TELSTRA

APAC Regional Summary 2019

Telstra Security Report 2019

Contents

Executive Summary

Asia Pacific (APAC) is one the world's largest emerging markets. With a booming population it is home to 60 per cent of the world's megacities, (defined as those with populations that exceed 10 million people). This is likely to remain the case into 2025, driven by population growth and urbanisation in China and India especially.[1] The region is home to a large millennial population accustomed to using mobile devices for everyday activities such as online shopping. There were over 2.5 billion smartphone subscriptions in APAC at the end of 2018, with 21 per cent of APAC residents using a mobile device to access financial services.[2]

Security attacks in the region are also pervasive. A 2018 report from FireEye found APAC based customers were twice as likely to experience multiple security incidents, from multiple attackers, compared to customers in Europe or North America.[3] Further, when an APAC organisation experiences a significant attack, the chance of experiencing another attack in the following year is more than 90 per cent.[4] Despite the risks, security is not preventing businesses determined to provide customers with personalisation and choice.

The Telstra Security Report 2019 highlighted that two in five APAC respondents believe that, 'security is essential for customer experience'. This view is common in the utilities sector and echoes loudest in Hong Kong where three in five (63 per cent) respondents agree. Improving customer experience and the ability to demonstrate it as a market differentiator is becoming more important across the board. Customer experience is also driving new requirements, such as the ability to deliver personalised offers, measure each engagement and all underlying touch points. APAC businesses, especially in the retail and financial services sectors, continue to invest in cloud and mobile technologies as part of a broader digital channel strategy.

There are many potential use cases for artificial intelligence in areas such as anticipating the next best actions. However, 63 per cent of APAC respondents reported their business has been interrupted in the past year by a security breach. When asked what their top security concerns were, 34 per cent of APAC respondents stated it was the potential loss of customers. Additionally, we saw more focus from businesses on protecting their customer's privacy, with 46 per cent of APAC respondents reporting an increased concern.

Security breaches are a challenge for any organisation and even more so in some industries such as financial services, manufacturing, and retail, which are disproportionately targeted. This report looks at the steps businesses can take to improve incident response and decrease remediation times. It highlights some of the awareness programs which are being implemented by respondents to better educate employees on the risks associated with cyber security. Employee education programs can help increase an organisation's defences against attacks and in turn, reduce the efficiency of attacks.

Over half (51 per cent) of APAC 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. 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.

In our 2019 APAC Regional Summary we also discuss how the landscape is broadening to converge cyber and electronic security into a single domain. This year there is evidence that the visibility, frequency of meetings, concern about customer privacy, and overall executive engagement around security is increasing. As organisations digitally transform, this is welcome news.

[1] GlobalData Predictions (2018). Retrieved from *https://www.globaldata.com/60-worlds-megacities-will-located-asia-2025-says-globaldata/*
[2] Ibid.
[3] FireEye (2018). M-Trends (2018). Retrieved from *https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html*
[4] Ibid.

Methodology

The Telstra Security Report 2019 provides research-based insights into the current security landscape to support you in mitigating and managing security risk. Whether you are 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 framing strategies for preparedness and incident response.

We engaged research and analysis firm GlobalData to interview professionals responsible for making IT security decisions within their organisation to obtain a number of key insights on a range of security topics. Our report also draws on the analysis of security information and data gathered from our 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 examine 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's online research in November and December 2018 provided 1,298 responses across 13 countries in total. 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. The respondents reported knowing their organisation's annual security budget and having either some influence or complete control over the security investment.

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

Asia Pacific respondents represented businesses of all sizes - from 50 employees to as large as 5,000-plus across 15 industry verticals. These verticals include broadcast and media, banking, financial services, and insurance (BFSI), mining, utilities and resources, government and public sector.

Position Titles

C-suite executives including CEO, CFO, CIO, COO, CTO, CISO and CSO accounted for 20 per cent of the global respondents, and 16 per cent in APAC. The remainder were in IT and security management roles. The single biggest role represented in the survey was the IT manager, at 34 per cent of the respondents.

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

Convergence of Cyber and Electronic Security

Underpinning the broadening of the security landscape is the convergence of information technology (IT), i.e. systems for data-centric computing; with operational technology (OT), i.e. 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, mining, and utilities. Further to these, OT is extending to other areas such as connected devices. These include building automation systems, video surveillance, heating, ventilation, and air conditioning (HVAC) systems, energy management, and health and safety systems, all of which are used in most organisations. Many of these systems never connected to an outside network historically and security was not a major focus. The Internet of Things (IoT) starts with connectivity being deployed increasingly to support a myriad of use cases – typically to improve operational efficiency or create new revenue streams. Like OT, the issue of security in IoT is often not discussed at the outset.

In the not too distant future, this convergence of technology will drive even more use cases in 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 converging OT/IT with IoT will be especially important for smart cities or transforming the manufacturing sector, for example, in APAC with connected factories to improve the balance of trade. This convergence speaks to the integration of cyber and physical systems, sector wide automation and real time data exchange.

The benefits of this convergence will need to be balanced with the possible security risks. A larger connected landscape can also increase the attack surface. Some of the common threats to both include:

- Backdoors. Over time, many security attacks have occurred through connected devices. This can include targeting connected HVAC systems or IP cameras as a backdoor into an organisation's network to steal corporate data. 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.
- Ransomware. While ransomware is a pervasive type of malware in the IT context, it has also surfaced in other areas such as building automation systems and industrial control systems. In these environments, this type of malware can function by locking an underlying boot system, rendering connected devices or sensors inoperable until they are restored either by a back-up, if available, or payment of a ransom in hopes of restoring operations. Beyond payment of the ransom, businesses can face downtime, related repercussions in operations, financial losses or damage to property or assets.
- Botnet Attacks. An adversary can gain access to connected devices, such as an IP surveillance camera through simple to crack default passwords. Adversaries have used malware strains to scan for open Telnet or SSH ports, discover IoT devices behind them, and perform brute-force attacks using common default usernames and passwords, before sending the payload. The adversaries can then install malware on the devices, program them for future use, or enlist them in a global army of bots with minimal investment. Mirai was an example of a botnet used to conduct one of the largest distributed denial of service (DDoS) leading to other variants, such as BrickerBot, Hajime, and Persirai.

[5] Cisco (2018). Cisco 2018 Annual Cybersecurity Report. Page 41

Security Reporting, Accountability and Escalation

This year's research indicates that in the event of a security breach, the ultimate responsibility in both the cyber and electronic security domains is similar.

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

Ultimately held responsible for an incident (top 5 nominated)	
Cyber Security	
IT Department	**48%**
CIO	**28%**
Employees involved	**22%**
CEO	**21%**
CISO	**20%**
APAC results, n=795	

Ultimately held responsible for an incident (top 5 nominated)	
Electronic Security	
IT Department	**43%**
CIO	**25%**
Employees involved	**20%**
Facilities Manager	**20%**
CEO	**19%**
APAC results, n=795	

When asked who is ultimately responsible in the event of a security breach, APAC respondents point to the IT department, the CIO, and employees involved. The CEO in both categories is held nearly as responsible as the employees involved. This is more evidence to suggest security is a board level issue. In terms of notification when there is a cyber or electronic breach, the CIO/IT department is the first to be notified, followed by the CEO. Nearly half of all board members and senior management are reportedly briefed on security incidents on a 'weekly or monthly' basis as indicated for cyber as 47 per cent and/or electronic at 46 per cent. This is an increase from around 40 per cent last year for this level of reporting frequency for both domains.

Security Considerations for Retail, Banking and Financial Services and Manufacturing

Security attacks are prevalent across businesses of all sizes. They continue to happen to organisations around the globe. Attacks are more frequent this year and don't seem to discriminate in terms of the type or size of business they are targeting. However, there are precautions businesses can take based on the dynamics of an organisation's industry and threat exposure. Understanding the potential attacker, including their motives and possible tactics can help to improve overall security posture and reduce the likelihood of a successful attack or data breach. The following section considers potential threats for retail, banking, financial services and manufacturing in APAC. The findings were gathered from survey results, partner contributions and third-party sources.

Retail

Retail and personal services such as hospitality, travel, gaming and entertainment can be prime targets for adversaries because of the wealth of customer data and personally identifiable information (PII) they hold. Within the past year, several high-profile high-street and consumer brands have experienced breaches. The breaches included instances of credit card compromise and stolen customer data.[6] When customer data is infiltrated, it is common practice for hackers to enrich data with information from other sources, such as social media, to create profiles which can be sold via the Dark Web. Once on these underground marketplaces, it can be resold to any number of adversaries for any number of purposes, such as identity theft, ransomware attacks or phishing campaigns.

Retailers tend to invest significantly in digital channels. This helps the sector capture customer spend as it shifts from physical stores to mobile and online platforms. Embracing omni-channel solutions are table stakes for APAC, especially for any traditional bricks and mortar retailer competing with online electronic retailers (e-tailers) such as Zalora, Flipkart or Lazada. Most retail brands are building out offline and online capabilities to have an integrated 'clicks and bricks' retail strategy.

In China, Alibaba rolled out over 100 digital stores, known as Hema Supermarkets, as part of their retail concept providing shoppers with online and offline digital stores.[7] Shoppers are prompted to download the app and use a mobile phone for in-store experiences (e.g. personalised recommendations, mobile payments). The company found omni-channel customers spend twice as much as shoppers that shop purely online or offline.[8]

Retailers of all varieties, including suppliers and partners, will continue to invest in digital platforms and payment technology. This is likely to take the form of working within an ecosystem. Mobile apps, for example, are important to glean customer insights in areas such as spend patterns, location and loyalty. A 2018 combined data report from IntSights and Riskified found a 297 per cent increase in the number of fake retailer websites designed to "phish" for customer credentials.[9] Retailers will therefore need to continue to manage the security risks associated with online shopping and ensure a balanced approach.

[6] 2018 Data Breaches: The List No One Wanted To Make (2018, 31 December). Retrieved from *https://www.pymnts.com/news/security-and-risk/2018/data-breach-user-account-card-retail-hack/*
[7] Alibaba says New Retail strategy is paying off as Hema shopper data shows bigger average spending (2018, September 18). Retrieved from *https://www.scmp.com/tech/enterprises/article/2164651/alibaba-says-new-retail-strategy-paying-hema-shopper-data-shows*
[8] Ibid.
[9] Teplow, N. (2018). Retail and Ecommerce Threat Landscape Report. Retrieved from *https://www.intsights.com/blog/introducing-the-retail-and-ecommerce-threat-landscape-report*

Phishing is one of the easiest and most efficient ways that adversaries use to get a constant stream of stolen credit cards. Whether it's through email, mobile-phishing, social media or messenger applications, the delivery options are endless, and so are the number of retailers available to impersonate online.

Our research found that 60 per cent of APAC respondents from the retail sector have experienced a breach in the past year, which significantly impacted their business operations. Some of the most common types of attacks reported include unintentional employee actions, such as human error and inadvertently triggering malware attacks. Retailers are a major target for data theft, as they have access to lots of data about their business operations, their employees, their suppliers and their customers. In the past, adversaries have also targeted digital payment processing systems.

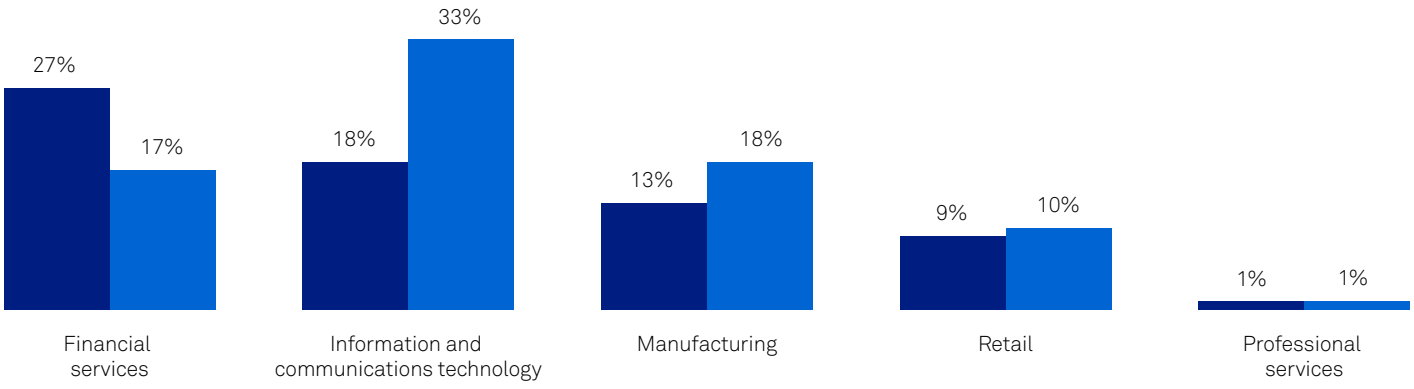
While only 50 per cent of APAC respondents reported having a regular occurrence of DDoS attacks, they are a constant threat for any retailer with a significant online presence, especially during peak seasons. DDoS, as well as other forms of attacks like ransomware, can also attack physical systems (e.g. POS machines, video cameras, kiosks, etc.). Attacks on physical systems, such as digital signage systems, can also be problematic for any retailer considering new connected concepts. Ambient commerce combines physical space or traditional retail environments with technology. One example is to allow users, for example, to select and pay for goods without the need for traditional cash registers.

Banking Financial Services and Insurance

The banking, financial services and insurance (BFSI) industry continues to be a prime target for many hacker and adversary groups. Many are looking to seek financial gain. Research from Cylance found that over the past two years, the financial sector continued to be at the top of the hit list for attackers spanning the full range of sophistication and capability.[10] Typical methods include everything from low level financial fraud targeting an individual customer (e.g. account fraud, malware or web application attacks) to more sophisticated malware and web application attacks, such as nation state backed campaigns, which tend to be the most damaging.

Similarly, a recent report from IBM found that financial services was the most targeted industry for the second consecutive year. This sector experienced the highest volume of security incidents in 2017 and the third highest volume of cyber-attacks.[11] The IBM report also found that more than 76 per cent of the activity involved injection attacks and nearly 10 per cent involved reconnaissance activity.[12]

Top five most frequently targeted industries - Percentage of security incidents and attacks in 2017



Source: IBM

Attackers are committing direct monetary theft from bank accounts by using phishing and credential stealing malware, as well as running malicious code to intercept online transactions.

Malware Families in the Financial Sector

Unique to the BFSI industry is the number of malware types that specifically target the banking sector. Some of these major malware types include Emotet, which is a modular banking Trojan attack. Emotet primarily functions as a downloader or dropper of other banking Trojans to further spread malware throughout a system or network. In 2018, there were a number of incidents recorded with Emotet enabling other strains such as IceID, Trickbot, and Qakbot[13]. A report by US-CERT found Emotet 'continues to be among the most costly and destructive malware' inflicting an average clean-up cost of USD $1 million after each incident.[14]

While the primary danger with this type of malware is theft or loss of data, there can also be a number of secondary events, such as opening backdoors to ransomware or crypto-related malware. The perpetrators behind the most sophisticated malware families are described as 'highly skilled and well resourced', constantly updating their tactics and paying close attention to the payloads themselves.[15] These adversaries are often planning second and third stage activities.[16]

[10] Financial Threat Trends – Cylance research for Telstra Security Report 2019.
[11] Security incident is often defined as an event that compromises the integrity, confidentiality or availability of an information asset as well as the associated security policies protecting these assets. Not all security incidents results in confirmed attacks.
[12] IBM Security (2018). IBM X-Force Threat Intelligence Index 2018. Notable Security Events in 2017, and a look ahead. Retrieved from *https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=77014377USEN*
[13] Financial Threat Trends – Cylance research for Telstra Security Report 2019.
[14] US-CERT (2018). Alert (TA18-201A) Emotet Malware. July 20, 2018. Retrieved from *https://www.us-cert.gov/ncas/alerts/TA18-201A*
[15] Financial Threat Trends – Cylance research for Telstra Security Report 2019.
[16] Ibid.

Manufacturing

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. Characterised by pervasive connectivity and the ability to collect vast amounts of data and communicate with other processes and systems – both cyber and physical in real-time. As these systems converge, they will usher in new possibilities with 3D printing, digital twinning, AR/VR, and sensor technology to deliver dramatic improvements in productivity and visibility across factory floor and supply chain operations. Furthermore, many security use cases are emerging in areas such as predictive maintenance. Other possibilities include the wider use of artificial intelligence (AI) for humanrobotic interaction (HRI) models to improve productivity and operational efficiencies in factory automation.

Manufacturing is critical in the ASEAN region, it represented US$670 billion in 2018 or 21 per cent of the region's Gross Domestic Product (GDP) with more than one-third coming from Indonesia alone. By 2018, it is expected to contribute US$1.4 Trillion to the region's economy.[17]

Due to the increasing reliance on digital data, the manufacturing sector also makes for fertile ground for cyber adversaries. There are many points of potential entry when considering the supply chain complexity including third-party suppliers. Within manufacturing, there are common attacks such as business email compromise (BEC), ransomware or insider threats, which are prevalent in all sectors. There are also vulnerabilities unique to this industry. The integration of cyber and physical systems expands an organisation's attack surface as connectivity extends to more devices, sensors, and embedded systems. OT, such as industrial control systems, is found in critical infrastructure including areas such as process manufacturing. Traditionally, OT has not connected to central IT systems or outside networks and only now is security a priority.

As both types of systems connect and converge, it is important for security to be considered from the outset. Non-traditional connected systems have many common vulnerabilities with classic IT systems. In both environments, there is the potential for malware to disable delicate equipment or reduce visibility of delicate processes from the control room (depending on the attack). A connected endpoint in the network (e.g. IoT or OT) has been used as a backdoor in past breaches to access sensitive corporate data on the network. In cases where machinery is the focus of an attack (as opposed to data in IT systems), the damages can be dire. The consequences could be personal injury, and/or physical damage to equipment and property depending on the type or severity of an attack.

OT, such as industrial control systems, have operated independently of IT systems for many years and are now connecting to outside networks for the first time. It also includes IoT devices, which connect, communicate and share data with other sensors, objects and things (depending on the use case). These connected systems have many common vulnerabilities, such as the potential for a malware attack or being used as a backdoor to infiltrate data from IT systems. As manufacturers continue to automate many processes to drive efficiencies, this has to be done in a secure manner.

[17] AT Kearney (2019). Accelerating 4IR in ASEAN: An Action Plan for Manufacturers (2019). Retrieved from https://www.atkearney.com/documents/20152/1849225/Accelerating+4IR+in+ASEAN.pdf/c1fd001b-a5cb-4a96-c73b-e666c0b88692

Consider, in a hypothetical scenario, an automotive manufacturer having a malware outbreak with robots on the assembly line leading to the mass production of a defective part and a major recall. A 2017 report by TrapX highlights cases where malware has been shipped pre-installed in hardware, software and even in the firmware logic of new semiconductor chips.[18] There are many moving parts in the supply chain. This can include the sourcing of raw materials, the assembly, fabrication and production of finished product to the transport, storage and last mile distribution.

A manufacturer could therefore have potentially hundreds of suppliers, partners and external contractors. In a security context, this can equate to multiple points of vulnerability at any point in time. It is, therefore, an imperative for supply chains to be secure at every point possible. Our research shows that 31 per cent of APAC respondents have implemented supply chain risk assessment solutions. Twenty nine per cent of APAC respondents are conducting evaluations/trialling and 29 per cent are considering these emerging technologies over the next 12 to 24 months.

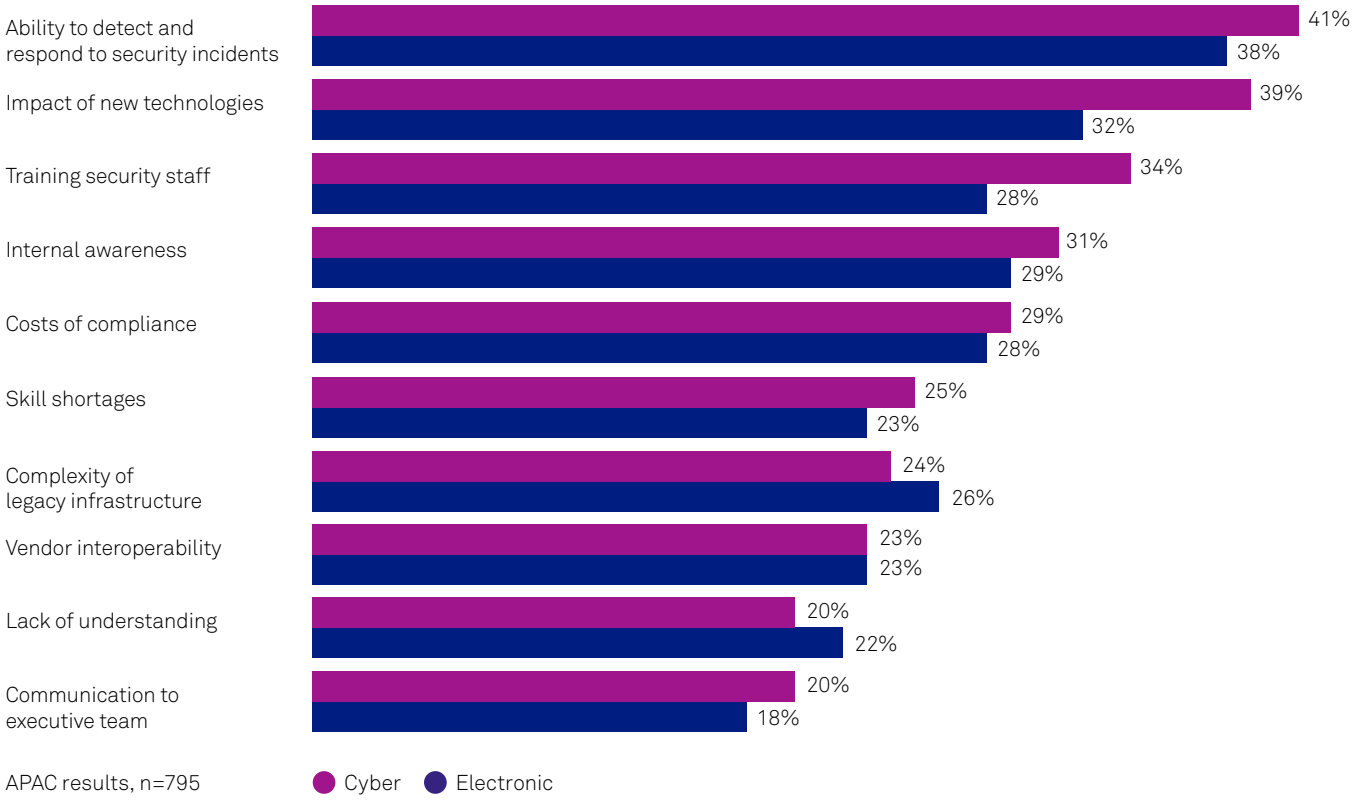
[18] TrapX Research Labs (2017). Anatomy of an Attack. Zombie Zoo. Weaponized Malware Targets ERP Systems. Retrieved from *http://trapx.com/wp-content/uploads/2017/08/AOA_Report_TrapX_AnatomyOfAttack-ZombieZero.pdf*

Security Challenges

Our 2019 Security Report identified the top two global cyber and electronic security operations challenges were: the 'ability to detect and effectively respond' to security incidents in a timely manner and the 'impact of new technologies'. This holds true for APAC organisations.

There were however some noticeable differences between industries in the region. The most frequently nominated challenge for businesses in the retail industry was the 'training of security staff'. Respondents from the health care sector most frequently highlighted 'skill shortages' as a concern, while those surveyed from construction industry highlighted the 'complexity of legacy infrastructure' as their most common challenge.

Q: What are the major challenges with regard to Cyber and Electronic Security Operations?



In APAC, 40 per cent of respondents agree 'security is essential for customer experience'. This sentiment is the strongest in industries such as media, professional services, and local government.

Cyber Preparation and Incident Response

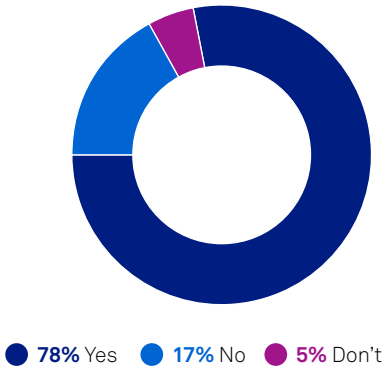
Cyber security preparedness is built on technology, business processes and people. Getting the balance right is essential for building cyber resilience. The problem is that although employees can be a company's best asset, they can also be the greatest IT risk when it comes to security. While there are many avenues of attack, such as system configuration or poor coding, cyber criminals can often specifically target employees as an attack vector, based on their lack of knowledge of security best practices.[19] Not all employees are aware of security risks.

Our respondents identified the greatest risk to IT security is human error – vulnerabilities are often caused by inadequate business processes and employees not adequately understanding their organisations' security posture. This type of insider threat has the potential to cause harm to both an organisation's reputation, and its bottom line. Our report finds that more businesses are focussing on security awareness programs, among other areas, through formal education and training of employees.

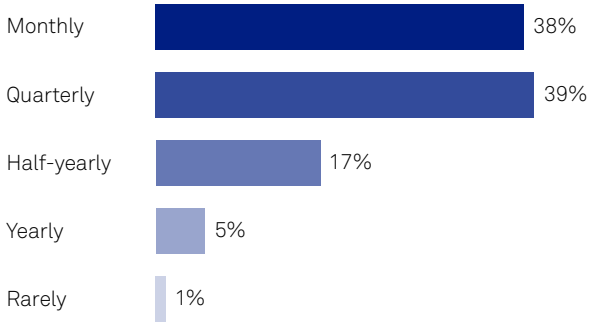
Security awareness programs can help to prevent incidents from both types of employees. A 2018 report from the SANS Institute argues that companies which have mature practices, that have been able to improve security competences and, over time, change behaviour, are in a much stronger position to avoid security incidents coming from employees.[20] Likewise, businesses that have little or no awareness programs are the most vulnerable.[21]

In terms of incident response, our research highlights that on average more than three out of four APAC respondents (78 per cent) report having an incident response plan. This is consistent with the APAC findings from our 2018 Security Report. Hong Kong, Taiwan and the Philippines were the most likely markets to report having an incident response plan in place. Of those that have an incident response plan, over 70 per cent of respondents report testing and reviewing their incident response plan at least once a quarter.

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



APAC (including Australia) results, n=795



n=620 (subset)

[19] 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*

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

[21] Ibid.

Emerging Technology

When it comes to emerging technology, APAC respondents report implementing, trialling or considering endpoint detection and response, supply chain risk assessment, and security for cloud native environments as the top three.

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

APAC Results (top 3 nominated)	
Endpoint Detection and Response	**94%**
Supply chain risk assessment	**93%**
Security for Cloud Native Environments	**92%**

APAC (includes Australia) results, n=795

Endpoint Detection and Response

Given the strong cloud and mobile first mindset in many APAC organisations, endpoint detection and response (EDR) is a strong fit for future security requirements. Technology challenges are moving from perimeter-based solutions to capabilities that reflect cloud and mobile first architectures. Cyber-attacks are pervasive and polymorphic. Having EDR that uses threat intelligence platforms, threat hunting solutions, and incident response tactics such as investigation, containment and remediation are becoming topics of conversation in the region for improving endpoint visibility. Our report findings validate these sentiments. While APAC respondents reported human error as the greatest risk to IT security; cloud and mobile are noted as the 'biggest source of concern' related to security attacks.

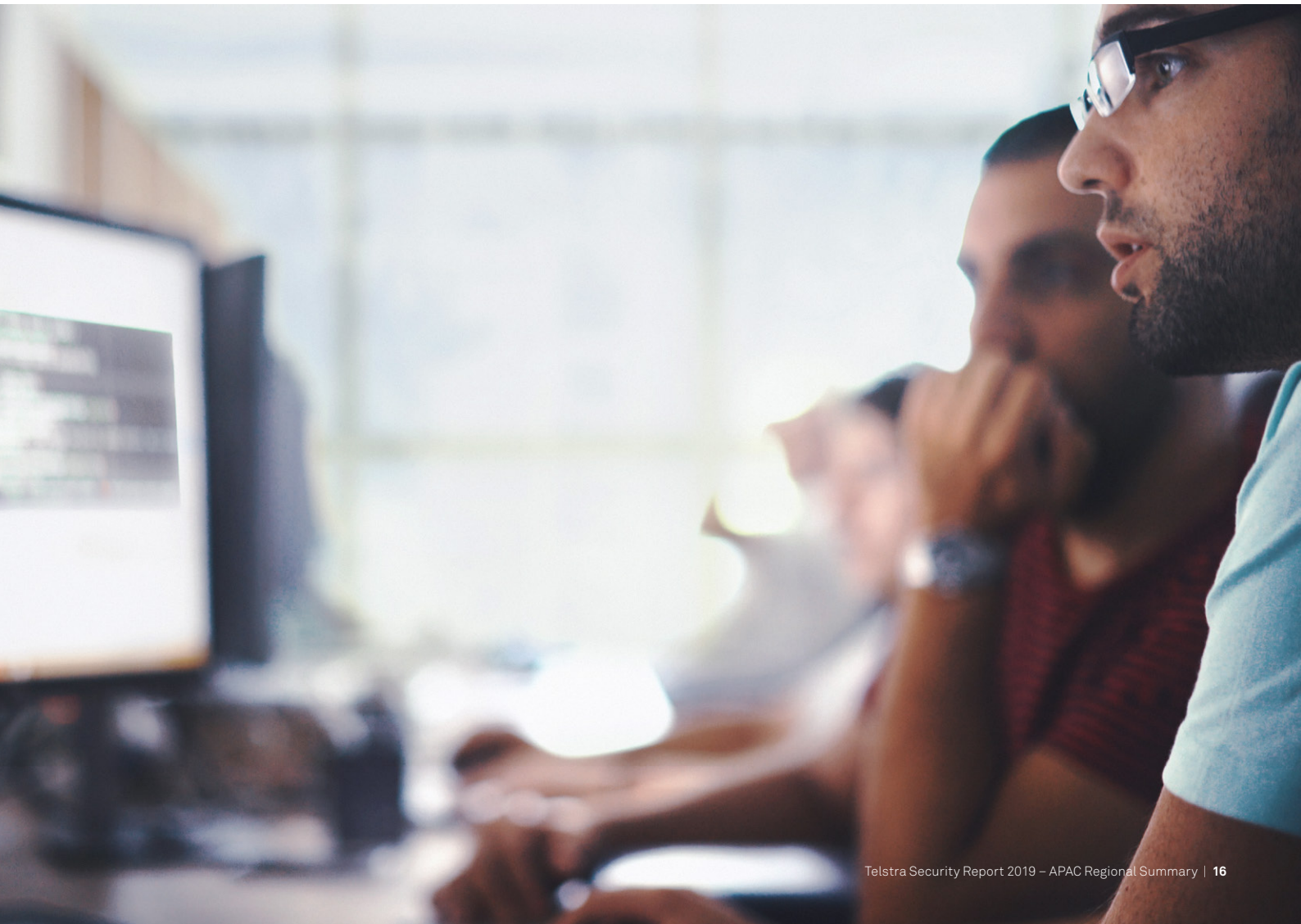
Supply Chain Risk Assessment

An increasing number of attacks are affecting multiple organisations such as affiliates and partners within a supply chain. APAC organisations are looking at ways to manage security at all stages. In the past year, there have been more attacks where a hacker breaches a third-party with weaker defences as a backdoor for its primary target which is likely to have stronger defences. These attacks are often carried out through privilege escalation. An example of this scenario is where a hacker uses one set of hacked credentials to allow for incremental hacking of other credentials, which possess greater system privileges. The sentiment for supply chain risk assessments was the highest in Taiwan with only one per cent of respondents not considering supply chain risk assessments. Sentiment was also strong in Indonesia, the Philippines, Singapore, and Hong Kong.

Security for Cloud Native Environments

Organisations located in APAC are continuing to modernise their application estate and are in the process of migrating to the cloud. As part of this journey, these organisations will turn to containers, micro-services, and in some cases serverless computer services which are introducing new tooling and processes such as continuous integration and continuous delivery (CI/CD). The idea for many businesses, as they transition more workloads to the cloud, is to write scalable code without considering the underlying infrastructure. The benefit from this approach is to achieve the speed to deploy new services and faster software development lifecycles. The end state objective is to create an IT organisation which is highly responsive to business requirements. That said, the desire for, and benefits of speed and agility need to be balanced against the appropriate security priorities. A recent report from F5 Networks found that nearly half of organisations they surveyed with a digital transformation initiative are having difficulties. Their challenge is in applying consistent policies to distributed applications among multiple cloud platforms.[22]

[22] F5 Networks. (2019). State of Applications Services 2019 Report. Retrieved from *https://www.f5.com/state-of-application-services-report*



In Summary

This 2019 APAC Regional Summary identified strategies and tactics that can be used to help businesses 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. With a broader landscape, the challenges of managing security, combined with the perceived risks associated with having a major breach, will continue to intensify. Sixty three per cent of APAC respondents reported a breach that interrupted their business in the past twelve months.

In 2019, adversaries will likely continue to increase their level of sophistication, build out new threat vectors and turn to the latest technologies, such as cloud and artificial intelligence, to be more effective. Because hackers are getting more sophisticated and opportunistic, businesses are upskilling their staff through formal education, training, and awareness.

At the same time, the demands from employees and customers for personalised experiences will continue unabated. Businesses looking to attract the best talent will need to ensure employees are equipped with the best technology tools. Cloud and mobile technologies are highlighted by APAC respondents as the two most pressing sources of concern related to security attacks in our survey. Nevertheless, adoption of both technologies will continue.

Ultimately, our research tells us that while these threats are real, security is about managing business risk on an ongoing basis. With the right balance, businesses can be simultaneously agile, innovative, compliant, and secure.

Here are some general best practices APAC business should consider:

Multi-layered Defences

With the number of threats that can penetrate IT systems, this approach, also known as defence in depth, relies on multiple layers of security controls throughout ICT and 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.[23] 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.[24] 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.

[23] GlobalData market estimates
[24] 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