TELSTRA

Summary Report

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 breaches of legislation 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, such as malware, are better-known, while other emerging security technologies are not well understood, but 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. Further, this will likely encompass measures to mitigate risk to improve response and recovery objectives.

Last year we discussed the threat of ransomware in detail including 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.

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

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.

Our research found that getting security right from the outset as 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.

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 towards meeting the challenge ahead.

Methodology

Our 2019 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

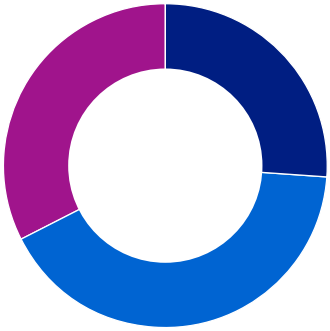
The Broadening Security Landscape

This year, 100 per cent of respondents identified that within their role they were responsible for both cyber and electronic security within their organisation.

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

Global

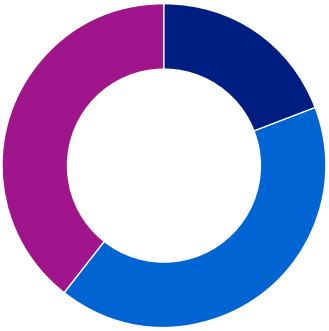
n=1,298



- **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 of the 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.

Cyber Preparation and Awareness

Our respondents identified the greatest risk to IT security is human error – often caused by inadequate business processes and employees not adequately understanding their organisation's 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

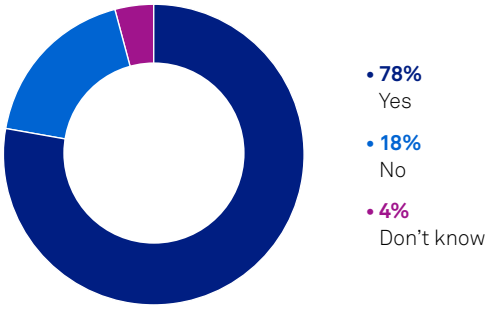
Cyber Resiliency and Incident Response

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

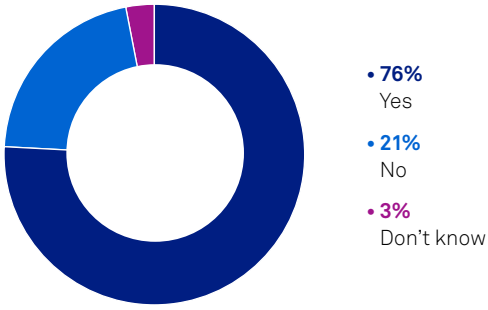
n=1,298



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

Australia

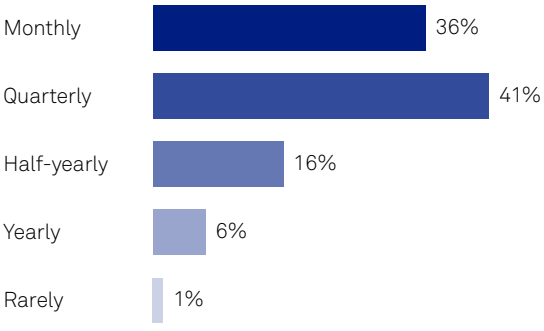
n=320



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

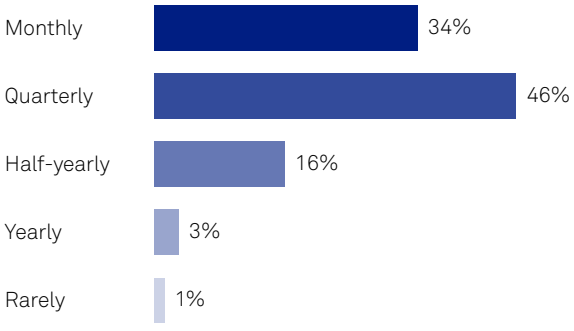
Q: If yes, how frequent is the testing and reviews of your incident response plan?

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.[1] As the frequency and complexity of attacks increase, businesses struggle with challenges such as skills shortages and investment in new technologies.

[1] Ponemon Institute LLC. (2018). The Third Annual Study on the Cyber Resilient Organization. Retrieved from *https://www.ibm.com/downloads/cas/D3RGN4AJ*

Security Challenges and Business Impact

Top challenges, such as the impact of new technologies and ability to reduce dwell times, will continue 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.

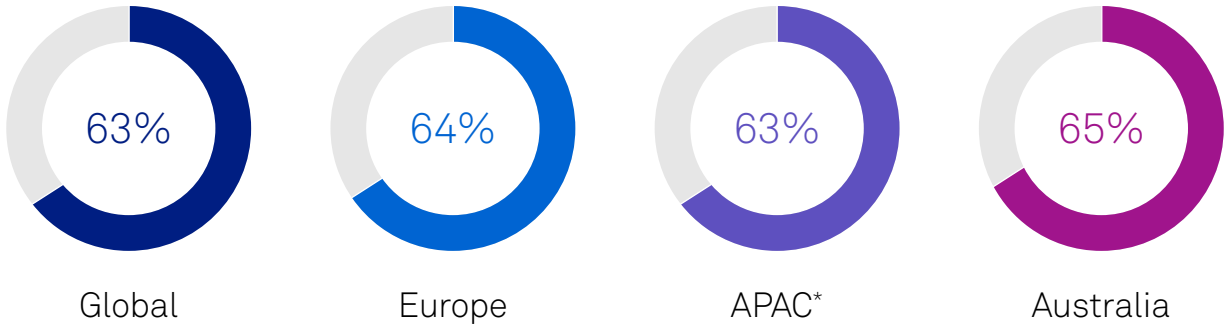
Challenges of Security Operations

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: 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 identify theft. Respondents identified 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.[2] 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.

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

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.[3]

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.[4]

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.

[3] 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*
[4] 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*

Security Threats and Trends

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.

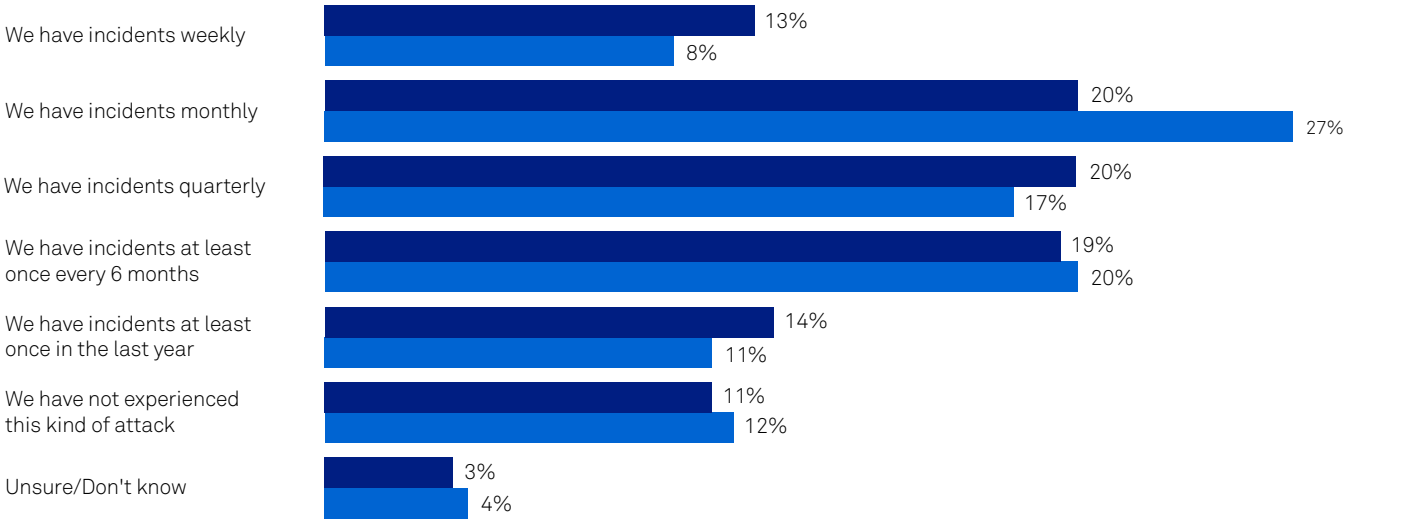
Ransomware and Crypto Mining

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.

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)

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.

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.[5] Research from GlobalData shows the typical business needs to support up to 20 different cloud environments at any given time.[6]

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.

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.

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

Security Trends and Future Investments

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.

IT and Security Investments

A majority of businesses are combining their cyber and electronic security budgets as these domains converge. Our research highlights 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.[7]

Spending Priorities

In terms of security initiatives, our research shows there have been priority shifts year on year. Our 2019 results show that compliance has moved to the eighth ranking spending priority within the global results, but is still the second highest spending 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.

[7] GlobalData IT Client Prospector Database.

In Summary

The challenges of a broadening security landscape 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. 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. Incident response can improve security performance, such as reducing dwell times, and what businesses need to consider from threats to the supply chain.

Compliance is another area we discussed, including new rules on disclosure and speed to respond and notify for data breaches. New compliance requirements will likely mean more investment to improve the ability to automate processes and demonstrate all necessary precautions to prevent a breach from occurring.

Our 2019 Security Report identified 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.

On top of this, 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.

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.[8] 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.[9] 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.[10] 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.

Do you feel in control of your organisation's security?

If not, remember:

- Security is as much about people as it is technology; consider how you're empowering your people to create a strong security culture.
- 'Just in time' isn't a security strategy – understand how your organisation is prepared, know what steps would be taken and how you will communicate in the event of a breach and rehearse!
- Every industry has a different set of compliance regulations – know your regulations, know your approach to achieve compliance and implement strong cyber security hygiene to minimise risk of non-compliance.

[8] GlobalData market estimates.
[9] Ibid.
[10] Telstra Five Knows of Cyber Security. Retrieved from *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 Cyber Security
- Telstra Legal Services

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

Telstra regional office headquarters

Asia

Level 19, Telecom House
3 Gloucester Road
Wan Chai, Hong Kong
T +852 2983 3388

EMEA

2nd Floor, Blue Fin Bldg,
110 Southwark Street
London, SE1 OTA
T +44 207 965 0000

Americas

44th Floor
40 Wall Street
New York, NY 10005
T +1 877 835 7872

Australia

363 Oxford Street
Paddington, NSW
Sydney 2021
T +61 2 8202 5134

Visit telstraglobal.com