Summary of Telstra Security Report 2018

By Neil Campbell, Director, Global Security Solutions at Telstra Corporation Limited

A year in review for security

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

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

Unfortunately, the risk of cyber attack is all too real. In 2017 cyber attacks not only resulted in the loss of intellectual property (IP), but impacted share prices and customer confidence, brought the threat of litigation, and caused businesses public embarrassment.

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

An overview of the Telstra Security Report 2018

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

Our 2018 Security Report is more comprehensive than ever before. We interviewed over 1,250 professionals with decision making responsibilities in their organisation for matters of security, three times more than our 2017 report.

We expanded our geographic reach to 13 countries, once again including Australia and Asia, but also Europe and the UK. We also asked respondents specific questions about electronic security, including their challenges and budgets, not just traditional cyber security.

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

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

However, other findings are more concerning. Ransomware is on the rise and is becoming increasingly targeted. Respondents reported more ransomware attacks in this year's survey than any previous years and 31 percent of Australian respondents whose business has been interrupted due to a security breach in the past year are experiencing these attacks on a weekly or monthly basis.

Cyber preparedness and incidence response

Security awareness continues to increase and our research indicates this is driving the adoption of certain frameworks, such as security audits, risk assessments and compliance tools through to continuous end user training.

Our research found that Australian, APAC and European companies tend to focus more on conducting security audits as their top priority, which is consistent with the results from our 2017 report.

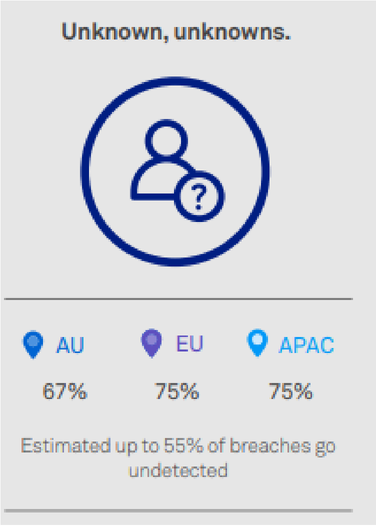
The 2018 data indicates a trend whereby businesses are undertaking a number of security initiatives. There is no area being excluded per se this year, there are only varying degrees of priority.

How often do breaches occur?

Unknown, unknowns: 67 percent of Australian businesses estimated that the number of breaches that had gone undetected in the past year was up to 55 percent. Within this figure, 28 percent of Australia respondents estimated this to be less than 10 percent which is consistent with the European results of 29 percent. In APAC, 35 percent of respondents estimated the number of successful undetected breaches to be less than 10 percent.

Known, unknowns: The study also shows that nine percent of Australian business, six percent of APAC and seven percent of European organisations indicated they did not know the number of successful, undetected data breaches.

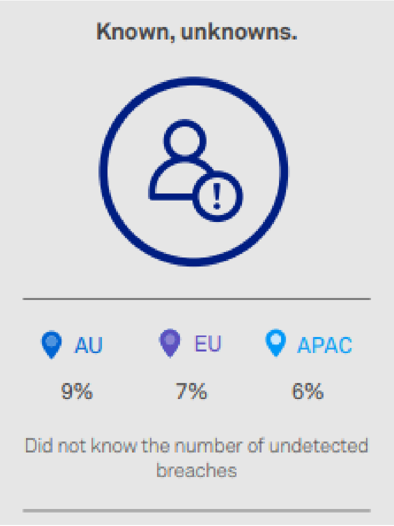
Known knowns: Approximately 75 percent of Australian businesses (and 81 percent of the APAC and 83 percent of European respondents) estimated that up to 55 percent of incident alerts in the past year had gone unanswered. Within this figure 27 percent of Australian businesses, 33 percent of APAC and 31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



Unknown, unknowns.

AU	EU	APAC
67%	75%	75%

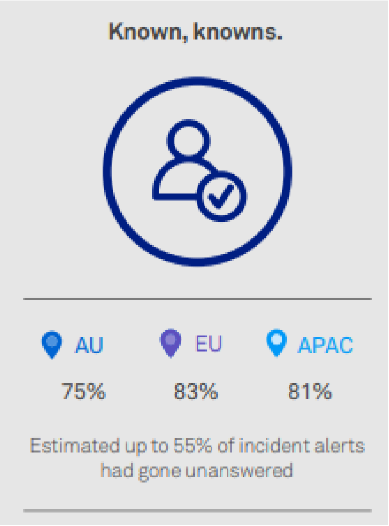
Estimated up to 55% of breaches go undetected



Known, unknowns.

AU	EU	APAC
9%	7%	6%

Did not know the number of undetected breaches



Known, knowns.

AU	EU	APAC
75%	83%	81%

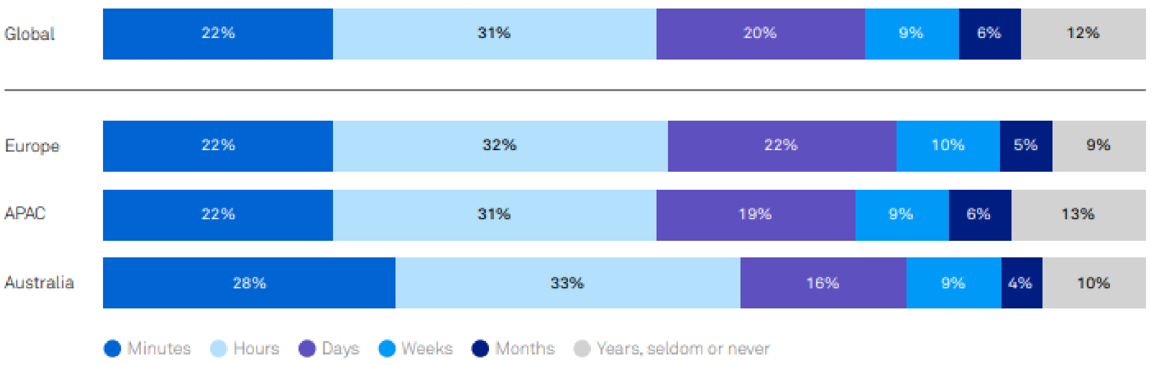
Estimated up to 55% of incident alerts had gone unanswered

Incident response and dwell times

61 percent of data breaches were discovered in minutes or hours by Australian respondents. This compares to 53 percent in APAC and 54 percent in Europe. However some 29 percent

of the security breaches in Australia were detected in days, weeks, or months, compared to 34 percent in APAC and 37 percent in Europe. 10 percent of the security breaches in Australia were not detected for years, seldom or never which was consistent with the European results.

Average time to detect a security breach



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

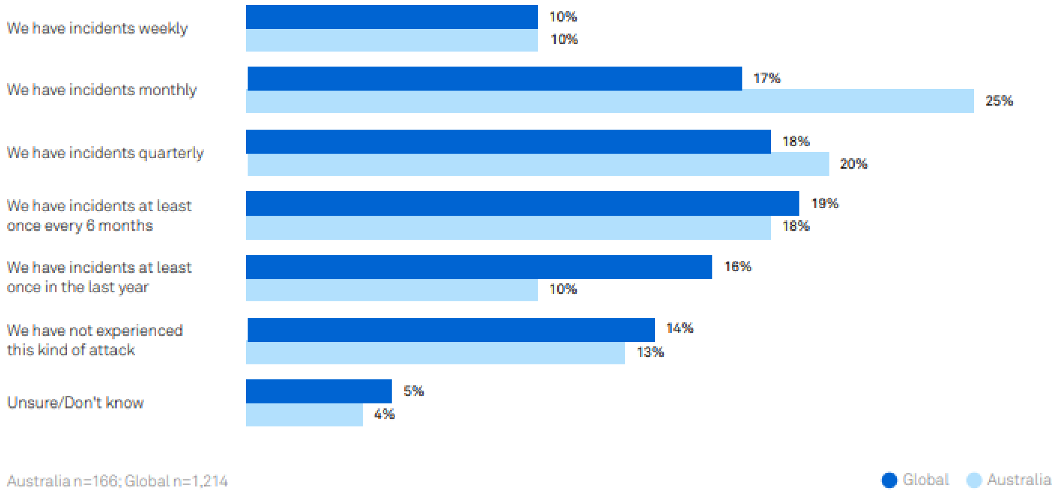
Security threats and trends

In our research, 68 percent of global respondents and 60 percent of Australian respondents report that their business has been interrupted due to a security breach in the past year.

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

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

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



Australia n=166; Global n=1,214

Ransomware

Attacks are inevitable

31 percent of Australian respondents whose business had been interrupted due to a security

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

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

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

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

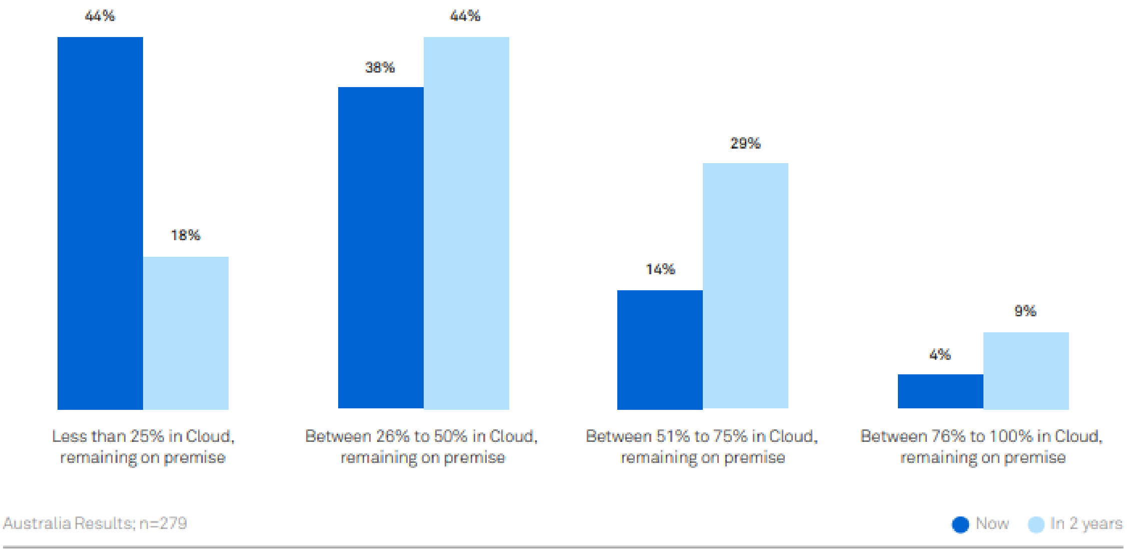
Cloud security

The migration and deployment of applications across public, private and hybrid cloud environments will likely continue into 2018.

Our research indicates that respondents see less than 20 percent of workloads in Australia are anticipated to remain on traditional on-premise infrastructure over the next two years. This is consistent with results in APAC at 19 percent and Europe at 17 percent.

However, businesses will continue to have some workloads on-site. Less than 10 percent of respondents foresee more than 75 percent of their workloads moving to a cloud environment in the next 24 months.

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

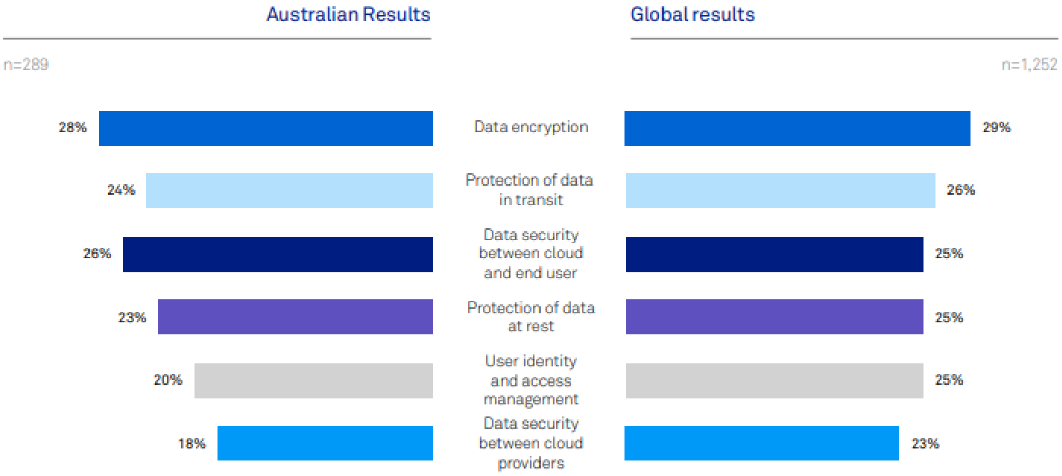


Our research shows that some of the top concerns for both Australian and global respondents for cloud security are data encryption, data security between cloud and end user, and protection of data in transit.

Some common concerns are around file integrity monitoring, data classification and detection of shadow IT systems. Others are around the ability to map workloads to the appropriate cloud environments.

Our research also shows that cloud services are the most frequently highlighted security concern in Australia, APAC and Europe in the context of all other possible threat vectors such as mobile devices, operating systems and databases.

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

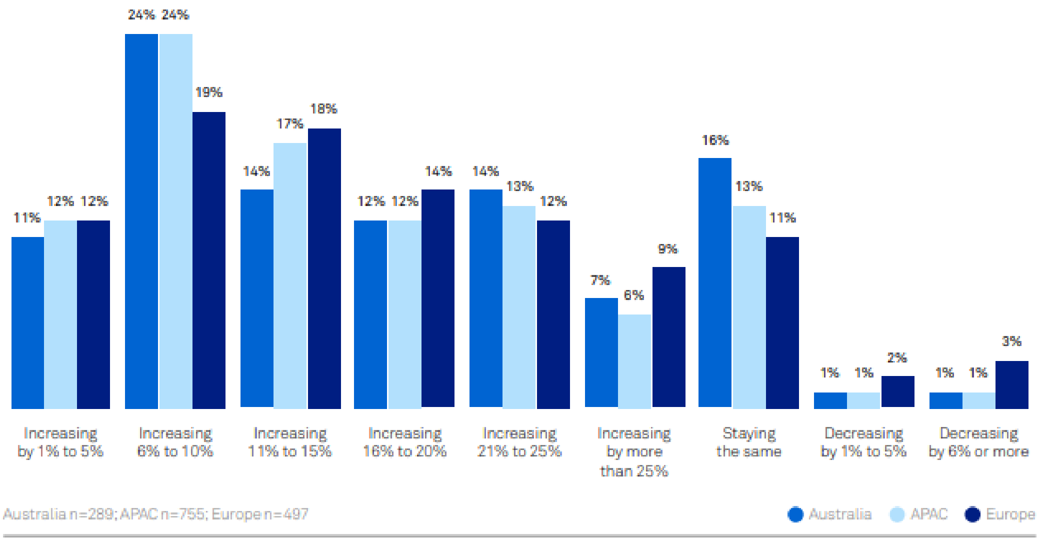


Future investments in security

The majority of businesses indicate they are planning to combine their cyber and electronic security budgets.

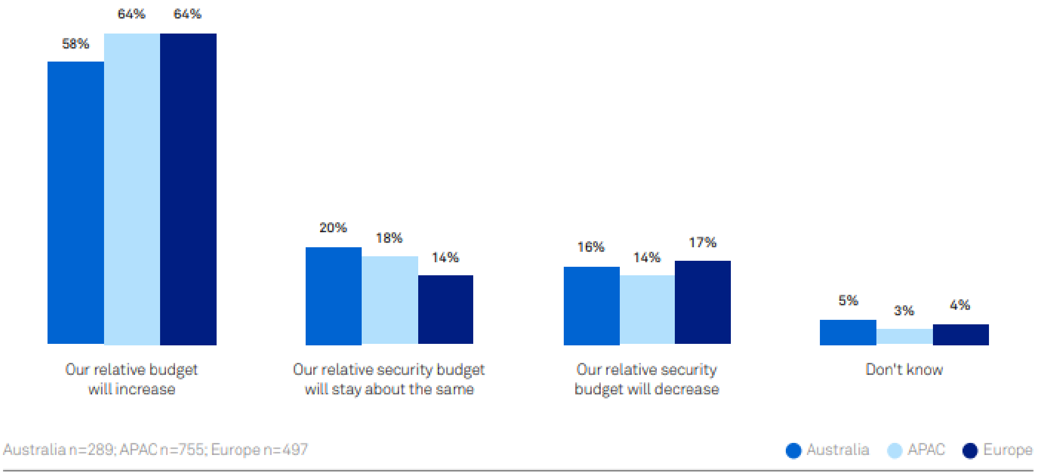
In terms of spending, our research highlighted security spending is also projected to increase in absolute terms in the next 12 to 24 months, but also relative to the percentage of total ICT budget. The table below shows the results for Australia, APAC and Europe.

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



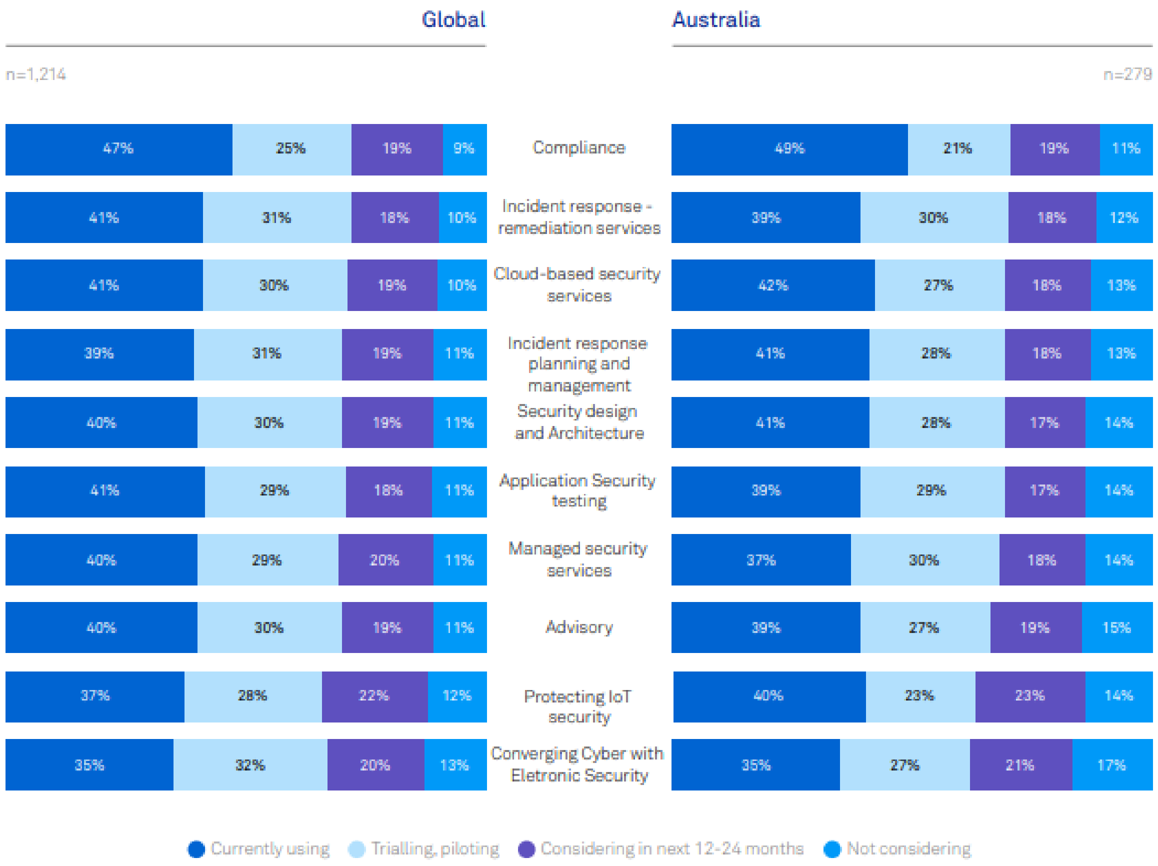
Australia n=289; APAC n=755; Europe n=497

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



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

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



Summary

As cyber and electronic converge and the industry prepares for a greater range and variety of attacks, organisations should start with the basics.

This includes ascertaining the location and value of data; who has access to the data; and the overall level of protection. There should also be clear ownership of this data.

From here, data classification can help an organisation understand the value, while data loss prevention can help ensure the data is not lost. Likewise, tools are available that can govern which employees have access to what, and from where. The location of data, for example, will be particularly important for compliance purposes.

Full report here.