passwords, PIN codes and encryption keys were 'modulated, encoded, and transmitted over the IR signals'.[19]

A study by Qualys, referenced in the Cisco 2018 Annual Cybersecurity Report, found that 83 per cent of IoT devices scanned (e.g. HVACs, door locks, fire alarms), had critical vulnerabilities.[20] One explanation for this was that the devices could be updated. Further, some devices require the support of an external vendor and were not up-to-date. In many cases, there were no clear indications of who was responsible for securing IoT connected devices.[21] As more devices and 'things' connect to the internet, managing potential backdoor breaches will become more important, and more challenging.

[12] Ericsson (2018). Internet of Things Forecast. Retrieved from *https://www.ericsson.com/en/mobility-report/internet-of-things-forecast*
[13] Mathews, L. (2017, July 27). Criminals Hacked A Fish Tank To Steal Data From A Casino. Retrieved from *https://www.forbes.com/sites/leemathews/2017/07/27/criminals-hacked-a-fish-tank-to-steal-data-from-a-casino/#1761e77e32b9*
[14] Vijayan, J. (2014, February 7). Target attack shows danger of remotely accessible HVAC systems. Retrieved from *https://www.computerworld.com/article/2487452/cybercrime-hacking/target-attack-shows-danger-of-remotely-accessible-hvac-systems.html*
[15] Greenberg, A. (2018, February 7). Mind the Gap: This Researcher Steals Data With Noise, Light, and Magnets. Wired. Retrieved from: *https://www.wired.com/story/air-gap-researcher-mordechai-guri/*
[16] Greenberg, A. (2018, February 7). Mind the Gap: This Researcher Steals Data With Noise, Light, and Magnets. Retrieved from: *https://www.wired.com/story/air-gap-researcher-mordechai-guri/*
[17] Mordechai G, Bykhovsky D, and Elovici Y (2018, September). aIR-Jumper: Covert Air-Gap Exfiltration/Infiltration via Security Cameras & Infrared (IR). Retrieved from: *https://arxiv.org/abs/1709.05742*
[18] Ibid.
[19] Ibid.
[20] Cisco (2018). Cisco 2018 Annual Cybersecurity Report. Page 41
[21] Ibid.



Operational Technology Ransomware

We've previously reported on ransomware as a pervasive type of malware in the IT context. This year's research indicates that ransomware continues to surface in the electronic security domain and is a growing problem.[22] This includes building automation systems or industrial control systems powering vehicles, industrial processes, production lines, and public systems such as water and power.

Ransomware can function by locking an underlying boot system, thus rendering connected devices or sensors inoperable until they are restored, either by a back-up system, if available, removal of the malware through technical means, or payment of a ransom in the hope it will restore operations. In 2017, 123 of the 187 CCTV cameras that monitored public areas in Washington DC were attacked with ransomware eight days before the inauguration of President Donald Trump. The attack hit the storage and rendered them inoperable for three days.[23] Beyond the payment of the ransom, businesses can face downtime and related repercussions in operations such as disruptions to the supply chain. They may incur financial losses, damage to property or physical assets. It can even impact health and safety. In the US, hacking fears prompted the FDA to recall 500,000 pacemakers.[24]

IoT Distributed Denial of Service and Botnet Attacks

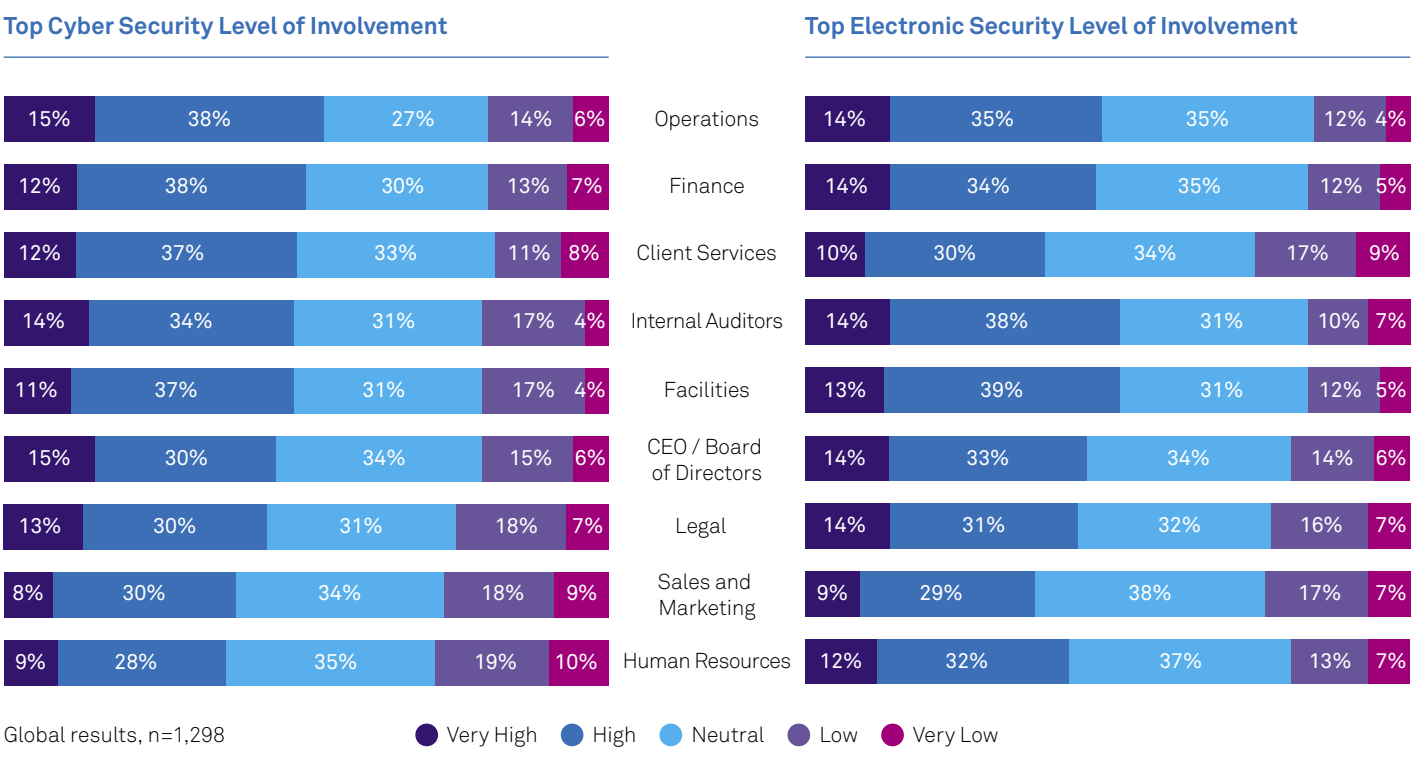
Distributed Denial of Service (DDoS) has been a leading attack over the years. With the convergence of cyber and electronic security, an adversary can gain access to connected devices, such as an IP surveillance camera, through simple-to-crack default passwords, and exploit access to thousands of other units with minimal effort. Mirai was an example of one of the largest DDoS attacks of this kind, peaking at 990 Gbps[25], and has led to other strains, such as Brickerbot, Hajime, and Persai.[26] Commonly, these malware strains scan for open Telnet or Secure Shell (SSH) ports, discover any IoT devices connected to them, and perform brute-force attacks using common default usernames and passwords, before sending the malware payload. The implication is that adversaries could install malware on the devices, program them for future use or enlist them in a global army of bots with minimal investment.

[22] Paul, L. Gibbons (2018, June 27). In Search of Industrial Cybersecurity Experts. Retrieved from *https://www.automationworld.com/article/technologies/security/search-industrial-cybersecurity-experts*
[23] Wang, W. (2017, February 3). Two Arrested for Hacking Washington CCTV Cameras Before Trump Inauguration. The Hacker News. Retrieved from *https://thehackernews.com/2017/02/cctv-camera-hacking.html*
[24] Hern, A. (2017, August 31). Hacking risk leads to recall of 500,000 pacemakers due to patient death fears. The Guardian. Retrieved from: *https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update*
[25] Holmes, D. (2016, October 27). Making Sense of the Last Month of DDoS Attacks. F5. Retrieved from *https://f5.com/Portals/1/Cache/Pdfs/5041/making-sense-of-the-last-month-of-ddos-attacks.pdf*
[26] Cisco (2018). Cisco 2018 Annual Cybersecurity Report.

Cyber and Electronic Security Accountability, Escalation and Reporting

We considered the different departments involved in electronic and cyber security and who is ultimately responsible in the event of an incident. This year's results show the CEO is one of the top three accountable people in the organisation both in Australia and globally for a 'very high' level of involvement. Other important stakeholders include: internal auditors, typically departments that are responsible for compliance, the finance department as well as operations. This is likely to reflect new regulations, such as the General Data Protection Regulation (GDPR) in the European Union, and willingness by regulators to fine companies who do not meet their security obligations. With fines recently applied in a case that involved Uber.[27] We also asked the question: which of the following individuals or departments are notified in the event of a security breach (cyber and electronic). In the Australian, APAC, European and global responses, the CIO/IT Department are notified first followed by the CEO. These results are consistent with our 2018 findings in all but one case.[28] From this point, the individuals or departments notified show slight differences in the ranking of perceived executive responsibility. Security professionals are essentially 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? (Global results)



[27] Ashford, W. (2018, September 27). Uber fined $148m for data breach cover-up. Retrieved from https://www.computerweekly.com/news/252449446/Uber-fined-148m-for-data-breach-cover-up

[28] In our 2018 Security Report, the European respondents would notify the CISO next after the IT department for a cyber breach.

This year's research further reflects the findings of our 2018 Security Report, as the IT department continues to be seen as the main business unit involved in security initiatives for both cyber and electronic security. Our research also indicates that IT plays the role of an orchestrator in understanding the importance of cyber security to carry out their own functions effectively, whilst also working with multiple lines of business. In the event of a security breach, our research shows a consistency in attribution of responsibility to the C-level.

A most noticeable change from our 2018 Security Report is the movement in our global results of the views of a CEO's responsibility over IT security from fourth place to third place. These executives are pushing the employees involved in the incident down in the responsibility ranking in both the cyber and electronic security domains.

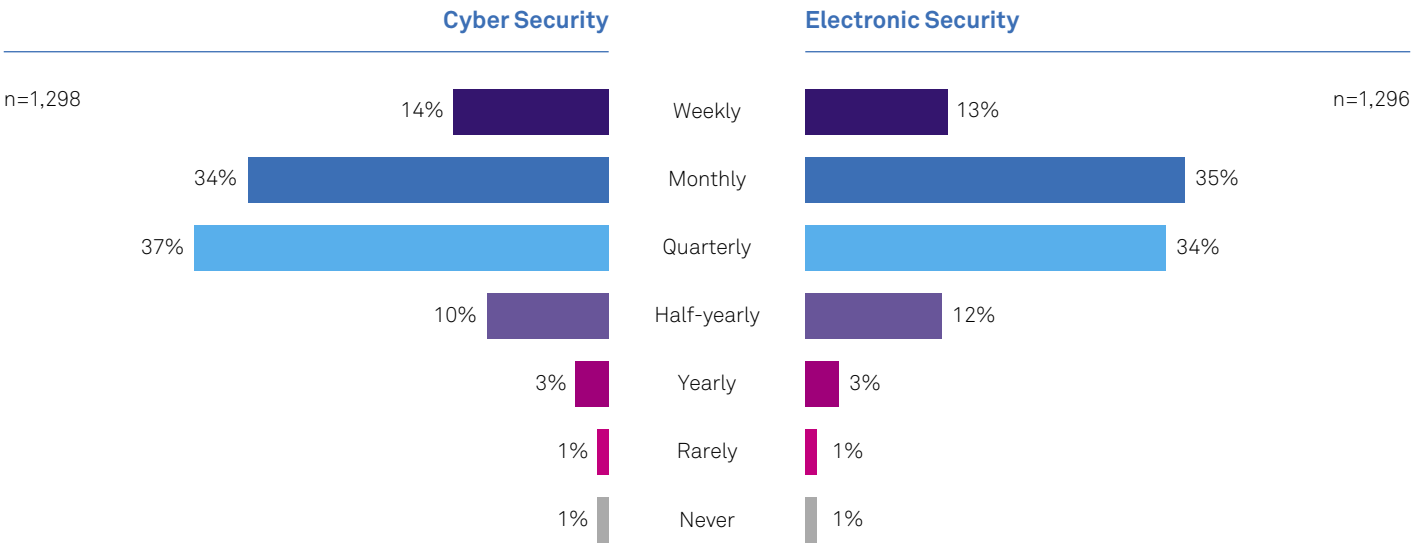
Q: In the event of an incident, who is ultimately held responsible?

Ultimately held responsible for a breach (top 3 nominated) – Global			
Cyber		**Electronic**	
IT Department	**47%**	IT Department	**41%**
CIO	**27%**	CIO	**25%**
CEO	**21%**	CEO	**21%**
Employees involved	**21%**		
Global results, n=1,298			

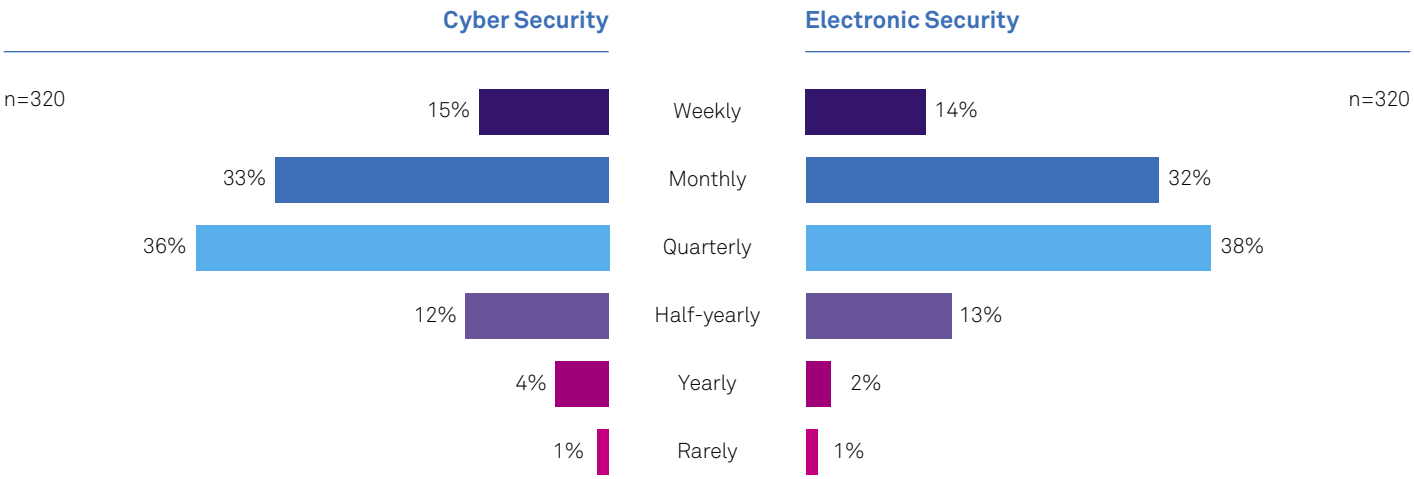
Ultimately held responsible for a breach (top 3 nominated) – Australia			
Cyber		**Electronic**	
IT Department	**48%**	IT Department	**37%**
CIO	**30%**	CIO	**24%**
CEO	**21%**	CEO	**18%**
Employees involved	**21%**		
Australian results, n=320			

C-level executives continue to take a more active role in understanding the importance of cyber security initiatives, increasing their involvement in and taking responsibility for security incidents when they occur. Our research also identified that the level of reporting seems to be increasing for both domains. As convergence continues between cyber and electronic security, briefings to senior management are likely to be more integrated. Some companies may choose to address security and associated topics, such as risk management, incident response and security policy for cyber and electronic as one topic with all the key stakeholders in the room.

Q: How frequently do you brief board and senior management on cyber/electronic security risk and mitigation? (Global results)



Q: How frequently do you brief board and senior management on cyber/electronic security risk and mitigation? (Australian results)



Outlook

Traditionally, IT and OT were managed in different parts of an organisation. OT was not connected to the internet and did not require much support from other departments. Industrial IoT delivers new efficiencies created through connectivity and integration of these systems. New insights from data is forcing businesses down a path where security has to keep up with the times. Security policy, as well as the underlying architecture, will support both cyber and electronic security. Given this reality, the areas will no longer be considered separate topics or treated in isolation. Over 70 per cent of all global respondents have, or plan to have, a combined budget for cyber and electronic security. Both domains will likely have a shared responsibility across multiple lines of business. The frequency of security reporting will likely increase.

Security budgets are increasing too. Eighty four per cent of Australian respondents report that budgets for overall security (cyber and electronic) will increase within the next 12 to 24 months, similar to the 79 per cent of the APAC and European respondents (down slightly from 84 per cent last year). Security budgets, when measured as a line item relative to the overall information and communications technology (ICT) budget, are expected to continue to increase for 60 per cent of Australian businesses, 64 per cent of APAC, and 70 per cent of European businesses surveyed. For the second consecutive year, our respondents indicated that security budgets continue to increase in absolute and relative terms.

The trend in converged and increased security spending could be explained due to common threat vectors, such as ransomware and botnet attacks. Often adversaries will target electronic systems or components which are less secure as a backdoor to ICT systems which are more secure. Many devices connected to the internet have critical vulnerabilities, as reported by Qualys.[29] Integrating the domains will be important for establishing areas of responsibilities in an organisation and holding external vendors to account. A continued imperative in 2019 will be addressing highly sophisticated attacks, such as the ability to launch an attack or infiltrate data through air-gap networks that are not connected to the internet.[30]

It is expected that the frequency of executive and board meetings to discuss security will continue to increase in 2019. These meetings will continue as a function of convergence and also in recognition of the many regulations coming into force. Thirty three per cent of Australian, and 36 per cent of global respondents indicated that these meetings are increasing in frequency due to recent regulatory and compliance requirements. We also expect to see the level of CEO involvement in cyber and electric security increase gradually in 2019. This appears to be in line with the market trajectory.

[29] Cisco (2018). Cisco 2018 Annual Cybersecurity Report. Page 41
[30] Mordechai G, Bykhovsky D, and Elovici Y (2018, September). aIR-Jumper: Covert Air-Gap Exfiltration/Infiltration via Security Cameras & Infrared (IR). Retrieved from: *https://arxiv.org/abs/1709.05742*

Recommendations

Coordinate Security Policy and Processes

As cyber and electronic security continue towards a path of convergence, it is important for organisations to have a common approach for both systems. This is in recognition of a broader threat landscape and the many challenges that go with it. As businesses look to consolidate security budgets for both areas, they should also look to integrate departments and merge units where it makes sense. Organisations with a holistic approach to security will be in a better position to strengthen security defences in areas like incident response. They should consider the impact of new technologies or security posture and enable the business to take advantage of new opportunities in a more secure way.

Consider new opportunities brought in because of IT and OT convergence

As cyber and physical systems continue down a path of convergence and integration, there are some businesses that have identified new use cases. This can include ingesting video feeds and location data into security information and event management (SIEM) platforms for better context and situational awareness. Other businesses have looked at multi-factor authentication (e.g. validating an employee has entered a building through building management solutions such as, facial recognition, before logging onto the corporate network). Other use cases include user and entity behaviour analytics. Security is foundational to the integration of IT and OT, and can also be an enabler of many new use cases.

Cyber Preparation and Awareness

Cyber security preparedness is built on technology, business processes and people. Getting the balance right is essential for building cyber resilience. The problem is that although employees can be a company's best asset, they can also be the greatest IT risk when it comes to security. Cyber criminals will often specifically target employees as an attack vector, based on their lack of knowledge for security best practices.[31]

There are other forms of insider threats. They range from a malicious insider intent on, for example, stealing corporate data or causing a company damage; to an employee who has been targeted by an external advisory such as a social engineering attack; to an accidental insider who might not adhere to basic precautions or due to IT systems or business processes, is unable to complete their job securely.

Our respondents identified the greatest risk to IT security is human error – often caused by inadequate business processes and employees not adequately understanding their organisations' security posture. This is the sentiment from the Australian, APAC, European and global results for consecutive years. This type of insider threat has the potential to cause harm to both an organisation's reputation, and its bottom line.

Q. Where do you think the greatest risk of IT security is most likely to come from within your organisation? (Insider Threats Only)

	Global	Australia
Accidental Insider	**24%**	**25%**
Targeted Insider	**12%**	**11%**
Malicious Insider	**11%**	**8%**
	n=1,298	n=320

Accidental and Targeted Insiders

The accidental insider is typically the benign employee who leaks data outside the company or exposes corporate data to a potential breach due to a negligent act or human error. While accidental insiders are not malicious by nature, they are often the root cause of an attack. A recent study found this group is responsible for 64 per cent of reported incidents.[32] Typical examples include: unintentionally sending out confidential data to the wrong recipients; losing a laptop, mobile device, or USB drive; and sharing too much information though social media channels. The root causes for most of these breaches can be lack of employee training and broken business IT processes, or a combination. In the case of the latter, employees may put data and systems at risk by implementing 'workarounds' to get their jobs done.

Regarding accidental insiders, we asked respondents to report on the frequency of events and the time it took to discover and recover from an incident. Our research found the following:

[31] Tarun, R. (2019, January 17). A Layered Approach to Cybersecurity: People, Processes, and Technology. Fortinet. Retrieved from *https://www.fortinet.com/blog/industry-trends/a-layered-approach-to-cybersecurity--people--processes--and-tech.html*

[32] Ponemon Institute LLC. (2018). *2018 The Cost of Insider Threats.* (Ponemon Institute report). USA

A subset of organisations that have had their business interrupted by a security breach in the last 12 months reported the following impacts of an accidental insider:

Frequency

Within a subset of Australian businesses who experienced a breach, 36 per cent of Australian respondents report weekly or monthly events due to the, 'accidental insider'. This is the same for the global respondents (30 per cent).

Discovery

Within a subset of Australian businesses who experienced a breach, when this type of event happens, 62 per cent of Australian respondents are able to detect this in 'minutes or hours' compared to 50 per cent of the global respondents.

Recovery

Within a subset of Australian businesses who experienced a breach, 68 per cent of Australian respondents are able to recover from 'accidental insider' related incident inside of two hours, compared to 64 per cent of global respondents.

Targeted insiders can be described as employees who fall victim to an external attack. The most effective types of attacks tend to involve some level of social engineering where an adversary builds up intelligence on their target prior to the attack. Social engineering attacks can target individuals or groups in a company and may involve emails, pretext calling, or having 'urgent outside queries'. These attacks are often designed for the target to send or receive a file, click on a link or provide outside access to corporate data. A common example of a campaign that falls under this category is the Business Email Compromise (BEC). In this exploit, the attacker typically uses the identity of an employee to trick the target into sending money to the attacker's account. The FBI reported BEC scams cost victims more than US$12.5 billion dollars in the last five years.[33] In our research, 56 per cent, within the subset of Australian respondents reporting a security attack, have experienced BEC on a weekly, monthly or quarterly basis which is slightly higher than the APAC and European results of 48 and 49 per cent respectively.

[33] Federal Bureau of Investigation (2018, July 12). Public service announcement. Business E-mail Compromise The 12 Billion Dollar Scam. Retrieved from *https://www.ic3.gov/media/2018/180712.aspx*

Outlook

While the external hacker can cause the most damage, negligent employees generally trigger the most incidents and over time inflict similar damage. There are employees who can be negligent or others who found themselves targets of cyber adversaries. Security awareness programs can help to prevent incidents from both types of employees. A 2018 report from the SANS Institute argues that companies which have mature practices, that have been able to improve security competences and, over time, change behaviour, are in a much stronger position to avoid security incidents surfacing from employees.[34] Likewise, businesses that have little or no awareness programs are the most exposed.[35]

Organisations need to strike a constant balance between ensuring robust security and delivering strong user experiences. As security practices evolve and organisations shift their focus towards end-user awareness and training, there will likely be a reduction in the frequency of events triggered by employees. Organisations can then start to see the financial benefits and potentially reallocate budgets to other external concerns. As many organisations look to employ more contractors and casual freelancers alongside remote workers, it will become more important to have strong identity and access management solutions in place.

Recommendations

Increase Security Awareness to Manage Risk

The consequences of a security breach include productivity loss, corrupted business data, customer loss and loss of intellectual property (IP), as shown in our results. These outcomes can be mitigated with awareness and training. Some organisations have reported reductions in security incidents and breaches through targeted programs. These include fake phishing email drills, identifying employees most at risk and continual training sessions.

Identifying the Right Starting Point

Organisations do not adapt to mature frameworks overnight. A great starting point is recognising the maturity of an organisation through frameworks to determine the level of maturity and what is required to move up. The SANS Security Awareness Maturity Model is one source to consider.[36] There are many other pragmatic challenges such as ability to work with business leaders and securing active C-level support. People, alongside cutting-edge technology and robust business processes, are all essential for cyber resiliency.

[34] SANS Security Awareness Report Building Successful Security Awareness Programs (2018). Retrieved from *https://www.sans.org/security-awareness-training/reports/2018-security-awareness-report*
[35] Ibid.
[36] Ibid.

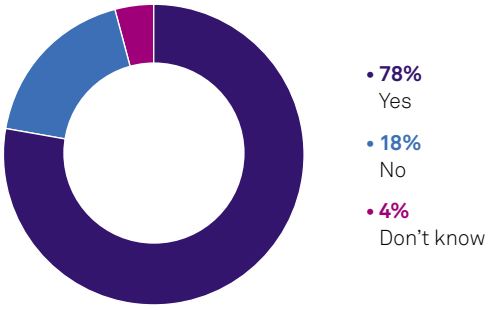
Cyber Resiliency and Incident Response

Our 2019 research shows that, on average, more than three out of four organisations (78 per cent) indicate having an incident response plan in place, which is a slight increase on our 2018 findings (75 per cent). Unfortunately, there is still a sizeable proportion globally that either confirmed no incident response plan exists (18 per cent) or did not know if their organisation had a plan (four per cent). These results indicate cyber maturity has increased only marginally year on year in respect to incident response planning.

Q: Does your organisation have an incident response plan in place?

Global

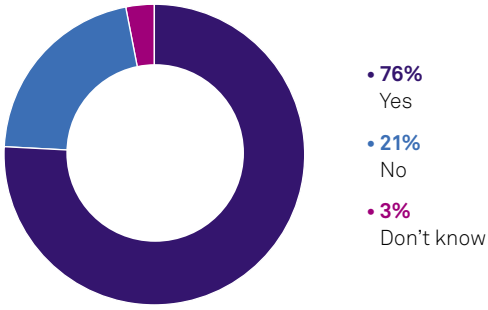
n=1,298



- **78%** Yes
- **18%** No
- **4%** Don't know

Australia

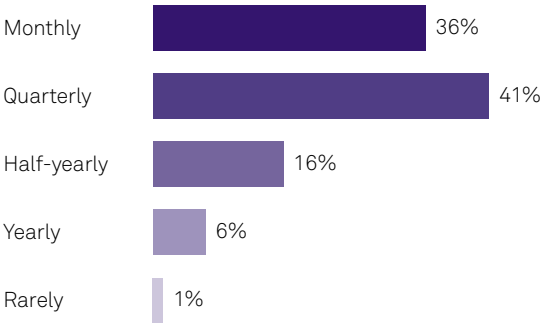
n=320



- **76%** Yes
- **21%** No
- **3%** Don't know

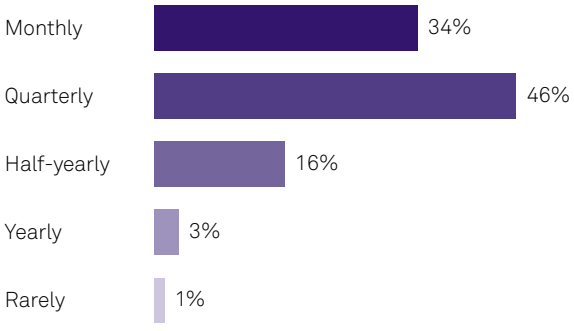
Q: If yes, how frequent is the testing and reviews of your incident response plan?

Global



n=1,012 (subset)

Australia



n=245 (subset)

Of the respondents that have an incident response plan, 77 per cent of them are testing and reviewing these plans at least once a quarter. In Australia, 34 per cent of respondents are testing monthly, marginally up from the 30 per cent reported in our 2018 Security Report. There were no changes year on year to the frequency of testing incident response plans between a monthly and quarterly basis.

Having a security response plan is not enough. A report from IBM found that 77 per cent of businesses do not have an incident response plan applied consistently across the organisation and less than one-third of respondents (31 per cent) feel that they have an adequate cyber resilience budget in place.[37] As the frequency and complexity of attacks increase, businesses struggle with challenges such as skill shortages and investments in new technologies.

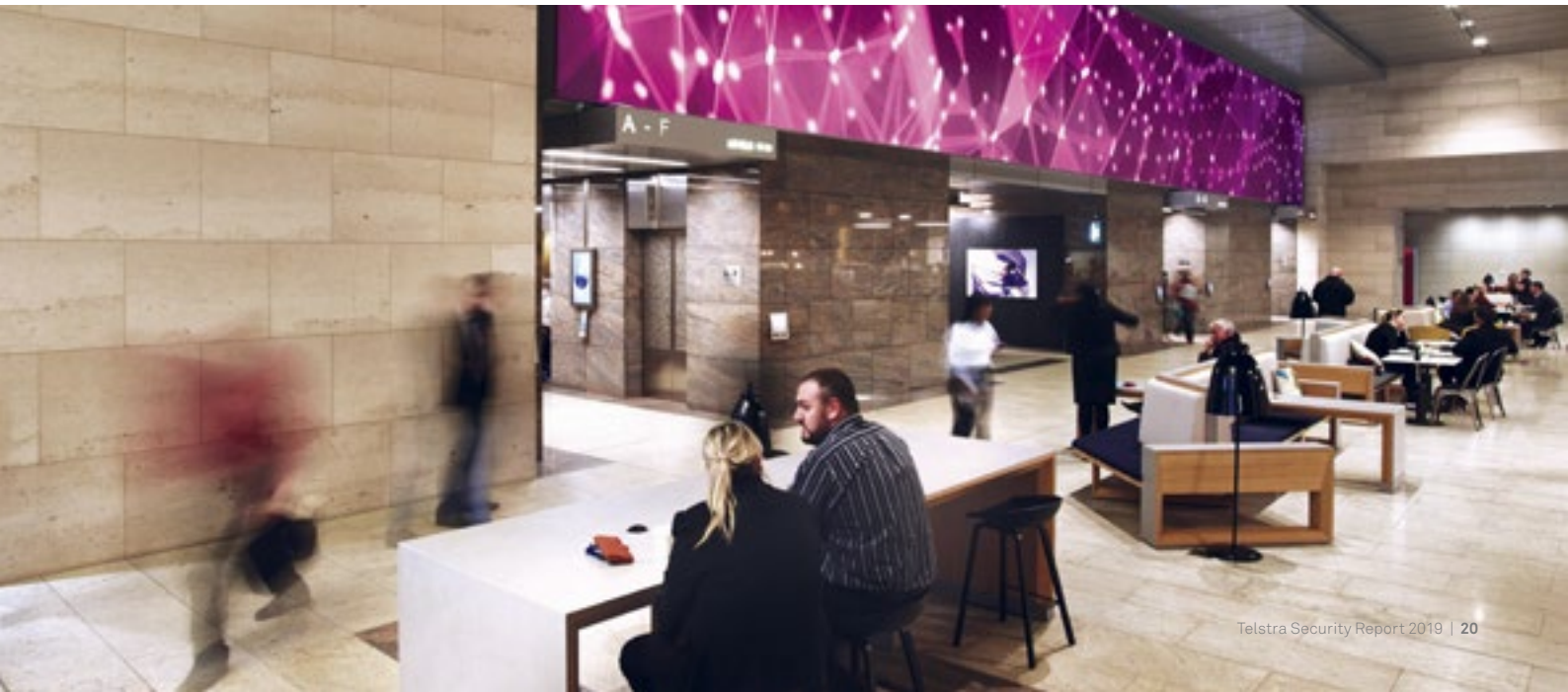
A recent Carbon Black research study surveyed incident response professionals and found that attacks are becoming more complex, and that in nearly half of the cases (46 per cent of attacks) the adversaries engaged in 'counter incident response'. This can be, for example, deploying tactics to evade sandboxing technologies or the widespread use of encryption to conceal activities. 'Island hopping' was another trend identified in 36 per cent of reported cases.[38] This is when an adversary first targets an organisation's affiliates – such as customers, suppliers, or partners – who may have a weaker security posture, before working their way through the supply chain to the primary target. In the Carbon Black study, 100 per cent of respondents observed the use of PowerShell for attempted lateral movements.

Given the frequency of attempted attacks, many defenders find it challenging to keep pace with their security adversaries. Some attacks can go undetected. Businesses can find themselves besieged by alerts and false positives, which can drain analyst resources. In this scenario, organisations may not be able to respond to every alert and will increasingly ignore some alerts. Sometimes one attack can mask another and distract analysts from the attacker's real target. This has been common in the past with some DDoS attacks.

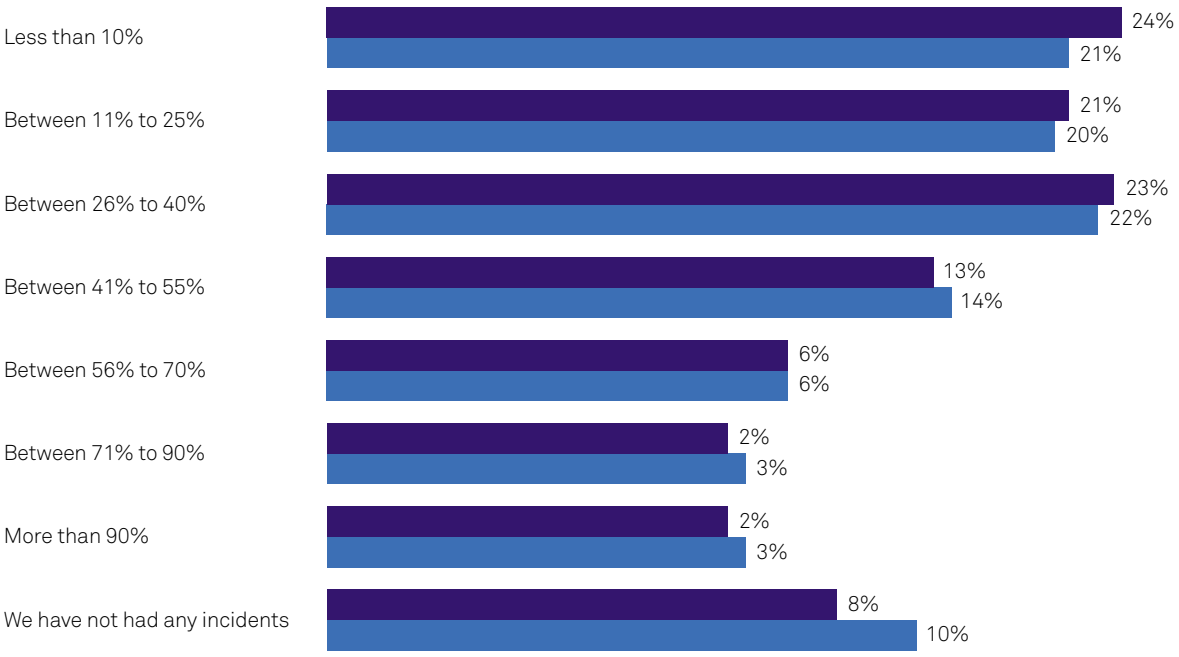
Advanced Persistent Threats (APTs), are engineered to evade security defences. APTs typically conducted by state-assisted or well-financed groups, are some of the hardest attacks to detect and are on the rise in the APAC region in particular.[39]

As part of our research, we asked respondents to identify the percentage of breach incidents their organisations responded to in the past year. The resulting data visualisations (page 21) highlights the sentiment of IT security professionals regarding the challenges of incident response, especially with regard to end-to-end visibility. It also reflects the large volume of alerts and threat intelligence experienced. Our research found that only 3 per cent of Australian, and 2 per cent of global respondents, believe they can respond to more than 9 out of 10 incidents. This compares to 5 per cent in Australia and 3 per cent globally, as reported in our 2018 Security Report. The number of respondents that 'have not had an incident' has decreased by seven per cent compared to last year in Australia (17 per cent in 2018 versus 10 per cent in 2019). Our 2019 Australian results are more in line with those for respondents globally.

[37] Ponemon Institute LLC. (2018). The Third Annual Study on the Cyber Resilient Organization. Retrieved from *https://www.ibm.com/downloads/cas/D3RGN4AJ*
[38] Carbon Black (2018). China, Russia & North Korea Launching Sophisticated, Espionage-Focused Cyberattacks Massachusetts, USA: Author. Retrieved from *https://www.carbonblack.com/company/news/article/china-russia-north-korea-launching-sophisticated-espionage-focused-cyberattacks-2/*
[39] GReAT (2018, July 10). APT Trends Report Q2 2018. Kaspersky Lab. *Retrieved from https://securelist.com/apt-trends-report-q2-2018/86487/*



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



Global n=1,298; Australia, n=320

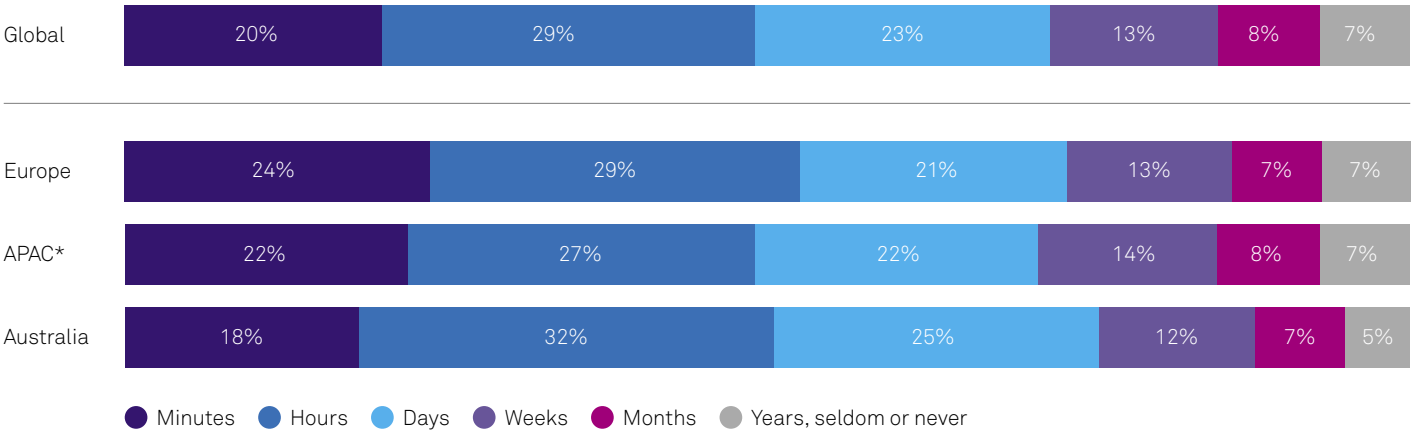
Improving Security Performance

Our research suggests that the average time to detect a security incident or breach is slipping. We considered 14 different types of threats and created an average. The results indicated only 52 per cent of Australian organisations are able to detect data breaches within 'minutes or hours', which is a decrease from 61 per cent in our 2018 Security Report. This compares to 49 per cent of APAC respondents (down from 53 per cent in 2018) and 50 per cent in Europe (down from 54 per cent in 2018).

With attacks on the rise this year, the data suggests more attacks are getting through and not immediately picked up. On the other hand, businesses are getting better at finding incidents and security breaches. Some 40 per cent of Australian businesses have been able to identify security breaches within 'days, weeks or months' compared to 29 per cent in the 2018 Security Report. Globally this figure was 44 per cent this year compared to 35 per cent last year.

The number of respondents who reported the time to detect a security incident or breach as 'years, seldom or never' dropped to seven per cent on average in the Australian and global results. In our 2018 Security Report this figure was 10 per cent in Australian and 12 per cent of global respondents. While businesses have shown improvement from last year's results, there is still a lot of room for improvement to reduce the initial detection times to seconds or minutes. The faster an incident or confirmed breach is identified, the quicker potential damage could be mitigated and reduced.

Q: What is the average time to detect a security breach across incident types?



Global, n=676; Europe, n=271; APAC (*includes Australia), n= 405; Australia, n=180
Average sample sizes across different types of incidents (subset of data)

In terms of recovery time from cyber-attacks, our research finds that on average, 70 per cent of the cases were recovered in less than two hours in Australia versus 74 per cent in our 2018 Security Report. Australia is, at present, slightly ahead of APAC and Europe in recovering faster from attacks. On average, 70 per cent of the attacks were recovered in less than two hours in Australia compared to 64 per cent and 65 per cent in APAC and Europe respectively.

Outlook

The frequency of attacks will likely increase in 2019 and beyond, as will the variety of attack vectors. The challenges many organisations face when it comes to security, such as timely breach detection and skill shortages, will continue to be top priorities. In previous reports we discussed how the industry has moved towards a presumption of breach approach. The focus for many has now evolved to reducing dwell times. The two most important KPIs respondents used to measure security performance has been time to detect from point where threat entered the environment and time to quarantine or contain a threat. While there are several ways businesses can measure the success of their security programs, metrics such as time to notify or analyse, will likely be the most important ones used in 2019. This approach will continue in recognition of industry trends as well as the stealth nature of many attacks. 2019 may also be a year where attackers become more brazen. Some attackers are moving away from a 'grab and go' approach to conducting a protracted 'campaign'. If trends highlighted in 2019 continue, APTs will also have a high concentration in the APAC region. Government and financial services will be some of the most targeted industries.

Despite some progress in detecting an incident or a breach, organisations are still taking too long to detect and contain. Time is arguably on the side of the attackers. In some cases, organisations will never know whether an attack has happened, how long it happened for and how much it was or still is costing their business. The quantity and severity of attacks and cost per attack will undoubtedly increase throughout the year. The costs associated with a breach will range from damage to physical infrastructure, loss of intellectual property, downtime, and in some cases health and safety if the target is a physical system such as an energy grid or plant assembly line.

The cost of a breach is increasing as well as the probability of an attack. A recent report from IBM and Ponemon Institute estimates the average cost of a data breach in their global results is US$3.86 million, an increase of 6.4 per cent from the previous year. The average cost of a record stolen was reported at US$148.[40] Their report also predicts that the probability of a material breach, defined as 1,000 or more records being lost or stolen, happening over the next two years is 27.9 per cent (up from 27.7 per cent last year).[41] The report also shows the extensive use of IoT devices increased cost per breach by US$5 per compromised record.[42] It will be increasingly important for businesses to continue to explore ways to automate threat analysis and consider the investment in game-changing technologies such as automation, AI and machine learning. It is also important to conduct simulations through red teams and blue teams. Security professionals should consider proactive threat hunting depending on their organisation's industry and level of exposure. Good incident response plans can improve dwell times and help to reduce the cost of data breaches.

[40] Ponemon Institute LLC. (2018). 2018 Cost of a Data Breach Study: Global Overview. Retrieved from *https://www.ibm.com/downloads/cas/861MNWN2*
[41] Ibid.
[42] Ibid.

Recommendations

Consider Proactive Incident Response

As attacks become harder to detect and more covert in nature, it will be important for organisations to upgrade their incident response plans. Organisations should also consider proactive threat hunting and the use of red teams and blue team simulations to test the effectiveness of the security program. Seventy one per cent of our respondents 'agree' or 'strongly agree' with this approach to strengthen cyber defences and set up such programs in both the Australian and global results. Having a communication plan in place for all stakeholders, both business and technical, when an incident occurs, and knowing your legal or regulatory requirements is essential. This is often part of a mature incident response plan, reinforced by regular testing through tabletop exercises. Our research identified 79 per cent of global respondents 'agree' or 'strongly agree' with this requirement for incident response versus 81 per cent of Australians.

Consider Impact of New Regulations

As regulations continue to be enforced around the world, it is important to review current incident response programs in place, at regular intervals. New rules on notification, such as 72 hours under GDPR, means businesses need to be more responsive in the event of a breach or incident. This requires having detailed and documented workflows and processes in place. While an incident or a breach may still be inevitable, businesses will want to show that all the precautions have been put in place and that reporting has been fast and transparent. This can help reduce potential liability. Purchasing cyber security insurance policies may also be considered for additional protection.

Protect the Supply Chain

With the advent of 'island hopping' attacks, an organisation's data is potentially vulnerable via a trusted third party. This means you need to be secured at every point in the supply chain. Supply chain risk assessments have been ranked as a high priority for APAC and European respondents. A strong incident response plan should therefore consider own and third-party systems connected to an organisation's ICT systems.

Security Challenges and Business Impact

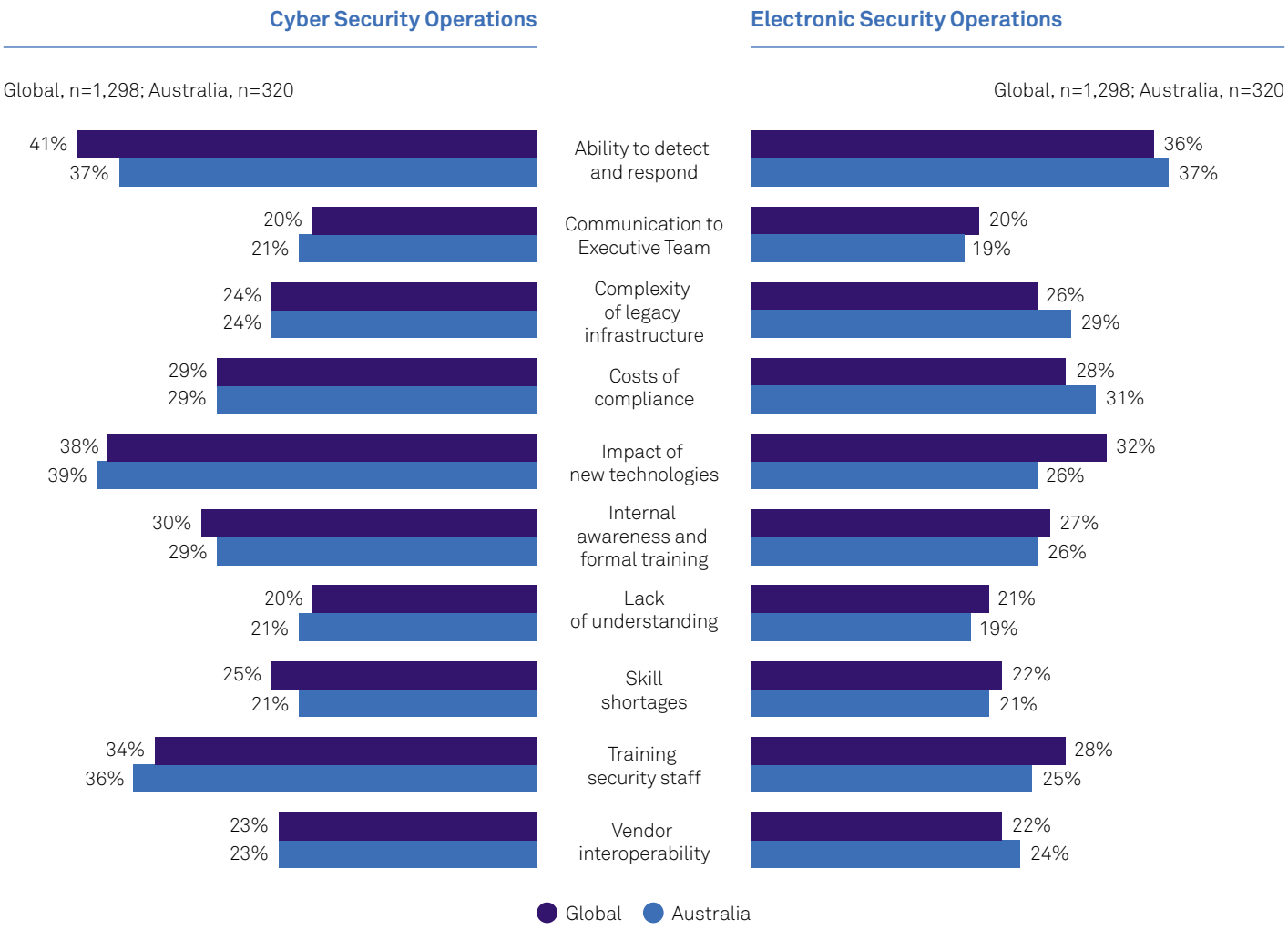
Challenges of Security Operations

Security threats have the attention of executives and boards. The CEO or board members have a 'high' or 'very high' formal level of involvement in cyber and electronic security in 48 per cent of respondent organisations. Business and IT leaders are also concerned about security, due to the difficulties in managing the IT environment and protecting against internal and external threats.

Our research identified the top two challenges globally regarding cyber security operations are the 'ability to detect and effectively respond' to security incidents in a timely manner and the 'impact of new technologies'. Training security staff was the third biggest challenge among the Australian, APAC, European and global respondents.

APAC, European and global respondents identified the same top two challenges for electronic security operations as they did for cyber security operations. Australian respondents also identified the 'ability to timely detect and effectively respond' as their number one challenge (37 per cent), with the second biggest challenge as being the 'cost of compliance' (31 per cent). This compares to 28 per cent in APAC, Europe and globally. Conversely the APAC, European and global respondents report the impact of technologies as the second biggest concern, at 32 per cent compared to 26 per cent in Australia.

Q: What are the major challenges with regards to your security operations?



As more security threats and breaches are reported, the perception is that security is becoming more difficult to manage due to the frequency and sophistication of attacks. In our 2018 Security Report, we touched on non-malware attacks such as social engineering and impersonation. Attacks are becoming more difficult to detect, track and predict. A 2018 report from Cisco highlights the expanding volume of encrypted web traffic – both legitimate and malicious.[43] This can create even more challenges and confusion for defenders trying to identify and monitor potential threats. Encryption is meant to enhance security yet it also provides malicious hackers with a powerful tool. It enables cyber criminals with cover to conceal lateral movements, conduct reconnaissance activities, and conceal command-and-control (C2) activity. Encryption affords adversaries more time to operate and inflict significant damage.[44]

Security Incidents

Each year there are several high-profile security breaches and for every publicised attack there are many other unreported incidents around the world. In our survey, the number of respondents who have reported that their organisation has experienced a cyber-attack (of any kind) in the past 12 months has increased. The biggest changes year on year were in Australia and Europe which reported an increase in security attacks (page 27).

[43] Cisco (2018). Cisco 2018 Annual Cybersecurity Report
[44] Ibid.

Q: Has your organisation experienced any kind of security attack in the past 12 months?

2018 Security Report Results	
Australia	**33%**
APAC*	**41%**
Europe	**36%**
Global	**39%**

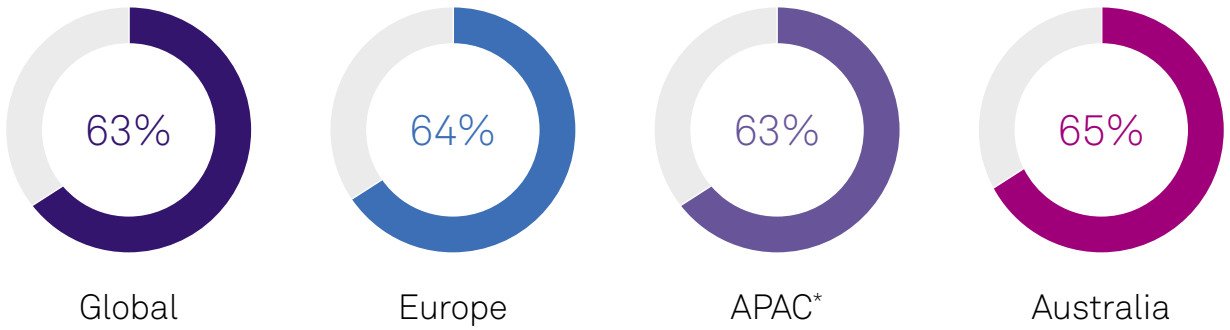
2018 Report: Australia, n=279; APAC (*includes Australia), n=739; Europe, n=475; Global, n=1,214

2019 Security Report Results	
Australia	**48%**
APAC*	**45%**
Europe	**52%**
Global	**47%**

2019 Report: Australia, n=320; APAC (*includes Australia), n=795; Europe, n=503; Global, n=1,298

Additionally, we asked survey respondents if their organisations experienced business interruption due to a breach in the past 12 months. Our research shows that 65 per cent of Australian respondents report having been impacted, up five per cent from our 2018 Security Report. APAC showed a decrease of three per cent (from 66 per cent in 2018 to 63 per cent in 2019) while Europe showed a decrease of six per cent (from 70 per cent in 2018 to 64 per cent in 2019).

Q: Has your business been interrupted due to a security breach in the past year?



Global, n=1,298; Europe, n=503; APAC (*includes Australia), n=795; Australia, n=320

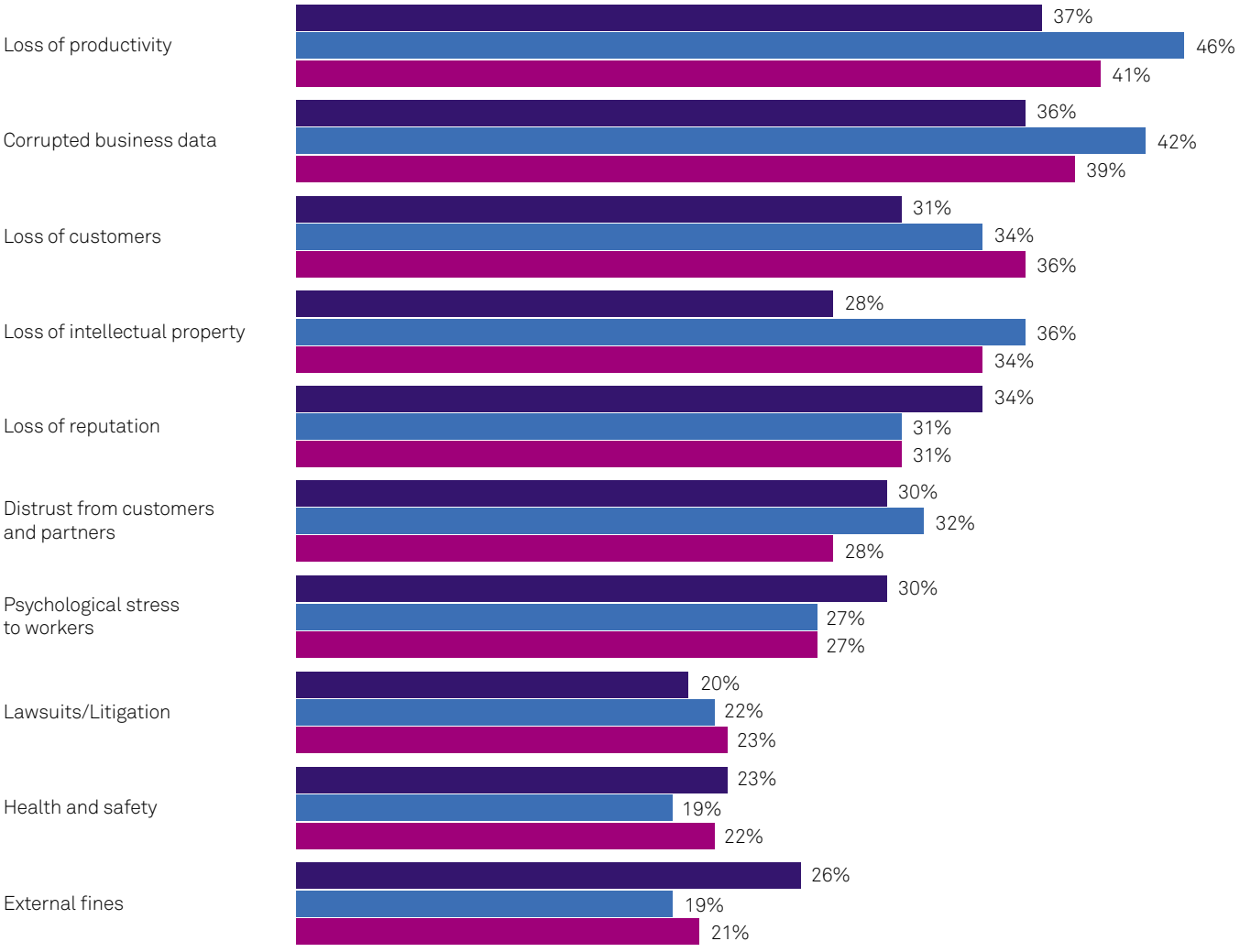
Our research shows there is an equal distribution of the attack vectors being perpetrated, from phishing to ransomware, and from ATPs to identity theft. Respondent responses indicate the two most widespread types of incidents in Australia are web application attacks and incidents caused by employee human error (38 and 37 per cent respectively of respondents who had a security incident). In 2018, RedShield mitigated one billion malicious HTTP requests for Australasian customers.[45] Business email compromise (BEC) events and phishing attacks – the most common types of attack reported in our 2018 Security Report – have decreased year on year but remain prevalent. In APAC, the two most common types were phishing and web application attacks. In Europe, the most common attacks target operational technology processes and systems.

[45] RedShield (2018). The State of Web Application Security in Australia

Business Impact

For the second consecutive year, respondents rated 'loss of productivity' as having the most detrimental impact to their business in Australia and Europe. This also ranked as the top concern in the APAC results in 2019. 'Loss of customers' also climbed up the rankings in Australia from fifth spot in 2018 to third spot in 2019. A likely explanation could be that in many organisations, a large proportion of future revenue will be from existing customers. A major security breach can undermine the relationship a brand has with their customers and unravel the efforts of many other departments.

Q: What are the more concerning potential impacts of a major security breach?



Europe, n = 503; APAC (*includes Australia), n = 795; Australia, n = 320

Europe APAC* Australia

Over the past 12 months renewed focus is on new compliance regulations and the financial consequences of not adhering to these regulations. There was a corresponding increase in the ranking of 'lawsuits/litigation' and 'external fines' as to be expected. However, these concerns have not ascended in terms of their ranking year on year. Last year, these two concerns were at the bottom of the list. In 2019, health and safety sits between litigation and external fines, and the relative ranking of external fines has not changed.

Outlook

In previous sections we discussed the broadening threat landscape driven, in part, by the convergence of cyber and electronic security and common threat vectors. We also discussed how organisations are focusing on security awareness programs, in part, as a counterbalance potentially to the frequency and pervasiveness of cyber-attacks. Nevertheless, the top challenges such as the impact of new technologies and ability to reduce dwell times, will continue in 2019. We expect the number of businesses that are reporting security attacks (and those that have seen their businesses interrupted due to a security breach) to remain stable in 2019.

While businesses continue to be concerned about the potential impacts of an attack, such as loss of productivity and corrupted data, organisations are likely to focus on the damage to reputation and customers over the next 12 months. New regulations are forcing the issue of public disclosure. This is making security breaches 'front page news' more than ever before. In the past, this was not the case. Major breaches known in the public domain can also expose a company brand to negative publicity. In these instances, some organisations may conclude that corrupted data or productivity loss can be recovered overtime, but the loss of customer confidence may be irreparable. As such, there will be more focus on preventive measures such as ensuring adequate protection for customer data and personal privacy. This is likely to be realised through continuous employee training and improvements to cyber defences.

Recommendations

Security Audits

It is likely that this trend will continue, with the majority of businesses expected to experience breaches in 2019 and beyond. The threat landscape is broadening and attacks will be more frequent and varied. Security is a common business risk which needs to be managed daily. A good way to understand your exposure is through a security audit conducted by an independent or third party. This can help identify which of your assets are potentially vulnerable and what these assets are worth, enabling you to assign a proportionate level of security protection.

Security Ownership

As cyber and electronic security converge, it is important to establish ownership of 'grey areas' such as responsibility to audit, manage, and patch unprotected connected devices which can be the source of a data breach. This may involve retiring connected endpoints that can no longer be updated, holding external suppliers to account, and ultimately extending a consistent policy across all connected devices.

Compliance and Privacy

During 2018, several new privacy regulations came into effect both domestically and internationally. Some of these were highly visible and discussed widely across industries, including the Australian Privacy Act amendment (Notifiable Data Breaches scheme) that came into effect in Australia in February 2018. The scheme includes an obligation to notify individuals whose personal information is involved in a qualifying data breach, including the recommended steps individuals should take in response to the breach. The Australian Information Commissioner must also be notified of eligible data breaches.[46]

In the European Union, the General Data Protection Regulation (GDPR) came into effect in May of 2018, establishing new requirements for protecting data belonging to EU citizens. 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 per cent of their total worldwide annual turnover.[47]

[46] 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*
[47] European Commission. 2018 reform of EU data protection rules. Retrieved from *https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en*

Q: As far as you know, has your organisation received any fines for being in breach of any new legislation enacted in the past two years?

	Australia	APAC*	Europe	Global
Yes	**55%**	**51%**	**63%**	**55%**
No	**36%**	**45%**	**35%**	**41%**
Don't Know	**9%**	**4%**	**2%**	**4%**
	n=320	n=795	n=503	n=1,298

*Includes Australia

While these are perhaps some of the most well-known regulations that have come into effect, there are many others coming into law across APAC, Europe and the United States (US). Some of the new regulations are industry specific, such as for the banking, energy, health care, and government sectors, which are highly regulated in most markets. There is evidence that the GDPR is getting the attention of other regulators looking at putting similar measures in place that protect individual privacy rights. For example, the California Consumer Privacy Act of 2018 will, once effective from 1 January 2020, give consumers the ability to view the data that organisations store about them and request that it be deleted and not sold to third parties.

Thirty eight per cent of Australian respondents indicated that the level of concern from customers on data privacy has increased over the past 12 months, compared to 46 per cent from the APAC and European respondents.

Beyond compliance, businesses are also relying on various security standards or frameworks as guiding principles for their corporate security policies. Australian respondents tend to work with government and industry bodies such as the International Organization for Standardisation and the International Electrotechnical Commission (ISO/IEC) family of standards for security of assets and systems. CERT Australia, now part of the Australian Cyber Security Centre, provides support and awareness for the business community.

A security framework is a set of documented processes that defines policies or procedures around how security controls can be implemented and managed on an ongoing basis. The challenge for many businesses is in choosing the right ones. There will be some nuances based on the type of organisation, size, location and compliance requirements, if applicable, amongst other considerations. Many frameworks align well with international standards and COBIT, specifically for best practices, quality control and management of IT environments. We asked respondents which 'security standards or frameworks they use within their organisation' or 'use as a guiding principle for their corporate security policies' and responses were as follows. With cross industry focus on GDPR, since becoming law in 2018, 73 per cent of the European respondents reported following this within their organisation. Respondents identified GDPR as ranked 30 points higher than the second item on the list, ISO at 43 per cent. The non-Australian APAC respondents reported 51 per cent following GDPR, with the next standard they reported following as ISO in second place at 44 per cent. Non-Australian APAC respondents identified as following the best practice framework, COBIT, with this item coming in at third place at 30 per cent.

Outlook

While there is currently a lot of focus on the GDPR, security frameworks and compliance reporting will continue to increase in complexity. Businesses will continue to follow the areas that are most important to their industry or company. This can be a blend of compliance, best practices and good security hygiene. There are signs that compliance monitoring is increasing. Our research found 91 per cent of Australian organisations report actively following the Australian Privacy Act, an increase of four per cent compared to our 2018 Security Report findings. Further, our research found 89 per cent of global organisations (not including Australian results) are actively following relevant national and regional legislation on cyber security, compared to 85 per cent in 2018.

Compliance is also being driven by the perception of heightened consumer awareness. This year 38 per cent of Australians reported the level of their customer concern about data privacy has increased, compared to 46 per cent in the global, APAC, and European results. These trends are likely to spark even more public debate, and potentially more legislation or regulatory intervention, depending on the region. There will also be several organisations who will receive fines or find themselves subject to increased regulatory scrutiny. Over half (55 per cent) of all respondents in our survey noted their organisation has received a fine for being in breach of any new legislation enacted in the past two years. We expect this trend to continue into 2019 as businesses contend with their new compliance and breach reporting obligations.

Recommendations

Continue to Co-ordinate Approaches

National and international standards and compliance reporting can be confusing. There is evidence of more security and privacy legislation coming into effect in the coming years, including industry specific regulations. Businesses are best advised to work with legal teams and compliance officers to keep pace with evolving standards. Organisations should be especially mindful on the use of customer data. Customer privacy issues and/or additional compliance reporting show no signs of abating in 2019.

Employee Training and Compliance Awareness

C-level executives and board members are taking on a fiduciary responsibility for security. Thirty per cent of our C-level respondents reported more frequent meetings to discuss security due to recent regulatory or compliance requirements. To assist in reducing the large number of human error breaches, organisations should provide end-user security training at all levels where possible. The good news is that our research indicates many businesses are increasingly implementing security awareness programs. Thirty one per cent of Australian respondents reported starting on this journey compared to 34 per cent in APAC and 37 per cent in Europe.

Security Threats and Trends

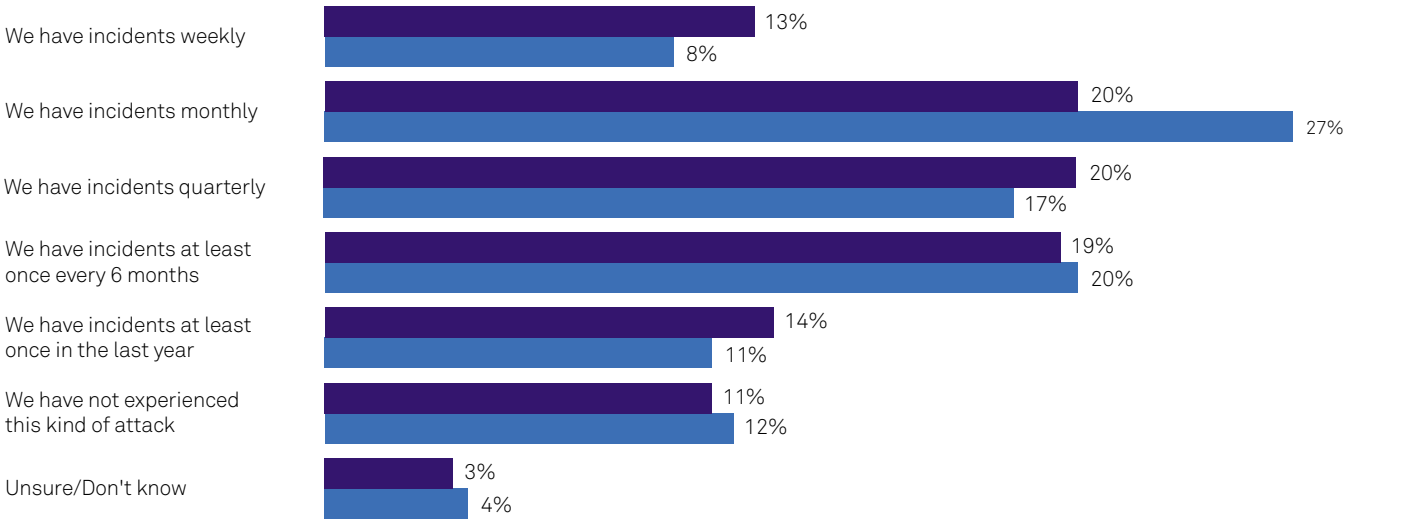
Email Threats and Phishing Campaigns

In Australia, FirstWave Cloud Technology scanned over 1.5 billion inbound and outbound emails across its customers' mail servers and blocked over 800,000 suspicious inbound emails. Within these, they identified examples of 'fileless malware'. This type of malware is described as an attempt to exploit software already installed on the victim's computer, such as macros and plug-ins, rather than trying to lure a victim into downloading an attachment.[48] A 2018 Microsoft article highlights how this strain can elude anti-virus software, be masked as a legitimate process and leave no trace on the disk, making it hard for forensic analysts to discover.[49] In another survey of 660 IT professionals responsible for endpoint security, respondents predicted that fileless attacks will represent 38 per cent of malware incidents in 2019.[50]

In our research, 63 per cent of global respondents and 65 per cent of Australian respondents reported their business was interrupted due to a security breach in the past year. Among the subset of organisations that suffered business interruption due to a security breach, 35 per cent of Australian organisations reported phishing incidents on a weekly or monthly basis. This is consistent with the findings we reported in our 2018 Security Report. Overall, the Australian and global results are consistent, however Australia tends to report greater instances of monthly attacks comparatively.

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



Global, n=821 (subset); Australia, n=209 (subset)

Global Australia

[48] FirstWave Cloud Technology. (2018). Cloud Technology's Threat Insights Report: 2018 Review.
[49] Microsoft (2018, 27 September). Out of sight but not invisible: Defeating fileless malware with behavior monitoring, AMSI, and next-gen AV. Retrieved from. *https://cloudblogs.microsoft.com/microsoftsecure/2018/09/27/out-of-sight-but-not-invisible-defeating-fileless-malware-with-behavior-monitoring-amsi-and-next-gen-av/*
[50] Ponemon Institute LLC (2018). State of Endpoint Security Risk. (Ponemon Institute report). USA

Outlook

Email will likely remain as a primary channel for business and personal communication, despite the rise of messaging apps and other social media platforms. As organisations increase their use of email, with this comes an expected increase in the proportion of spam emails. The number of malicious emails is likely to increase in 2019 and with that will come more phishing attacks. A report from Cofense Inc. found that one in ten emails reported by users were identified as malicious between January and June 2018.[51] These reported emails had bypassed other security solutions such as email gateways to make it to inboxes. The report also identified that over 50 per cent of reported malicious emails were tied to credential phishing over the first six months of 2018.[52]

Recommendations

End User Awareness

With organisations showing an increased focus on formal education, the topics of malicious email and malware should be among the first covered for end users. Some IT departments undergo fake phishing email drill scenarios to evaluate how well employees are prepared to evaluate a phishing email relative to a legitimate message. Other organisations have sought to identify 'at risk' employees. Businesses should also consider other corporate policies regarding money transfers and social media policies to reduce the likelihood of employees being targeted. There is research showing businesses who can focus on education programs are able to reduce costs per breach.[53]

Be Aware of Phishing Campaigns Targeting Mobile Devices

Mobile-phishing campaigns are also a major challenge. A report from Wandera shows that users are 18 times more likely to be exposed to a phishing attack than other malware.[54] Training employees on how to spot phishing activities is recommended in addition to implementing solutions to detect and prevent these types of attacks.

Consider Multi-Factor Authentication and Frequent Password Changes

In addition to improving end-user awareness and alerting them to specific types of phishing campaigns, implementing multi-factor authentication for corporate email and using a secure corporate network can mitigate the potential for an attacker to gain access through stolen credentials. Organisations should also evaluate strong tools and consider strict policies for password management. For example, frequent password changes with the inability to reuse previous passwords, are fast becoming the norm. Security enforcement will also have to be balanced with user experience to avoid IT workarounds and increase chances of adherence to policies. Sometimes a direct line of communication between IT and end-users can lead to better outcomes.

[51] Cofense. (2018). The State of Phishing Defense. Report. USA: Author. Retrieved from: *https://cofense.com/state-of-phishing-defense-2018/*
[52] Ibid.
[53] Ponemon Institute LLC. (2018). *2018 The Cost of Insider Threats.* (Ponemon Institute report). USA: Author.
[54] Wandra (2018). Mobile phishing report 2018. Retrieved from *https://www.wandera.com/mobile-security/mobile-phishing-report-2018/*

Ransomware and Crypto Mining

As we have reported for the past several years, ransomware is another common form of malicious software. It targets both human and technical weaknesses in an effort to deny the availability of critical data and/or systems. Ransomware is frequently delivered through various channels. Phishing is one of the most common ransomware infection vectors, where a user is enticed to click on a seemingly routine email attachment such as an invoice or receipt. Once the victim opens the file, malware is surreptitiously installed onto the computer. This attack spreads quickly, encrypting files on the victim's device and usually across connected networks as well, often going undetected. When the victim is no longer able to access his or her data, the attacker typically demands the payment of a ransom. The common form of payment is by some form of cryptocurrency, such as Bitcoin or Monero. The adversary will often promise the victim will regain access to their data once the amount is paid by a set deadline. If the ransom is not paid, the encrypted files remain inaccessible.

In our 2018 Security Report we discussed how ransomware is moving from 'spray and pray' tactics to campaigns targeting individuals and/or specific industries. Other ransomware observations included:

- Social media research has helped adversaries to identify individual employees or departments working within target companies they intend to attack.
- Some strains of malware attempt to find ways to attack back-up systems first, to increase the price of the ransom.
- Ransomware as a Service (RaaS) has allowed malware developers to offer their malware services to others using the dark-web as a major distribution channel.

Our 2019 research found the following on ransomware:

Attacks are inevitable

Among the subset of organisations we surveyed, that reported being interrupted due to a security breach in the past 12 months, 32 per cent of Australian respondents indicated that their business had been interrupted 'on a weekly or monthly basis' from ransomware attacks. This is comparable with what we presented in our 2018 Security Report (31 per cent). For the APAC and European regions, this figure was recorded at 26 per cent and 24 per cent respectively. Australia's percentage is considered relatively high even compared to other developed countries such as UK, Germany, and France; recorded at 19 per cent, 27 per cent, and 26 per cent respectively. Among the subset of organisations interrupted due to a security breach in the past 12 months, 81 per cent of Australian respondents indicated they had experienced a ransomware attack. This is an increase of five per cent compared to the previous year. Within the same region, 83 per cent of Singaporean respondents, and 93 per cent of New Zealand respondents, reported ransomware attacks in the past year.

Around half the victims pay the ransom

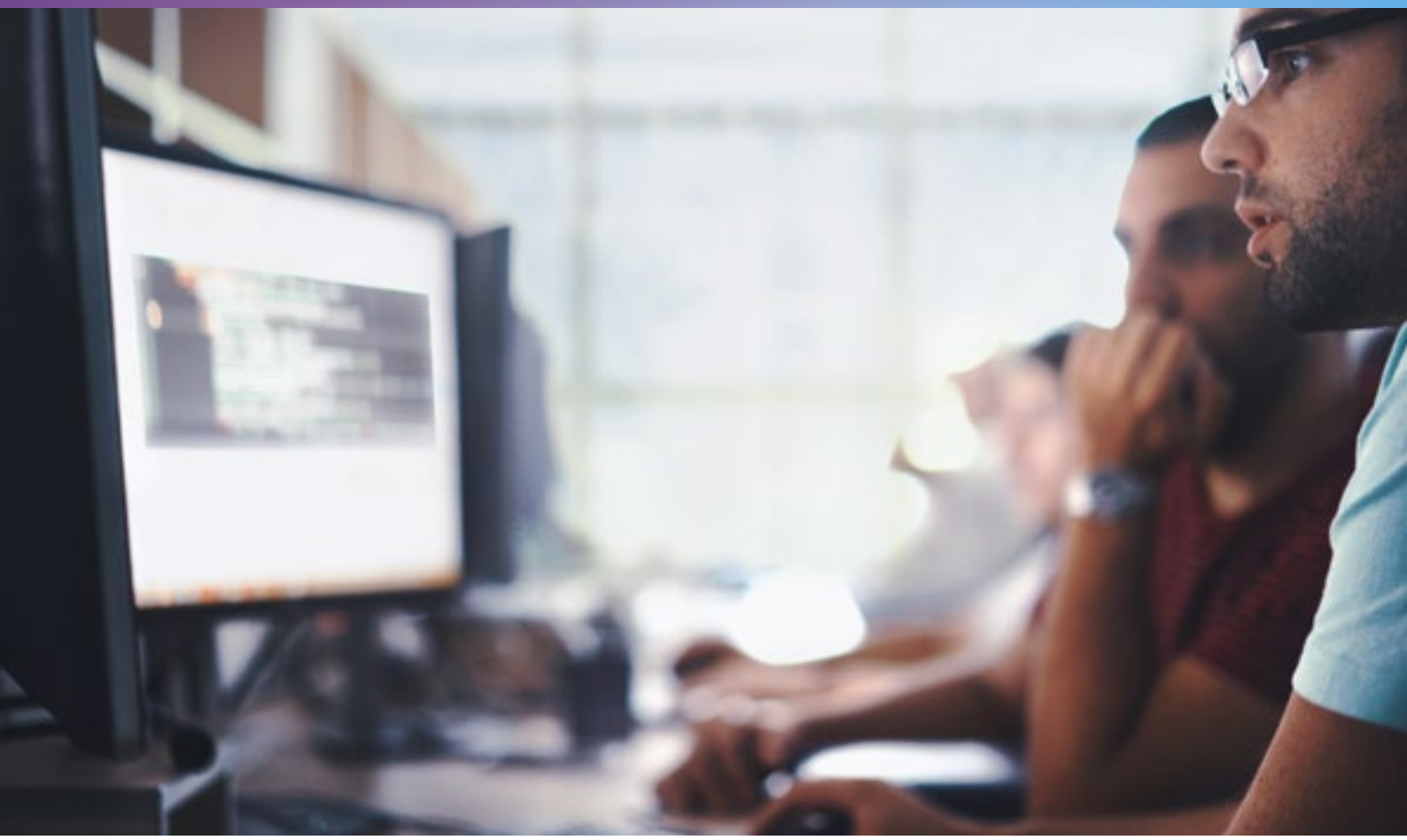
Fifty one per cent of Australian respondents, who were victims of ransomware, reported paying the ransom. This is an increase of four per cent year on year. This rate is higher than in the APAC and European regions, where 48 per cent and 50 per cent respectively indicate having paid a ransom. Singapore and New Zealand both reported a higher incidence of ransomware attacks, and also report the highest rate of paying the ransom after an attack (61 per cent respectively).

Most retrieve data after paying the ransom

Seventy seven per cent of Australian businesses which paid a ransom were able to retrieve their data after making the payment. This is a decrease of nine per cent year on year. As for the APAC and European regions, both recorded higher figures than Australia at 83 per cent and 88 per cent respectively in 2018. Interestingly, Germany and France recorded a significantly higher rate of 96 per cent.

Some would pay again

In spite of the lowest rate of data retrieval after paying ransom, 79 per cent of Australian respondents indicated they would pay the ransom again next time if there were no back-up files available. This is relatively high compared to other APAC and European regions, which recorded 75 per cent and 73 per cent respectively. Further, countries such as Germany and France, which had a higher success rate of retrieving data after ransom payment, both indicated a lower propensity to pay a ransom again at 78 per cent and 68 per cent respectively.



Ransomware remains prevalent, and our research also shows evidence of an increase in crypto mining. This is due in part to the value of cryptocurrencies being driven by the phenomenal rise of Bitcoin, until its crash in the second half of 2018. Any resurgence of cryptocurrency would likely propagate more attacks. Crypto mining is where coin-miner malware hijacks systems to use computer processing power to create (or mine) new cryptocurrency without the victims' consent or awareness. A report from McAfee shows a decline in new families of ransomware, due in part to threat actors switching from ransomware to crypto mining. Specifically, McAfee reports a nearly 4,000 per cent increase in crypto mining in Q3 2018 as compared to the previous year.[55] In some quarters in 2018, crypto mining was seen on a grand scale, making an appearance on all platforms, devices, operating systems, and in all browsers.[56]

There are several methods used to spread crypto mining malware, some are listed on page 39.

- Compromised Mobile Apps. Similar to other common forms of malware, it's relatively simple for attackers to add mining modules to already malicious apps. Unsuspecting users could be infected by clicking an ad banner or downloading fake AV software. As an example of one type of malware, the Loapi Trojan can demand administration rights as part of the download process. Users that do not comply are locked out from their devices.
- Drive-by Mining. In September 2017, Coinhive introduced an API that could mine Monero currency directly within a web browser. Following this, some adversaries introduced copycat technology to force unsuspecting visitors of a website to mine their currency. However, once a victim is no longer on the website, the mining stops. This, in turn, has forced these malicious attackers to seek to extend sessions through pop-ups hidden beneath the taskbar and the use of compromised plug-ins amongst other means.[57]

[55] McAfee Threat Labs Report (2018). California, USA: Author. Retrieved from *https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf*
[56] Malwarebytes (2018). Cybercrime tactics and techniques Q1 2018. California, USA: Author. Retrieved from *https://www.malwarebytes.com/pdf/white-papers/CTNT-Q1-2018.pdf*
[57] Concordia University (2018). A first look at browser based cryptojacking. Retrieved from *https://arxiv.org/pdf/1803.02887.pdf*

Outlook

Whilst the global ransomware market has grown substantially over the years, recently it has begun to slow down. As the market readjusts, ransomware attackers are shifting their focus to more profitable areas of the market, such as crypto mining, etc. Formjacking, for example, has been identified as a new malware variant as criminals consider new campaigns.[58] Carbon Black research has reported US$1.1 billion in cryptocurrency related thefts in the first six months of 2018, which is attributable to cryptocurrency stealing malware.[59] Early in 2018, a report from Malwarebytes highlighted the prospect of crypto mining surpassing all other cybercrime.[60] We do note, however, that crypto mining is showing signs of slowing and the price of cryptocurrency in 2019 and beyond will ultimately determine the level of crypto-related activity and crime.

Recommendations

Continuously Evaluate Ransomware and Other Malware Variants

Ransomware is pervasive, but the number of types is in decline. Businesses should continue to identify critical data and ensure regular offline backups and versioning is performed. Be mindful of crypto mining and other crime resulting from the rise of cryptocurrencies. With the current declines in this market, we will most likely see scammers turn to new campaigns such as formjacking.

Patch Early and Often

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

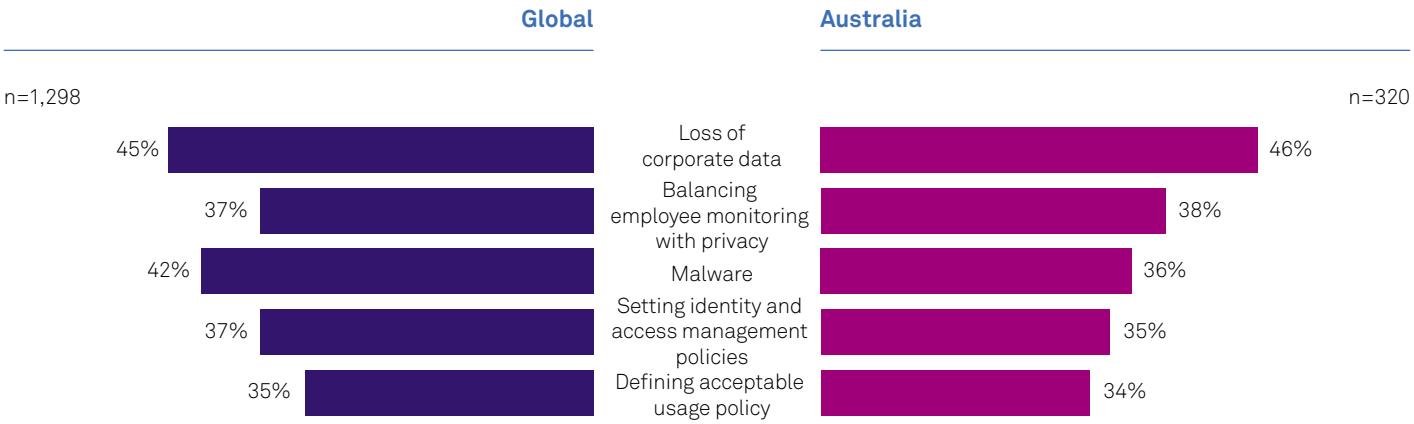
[58] SecurityBrief Newsdesk (2019, February 26). New threats on the block: Formjacking, IoT, LotL attacks. SecurityBrief Retrieved from *https://securitybrief.asia/story/new-threats-on-the-block-formjacking-iot-lotl-attacks*
[59] Carbon Black (2018). Cryptocurrency Gold Rush on the Dark Web. California, USA: Author. Retrieved from *https://www.carbonblack.com/cryptocurrency-dark-web*
[60] Malwarebytes (2018). Cybercrime tactics and techniques Q1 2018.

Mobile Security

Mobile security remains one of the biggest sources of concern related to security attacks. In Australia, 38 per cent of respondents identified mobile devices as one of their biggest concerns, alongside cloud services. This is an increase from 26 per cent in our 2018 Security Report.

Within the global, APAC and European results, mobility was the second most frequently identified concern after cloud (at 39 and 34 per cent respectively). When asked about the top security concerns for when employees are accessing corporate data from mobile devices, the Australian, APAC, and global respondents tend to be most concerned about the loss of corporate data. European respondents are most concerned about malware.

Q: If employees are accessing corporate data from mobile devices, what are your top security concerns?



Common Attack Methods

There are several methods for the delivery of malware to mobile devices, such as phishing, malware and malicious apps. Symantec reported that there was a 54 per cent increase in new malware variants alone in one year – from 17,000 in 2016 to 24,000 in 2017. Attackers developed new methods of infection allowing the malware to remain on infected devices for longer periods. The report also indicated adversaries were finding 'a variety of means to generate revenue from devices, from ransomware to cryptocurrency mining'.[61]

While mobile device-targeted attacks have been numerous and persistent, this has not always been matched with an increase in employee awareness. For example, when employees give sweeping permissions to apps and services, they can often inadvertently expose their devices to potential data breaches. This could include tracking of individuals, and/or exfiltration of user, app, or corporate data. In some cases, this can be the result of outdated IT policies, for example IT departments not extending the same security policy required for laptops to personal devices. This can range from using default passwords and/or not changing passwords frequently; not using threat response actions, to not using two-factor authentication or encrypting sensitive data. Sometimes organisations may not have a defined policy for using public Wi-Fi access points. Research from Zimperium shows one in five users have connected to malicious Wi-Fi in the past.[62]

[61] Symantec. (2018). Internet Security Threat Report: Volume 23. California, USA: Author. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf
[62] Zimperium (2018). Mobile Security and BYOD Report. Retrieved from https://get.zimperium.com/2018-mobile-security-byod-report/

Outlook

Mobility has led to sweeping efficiencies across many businesses, from improvements with individual productivity to streamlined business processes. However some organisations struggle to balance security with operational efficiencies and user experience. Organisations will continue to support employees using personal or work devices remotely as there are many other potential benefits, such as the ability to attract top talent and employee satisfaction. Bring your own device (BYOD) policies remain popular, a recent survey by Zimperium reported that 74 per cent of businesses attribute 'improved employee mobility and productivity'[63] to this policy. There are, however, other models that should also be considered. Some businesses have moved to alternate models of choose your own device (CYOD); company-owned, personally expensed (COPE); and company owned, business only (COBO). While policies set out basic approaches, business leaders should focus more on IT solutions, such as device, network, and application management solutions alongside employee training.

Recommendations

Consider Unified Endpoint Management

Unified endpoint management (UEM) is the evolution of enterprise mobility management (EMM). UEM discovers, manages, and secures mobile devices and governs the access those devices have to enterprise applications and data just like EMM. Many UEM products now also provide management and control functions for traditional desktops, laptops and client-server applications. Some of the security capabilities of UEM can include secure collaboration, compliance checking, VPN connectivity, encryption and device certificate management. UEM can help organisations to unify management of mobile and traditional endpoints as well as provision applications across multiple platforms. It is an important consideration for companies with cloud-first/mobile-first strategies. UEM platforms also support other security functions, including compliance checking, VPN connectivity, data security/encryption and device certificate management. These solutions have been very effective in supporting businesses with policies such as BYOD.

Mobile Threat Defence Solutions

Mobile Threat Defence (MTD) solutions deliver mobile specific security outcomes using a 'mobile-first' approach to endpoint security. They are designed to protect against the key threat vectors affecting mobile (including app, device and network). MTD solutions may use any of a combination of techniques to detect threats across these vectors, including machine learning, crowdsourced threat intelligence and behavioural anomaly detection. These techniques are necessary to respond to the rapidly evolving and increasing threats affecting mobile.

Selecting MTD solutions which integrate well with the UEM platform is recommended to create a multi-layered security approach. UEM platforms offer certain security functions, however they do not always actively scan for mobile-related threats on devices or networks. Integrating MTD with UEM delivers enhanced capability, such as simplifying deployment and ensuring user adoption of the MTD solution, through to automated remediation policies and conditional access based on a devices security posture as determined by the MTD solution.

[63] Ibid.

Advanced Persistent Threats (APTs)

Advanced persistent threats (APTs) have been a pervasive part of the cyber threat landscape year on year. A recent report from FireEye shows an increased use of this attack type by nation-state groups, such as Iran.[64] The FireEye report also highlights new APT types. Uniquely, their customers in the APAC region are twice as likely to have experienced multiple incidents from multiple APT attack vectors, compared to customers in EMEA or North America.[65]

APTs can be extremely dangerous. This is especially true from the perspective of intellectual property theft. APTs use multiple phases to infiltrate a network while avoiding detection. Their primary objective is to monitor activity and harvest valuable data, often slowly over a period of months and years. Unlike other types of attack vectors, APTs aim to evade detection by blending in with other traffic, adapting to the victim's organisation, communicating infrequently if necessary, and even circumventing security measures designed to defend against them. There is often no signature associated with an APT and their attacks are often based on zero-day exploits.

Techniques

APT attacks use one of many ways to gain entry such as spear phishing, exploiting system vulnerabilities, delivery of attack code through USB devices, or penetration through partner, customer, or supplier networks. Many attackers target the supply chain as an entry mechanism into target organisations. Once in place, APTs can move laterally through data centre networks and blend in with normal network traffic to achieve their objectives. Our research found that among the subset of Australian respondents whose businesses have been interrupted due to a security breach in the past year, 29 per cent believe to have experienced an APT attack on at least a monthly basis, which is consistent year on year. In APAC, this figure is 26 per cent, up from 22 per cent last year. This is also slightly higher than in Europe, where 24 per cent of APT attacks were reported to have occurred at least once per month.

[64] FireEye (2018). M-Trends 2018. Retrieved from *https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html*
[65] Ibid.

Outlook

The focus of APT attacks will remain to be the theft of commercial secrets and the main industries targeted will continue to be banks, consulting and IT companies, manufacturing, and government. Major real-world events are also likely to be APT targets. An example of this was the high-profile APT attack directed at the infrastructure supporting the Winter Olympics in South Korea.[66] APT attacks vary widely, but organisations should look at the motives of a potential adversary as a way of identifying the appropriate response. Responses can range from reducing the attack surface, improving threat intelligence, collaboration with the government or with industry partners, through to the use of cutting edge AI-driven technologies. While APTs are common and universal, APAC will likely continue to see a lot of APTs in 2019 from both point of origin and destination location of many intended targets.

Recommendations

APT-Specific Threat Hunting

APTs and zero-day attacks are often designed to steal as much sensitive data and corporate secrets as possible. Given the sophistication of these attacks, organisations that are most at risk should also consider adopting threat hunting specific to APTs. There are a several platforms and methodologies to consider. Good business outcomes should focus on ability to identify zero-day exploits at scale, improve security performance metrics such as the ability to reduce dwell times and improve the businesses understanding and motives of would be attackers. Red team and blue team exercises, where internal resources play the role of an attacker, can also help to identify and shore up vulnerabilities in cyber defences. In many cases, independent or third-party audits should also be considered.

Consult Third-party Resources

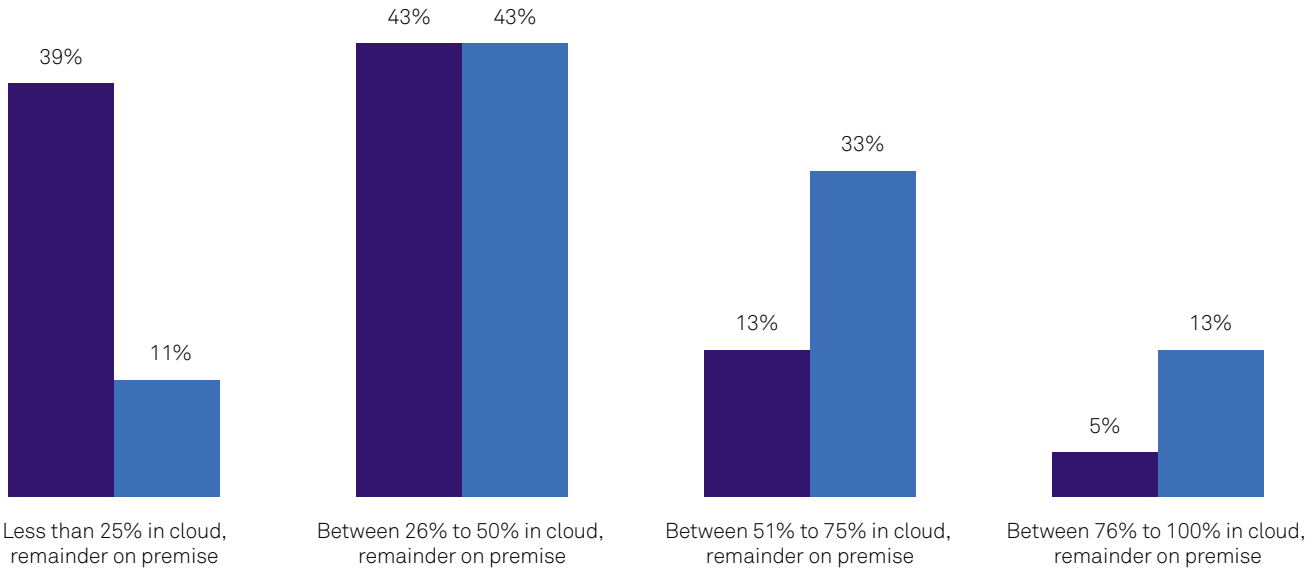
The MITRE Corporation, a not-for-profit research organisation, developed a methodology called ATT&CK, for threat hunting. This methodology is specifically focused on understanding the potential attacker, motives, possible moves, and evasion strategies.[67] These strategies can help organisations to better prepare and defend against these threats. Others to consider are local computer emergency response teams (CERT) that often work between industry and government.

[66] GReAT (2018, March 8). OlympicDestroyer is here to trick the industry. Kaspersky Lab. *https://securelist.com/olympicdestroyer-is-here-to-trick-the-industry/84295/*
[67] MITRE (2017) Finding Cyber Threats with ATT&CK-Based Analytics. Retrieved from *https://www.mitre.org/publications/technical-papers/finding-cyber-threats-with-attck-based-analytics*

Cloud Security

A recent report from F5 Networks found that nearly 90 per cent of businesses have multi-cloud architectures driven by applications and use cases.[68] Research from GlobalData shows the typical business needs to support up to 20 different cloud environments at any given time.[69] Hybrid cloud, defined as a cloud-based IT infrastructure that encompasses multiple cloud environments, is the de facto industry standard. The migration and deployment of applications across public, private, and hybrid cloud environments will only continue in the coming years. While businesses will likely retain some data on-premises for various reasons, cloud computing adoption continues to increase. The success of many IT projects, such as enabling DevOps, deploying micro services or building apps native to cloud, would not have been possible without this architecture.

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



Australia results, n=320

While cloud has also brought many efficiency improvements in a similar sense to mobility, cloud too has several security considerations. There are many web-scale companies that are active in APAC and globally, such as AWS, Azure, Google, AliCloud, IBM and Huawei. There are many other traditional independent software vendors (ISVs), that offer very mature cloud solutions, such as SAP and Oracle. Running applications in cloud environments is changing network topologies from a north-south direction (typical for perimeter security) to an east-west flow, reflecting a high-level of interconnection between data centre and cloud providers. This paradigm shift is challenging traditional perimeter security defences, such as authentication, data access and control. As applications and data move to the cloud, IT managers often lose some visibility and control when compared to a premise environment. While in many cases cloud has led to dramatic improvements in update cycles, premise-based solutions do not have same frequency of updates. The challenge is delivering a consistency of user experience. These paradigm shifts challenge traditional security constructs and thinking.

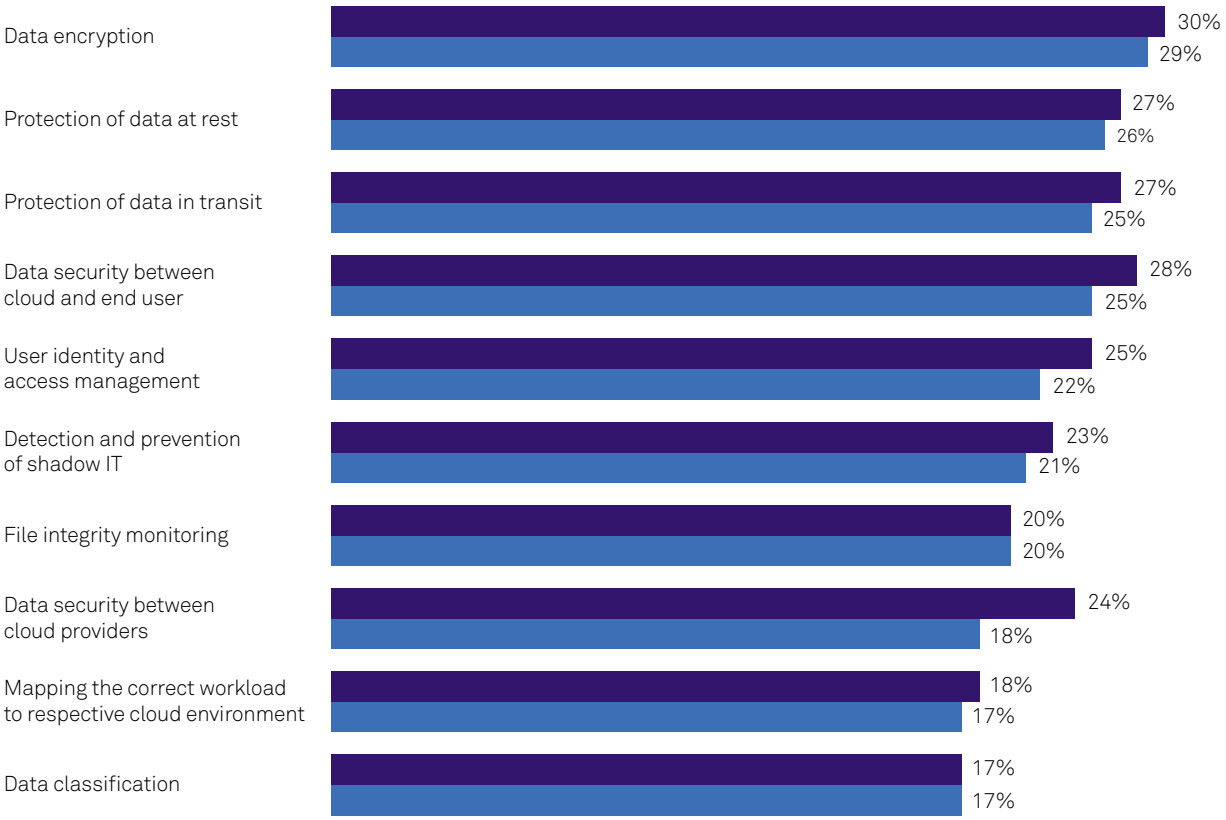
[68] F5. (2019). State of Applications Services 2019 Report. Retrieved from *https://www.f5.com/state-of-application-services-report*
[69] GlobalData market estimates

Security management is further complicated by the dynamic nature of virtualised applications, which can be moved between host servers as resource demands change. Businesses are also virtualising applications and moving to new architectures, such as containers and serverless compute. The rise of mobile applications and cloud-based environments means that there is a heightened risk of malware spreading laterally throughout IT environments unless IT invokes some form of central user authentication and ensures the appropriate data storage/access controls. Research within the past year shows cloud providers themselves are also being targeted.[70]

Top Perceived Threats

Our research shows that the most nominated concern for both Australian and global respondents when it comes to cloud security is data encryption protection. Australian respondents place slightly more emphasis on the protection of data in transit than their global peers. Global respondents have slightly more focus on the protection of data between the cloud and end-user (north-south traffic). Some common concerns are around file integrity monitoring, identity and access management through to the detection of shadow IT systems. Others are around the ability to map workloads to the appropriate cloud environments.

Q. In cases where applications / data are stored and accessed from the cloud, what are some of the top security considerations?



Global, n=1,298; Australia, n=320

[70] Bond, D (2018, July 12). Hackers target cloud services. Retrieved from https://www.ft.com/content/4f990a78-537a-11e8-84f4-43d65af59d43

Outlook

Cloud continues to be a major talking point. A recent report from Palo Alto Networks found that 91 per cent of organisations are concerned about public cloud security.[71] An area that is being impacted dramatically by the virtualisation of infrastructure includes networks and data centres. Many purpose-built appliances, such as firewalls, load balancers and WAN optimisation solutions will continue to be instantiated and deployed in cloud environments. Businesses will also continue down a path of application modernisation, and increasingly migrate away from legacy applications to containers. By so doing, adopting micro-services development strategies and serverless computing infrastructure become more accessible. The desired end state will vary by company. For some, this could be the ability to write scalable code without considering the underlying architecture. For others, it can be removing any barriers between operations and developers to create an ICT environment that is more responsive to the business and the end-users it supports.

The business requirement for cost efficiency, agility, and scale needs to be balanced with managing risk and compliance. Our survey results confirm that cloud adoption plans continue. The adoption of cloud-specific workloads will continue to grow and accelerate continuous delivery. Likewise, adoption of containers, micro-services and even serverless computing will continue to push the boundaries of virtualisation and iterative development cycles. GlobalData estimates that by 2020, at least half of all large IoT implementations will be deployed from the cloud.[72] As businesses deploy more workloads to the cloud, they will also need to mitigate potential threats. These can range from authentication, proxy attacks (e.g. man-in-the-middle), malware (e.g. ransomware), injection attacks (e.g. LDAP, SIP, SQL or XML), cross site scripting, through to DDoS attacks.

Organisations also must consider the trade-offs between managing data though private, public, or hybrid clouds. Cloud providers themselves are likely to be targets of cyber-attacks. There are limitations on what cloud providers are liable for in the event of a breach and this also needs to be considered when choosing between platforms. There are also risks in shadow IT, which will need to be mitigated with end-users. A number of platforms exist that can help IT departments discover this phenomenon, monitor usage, apply templated policies and even predict the expense of public cloud environments.

[71] Palo Alto Networks (2018). 2018 Cloud Security Report (created in partnership with Cybersecurity Insiders). Retrieved from *https://www.paloaltonetworks.com/resources/research/2018-cloud-security-report-palo-alto-networks*

[72] GlobalData market estimates

Recommendations

Consider Cloud Access Security Brokers (CASBs)

Cloud Access Security Brokers (CASBs) are a visibility and policy control point to secure cloud Security as a Service (cloud SaaS). Capabilities vary but can be provisioned as a proxy gateway, as a hosted agent or as 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, improved compliance, threat prevention, and data loss prevention. For the second consecutive year, our research shows a strong interest in these types of solutions to support cloud security issues.

Embrace Zero Trust for Network Segmentation

To maintain IT security in virtualised public and private clouds, businesses 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. Access, for example, should be granted for specific applications based on credentials. It works by assigning policies to users, applications, and workloads.

Consider Cloud Management Platforms

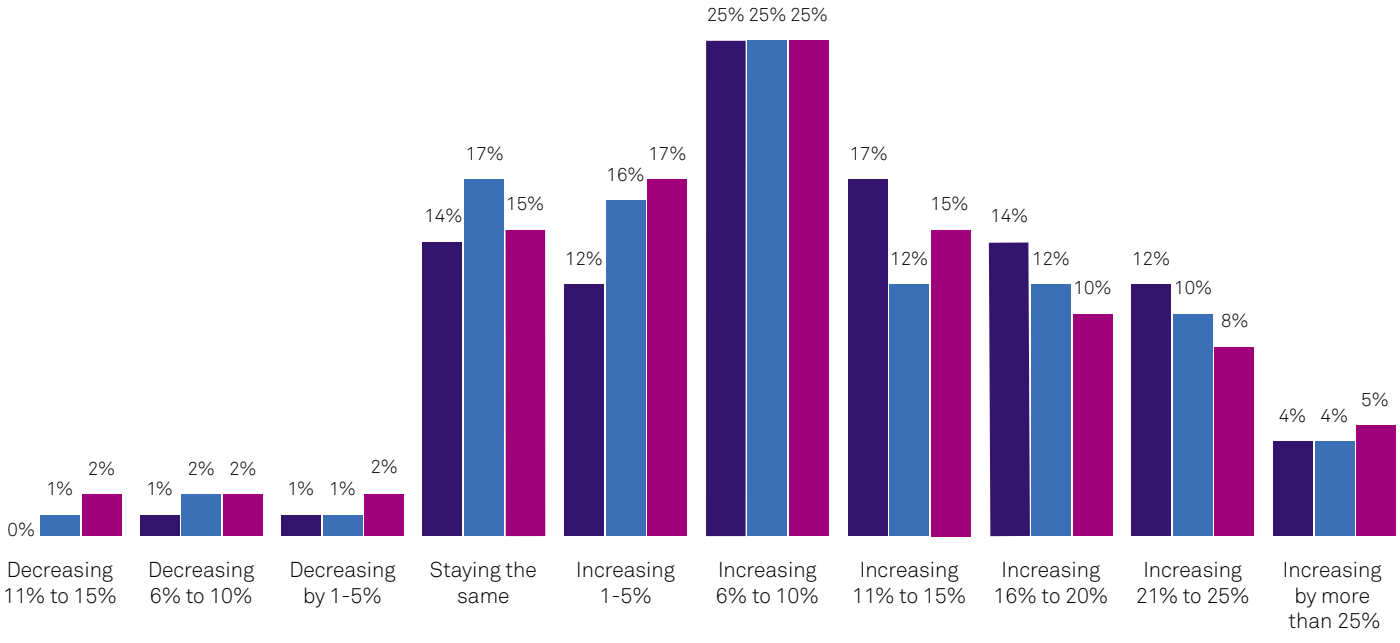
A number of service providers have developed cloud management capabilities to help businesses connect securely to third-party cloud environments, often through standard configurations which are managed by a third-party supplier. Other capabilities are around the identity and access management of users, analytics, usage stats, cost management and compliance controls including the discovery of shadow IT. These solutions will often provide a self-service capability for managing workloads between the premises and multiple third-party cloud environments.

Security Trends and Future Investments

IT and Security Investments

A majority of businesses are combining their cyber and electronic security budgets as these domains converge. Our research highlighted security spending is projected to increase, both in absolute terms in the next 12 to 24 months, but also relative to the percentage of total ICT budget. In Australia, the average security budget (cyber and electronic) was just over A$900,000 per annum.[73]

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

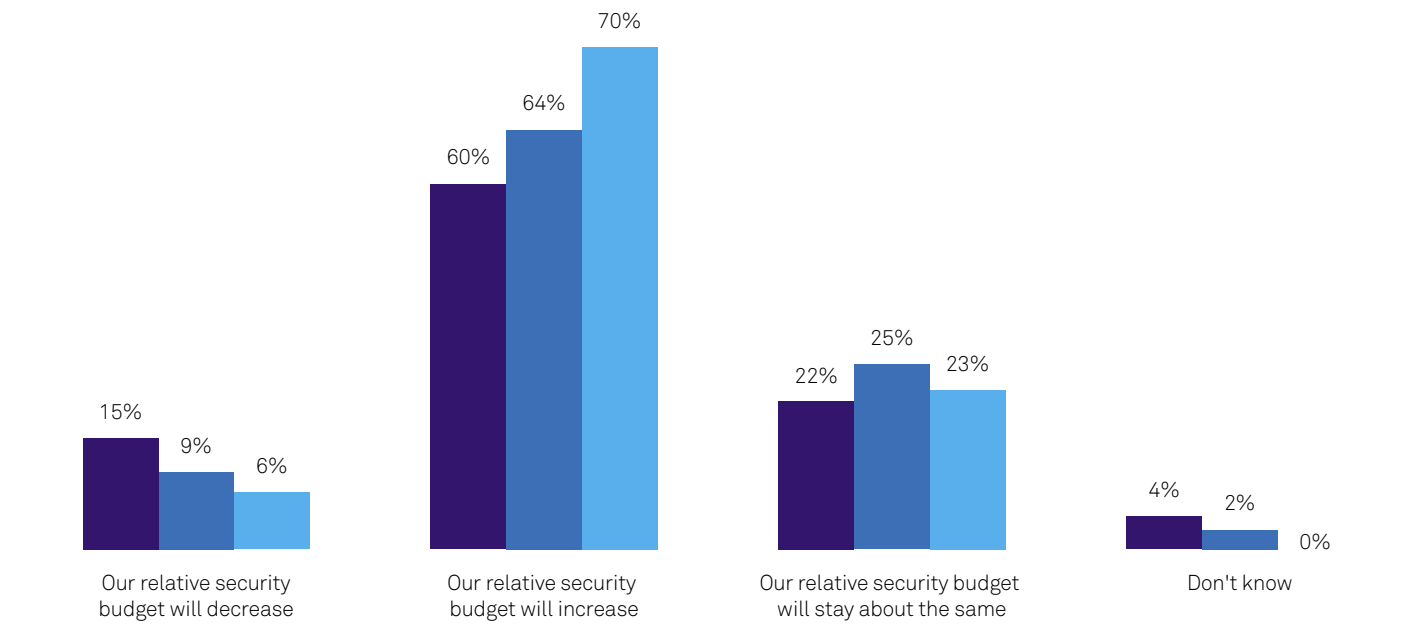


Australia, n=320, Europe, n=503, APAC (*includes Australia), n=795

Australia APAC* Europe

[73] GlobalData IT Client Prospector Database.

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=320; Europe, n=503; APAC (*includes Australia), n=795

Spending Priorities

In terms of security initiatives, our research shows there have been priority shifts year on year. Our 2018 Security Report identified compliance as the most important priority, likely in recognition of the many local and regional laws coming into force within that period. Our 2019 results show that compliance has moved to the eighth ranking within the global results but is still the second highest priority in the Australian results. Global and European respondents are looking at incident response remediation services as their top spending priority, focussing their efforts on areas such as business continuity planning. Meanwhile, APAC and Australian respondents have placed security design and architecture at the top of their respective priority lists. Australian respondents also placed a strong focus on having security delivered as a managed service, moving up to a third place ranking from ninth in the previous year.

Technologies being implemented

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

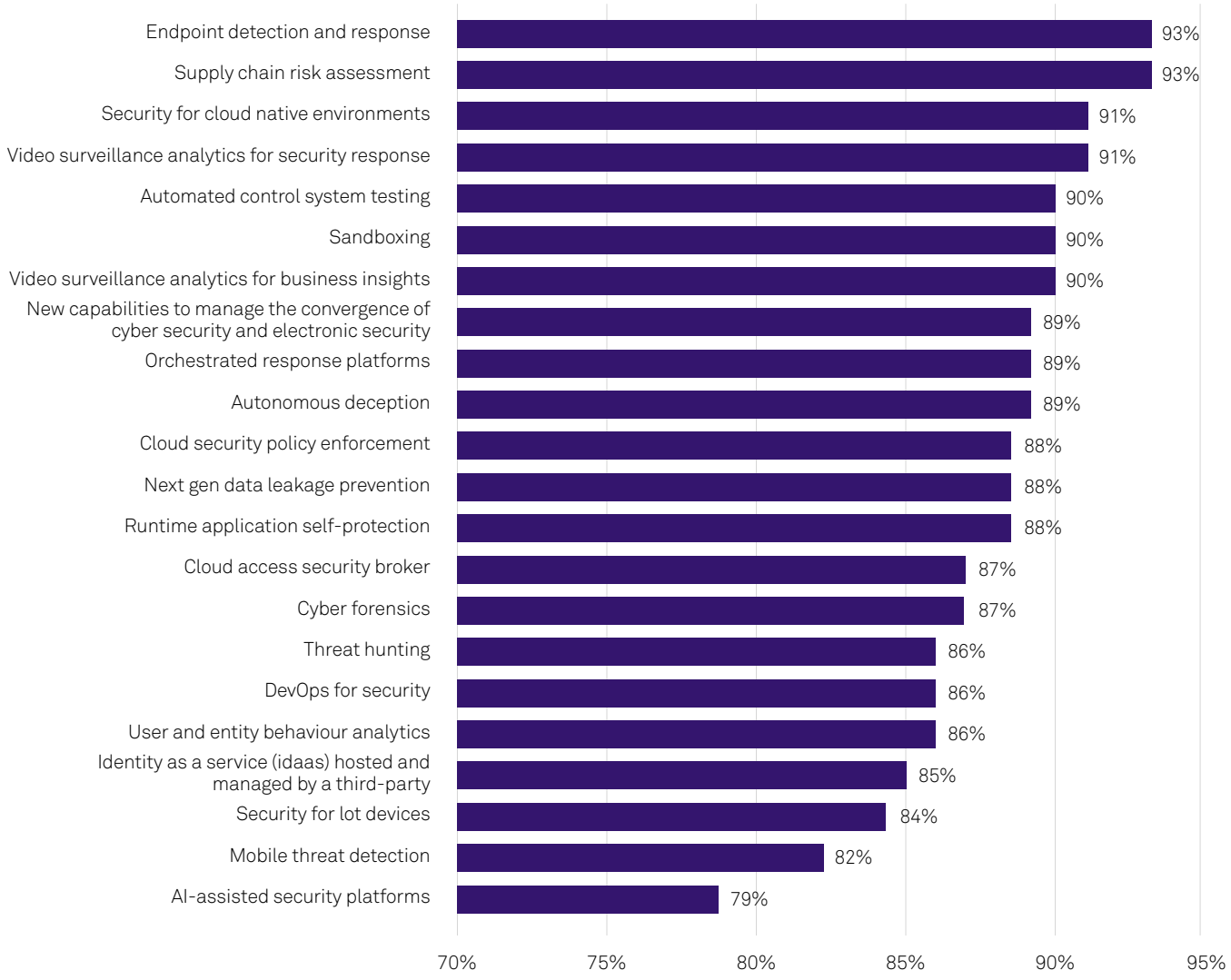
Global, n=1,298; Australia, n=320

Currently using | Trialling/piloting | Considering in the next 12-24 months | Not Considering

Technologies being trialled or considered

In terms of the emerging technologies being trialled, implemented or under consideration in the next one to two years, there are some divergent findings. Our 2018 Security Report found endpoint security was amongst the highest on the list of technologies being trialled or considered, followed by new capabilities to manage the convergence of cyber and electronic security and application testing. Our current research found none of these technologies at the top of the list. There is also some divergence between the European versus Australian and APAC results. The European respondents reported looking at the use of video surveillance for security analytics and business insight, converged video with cyber systems and awareness programs. The Australian and APAC respondents reported sandboxing and autonomous deception technologies, such as honeypots. When including respondents who have implemented, trialled, or are considering conducting trials, then the Australian results are showing a clear preference for these two types of video analytics solutions. Only nine per cent of respondents have no plans to integrate such video solutions.

Q: Which of the following emerging technologies or capabilities is your organisation considering/has your organisation implemented?



Global results, n = 1,298

Outlook

Security budgets will continue to increase in 2019 with many factors driving this increase. There is recognition of new compliance measures, which changes how businesses report and disclose events. When factoring in cyber and electronic security, there is a much broader security landscape. The more devices that become connected, the broader their security footprint becomes. It is also likely to be driven by importance of customer privacy at a time when attacks are more frequent and sophisticated.

In terms of the many established technologies, there continues to be variations by countries and regions. Capabilities such as incident response, compliance and security design and architectures are likely to be in recognition of changes in legislation, new reporting mandates, and the need to involve more stakeholders combined with the real-life threats in the security landscape. Many of the established technologies are interdependent. Some of the variations are also likely to reflect vulnerabilities identified in an organisation's security posture, which also varies by industry.

There are also several emerging technologies. For example, this year the focus on supply chain attacks with techniques like 'island hopping' is suggesting the industry focuses on protecting the supply chain. Likewise, many new capabilities available with mobile endpoint and response, such as threat intelligence, is generating new interest from the market. As businesses adopt a cloud-first mindset, the need to secure applications built for the cloud will follow.

Recommendations

Interoperability and Integration

As security spending increases along with the interest in established and new emerging technologies, organisations should constantly be looking for tighter integration of vendor platforms. A recent Cisco report found that 55 per cent of businesses used more than five security vendors and 65 per cent used more than five products.[74] Multi-vendor solutions will be the norm for most, but steps are necessary to ensure systems work together, are compatible and address security effectively.

Involve Lines of Business in the Plan and Technology Selection

A holistic security plan should support many lines of business, depending on the nature and extent of a potential breach. For example, the theft of intellectual property caused by an employee leaving the organisation should involve human resources and/or legal. Similarly, a breach which impacts the company's brand, reputation and share price should actively involve public relations, investor relations, and marketing, among other departments. Facilities and operations managers need to be involved in electronic breaches. As C-level executives become more involved in security, it is imperative for organisations to be working together. Technology decisions need to reflect the priorities of business owners and any security challenges that might be unique to their department.

[74] Cisco (2018). Annual Cybersecurity Report. Page 63. Retrieved from *https://www.cisco.com/c/en/us/products/security/security-reports.html*

In Summary

This report presents strategies and tactics for helping businesses to achieve their security objectives. From a strategic point of view, we guided readers through the latest challenges of a broadening security landscape which encompass both cyber and electronic security. This groundswell of innovation has been building for over a decade, with the data security footprint extending to many connected endpoints including IoT. The number of stakeholders involved in day-to-day matters are increasing as well as the frequency of reporting to the executive management. Security policies need to be coordinated. The convergence of cyber and electronic opens the door for new technologies and use cases for improving end-to-end visibility.

Despite having strong technology and robust business processes, employees and human error can sometimes negatively impact an organisation. Organisations are accelerating their investments in awareness programs. There are a number of tools that can help businesses to identify their current level of maturity. This can range from non-existent (in the worst cases) towards a more robust metrics-driven framework where behaviours are changed and security becomes engrained in culture (in the best cases). Each phase in the maturity model has a path with specific recommendations along the way to continuously improve security awareness.

No matter how well an organisation is prepared, employees trained and C-level briefed on the topic, businesses need a plan for policies and procedures when an incident occurs. Adversaries are very active and growing in sophistication with each new attack campaign. Adversaries also enjoy inherent advantages over defenders. The section on cyber resiliency discussed incident response, how it can improve security performance, such as reducing dwell times, and what businesses need to consider from threats to the supply chain. We discussed how adversaries are targeting partners and suppliers with weaker defences to reach a primary target and why it is important to apply security policy uniformly.

Compliance is another area we discussed, we covered new rules on disclosure, speed to respond and notify for data breaches. Compliance will likely mean more investment in the ability to automate processes and demonstrate all necessary precautions before the event. Compliance will be a matter of more importance for an organisation with more legislation coming into force. In some markets, it is being linked to customer privacy and opening up a broader debate. This is another high impact area for security strategy in terms of the alignment of people, process and technology.

In terms of tactics, we learned that security is becoming a more difficult day-to-day challenge with organisations seeing incidents more frequently. There are also new variants of malware attacks, such as formjacking and crypto-related crimes, replacing older ones like ransomware campaigns. There are many types of attacks. For example, phishing is present on mobile devices and APTs are pervasive in some key industries, such as financial services. The widespread adoption of cloud and mobility services also presents other challenges on security that need to be addressed.

Businesses are also increasing their security budgets. They are improving their capabilities in areas such as incident response, adhering to compliance requirements and assessing their underlying architectures. Likewise, the realities of a rapidly changing landscape are driving customers to consider new technologies, such as new endpoint detection and response, security for cloud native environments and supply chain risk assessments. The deployment of established and emerging technologies vary widely depending on the country, size of organisation and industry vertical.

There are also some general best practices businesses 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 physical security environments. Its intent is to provide redundancy in the event that one security control fails or is exploited. Layered security examples include: combining the use of web security gateways to block malicious code from being downloaded, whitelisting to prevent unknown executable files from running, and advanced endpoint protection on laptops, mobiles, and servers. 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. Password managers or passphrases should also be considered – with the purpose of enabling employees to select long, complex and unique passwords whilst also allowing them to be memorable.

Architecture Reviews

Architectural reviews should be a constant for planning for a system refresh, considering ways to interconnect physical with electronic or needing a third-party validation. This should also include system and vulnerability scans, penetration testing, and other tests to understand environments, discover vulnerabilities and prioritise fixes. Over the next 24 months, 80 per cent or more of an organisation's employees will be performing the core tasks required for their job from a mobile device. Up to 20 per cent of organisations may have moved their entire IT infrastructure to the cloud, with many employees working from home and other remote locations.[75] Considering the demands placed on IT, architectural reviews conducted regularly can help a business with an improved security posture.

Employee Awareness

Considering security adversaries will often choose the path of least resistance before launching an attack, employees can be the focus of attacks. This can be the benign employee who accidently clicked a malicious link or a person who has been targeted through social media. Organisations that have formal training programs will likely minimise security gaps, incidents and overtime contribute to improved security resiliency. A strong security capability rests on a well-trained and vigilant workforce, and having strong processes and technology capabilities. The weakest link can often be around individual employees.

The Five Knows of Cyber Security

The five things businesses should know to effectively manage risk include: know the value of their data; know who has access to their data; know where their data is; know who is protecting their data; and know how well their data is protected.[76] With these basic practices in place, known as Telstra's Five Knows of Cyber Security, additional measures may also be needed. For example, data classification can help businesses know what they own, identity and access management can ensure the right employees have the right level of access.

[75] GlobalData market estimates
[76] Telstra Five Knows of Cyber Security. *https://www.telstra.com.au/content/dam/tcom/business-enterprise/security-services/pdf/5-knows-of-cyber-security.pdf*

Acknowledgements

Telstra contributions

- Corporate Affairs
- Enterprise Marketing and pricing
- Product and Technology
- Telstra Legal Services
- Telstra Cyber Security

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 help 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 includes:

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 help 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

Carbon Black. · Cisco · Cofense · CrowdStrike · Cylance · F5 · FireEye · FirstWave Cloud Security Technology

Fortinet · McAfee Together is power. · Microsoft · paloalto Networks · Qualys. · Redshield · Symantec · Zimperium Mobile Threat Defense

Contact your Telstra Account Executive
Or call 1300 835 787

Visit telstra.com/enterprisesecurity