2018/2019 CYBER SECURITY SURVEY

AUSCERT

FOREWORD

The cyber landscape is continually changing. New actors are entering the mix, the types of attack methods being used are evolving, regulatory obligations are shifting and organisations are looking at cyber security differently. The 2018/2019 BDO and AusCERT Cyber Security Survey Report highlights this more than any of our previous reports, as we draw upon three consecutive years of in-depth data to provide an insight to the cyber landscape in Australia and New Zealand.

This year the data paints a picture of an industry that is focused on prevention and compliance to regulatory changes, most notably the (Notifiable Data Breaches) Act 2017 (NDB) in Australia or the General Data Protection Regulation (GDPR). These changes have been a valuable mechanism to uplift cyber security maturity and instil a stronger focus on planning. With this has come higher spending on cyber security measures and a rise in confidence amongst respondents regarding their level of preparedness.

On the surface, all of these trends seem to position industry in a good place, but the reality is that more attention is needed on incident response. Even the best plans are of no help in the event of a cyber breach if they are not tested and continually reviewed and adjusted to remain relevant.

The continual rise of phishing, which is heavily reliant upon human interaction, only fuels this need for testing. A genuine business continuity risk exists for many Australian and New Zealand businesses and the key to overcoming it is education and testing of the learning process.

Interestingly, the report findings also pinpoint a significant increase in suspected attacks from foreign governments/ nation states, and a view by many respondents that hacktivist attacks will increase in the future.

These trends are reflective of what our global BDO Cyber Security team is witnessing worldwide. Our Cyber Threat Insights Report for the fourth quarter of 2018 highlighted a blurring of nation-state cyberattack groups with criminal cyberattack groups from their respective countries and other nations worldwide.

What is of particular note is that the impacts of cyber attacks are also shifting. While organisations are reporting less business disruption, the potential for reputation damage is on the rise. Regulatory changes have brought cyber resilience into the public eye and rarely a month goes by without the media reporting on a cyber breach and the impact it's had on an organisation's customers. Intangible risks like these are challenging to recover from and impossible to insure against.

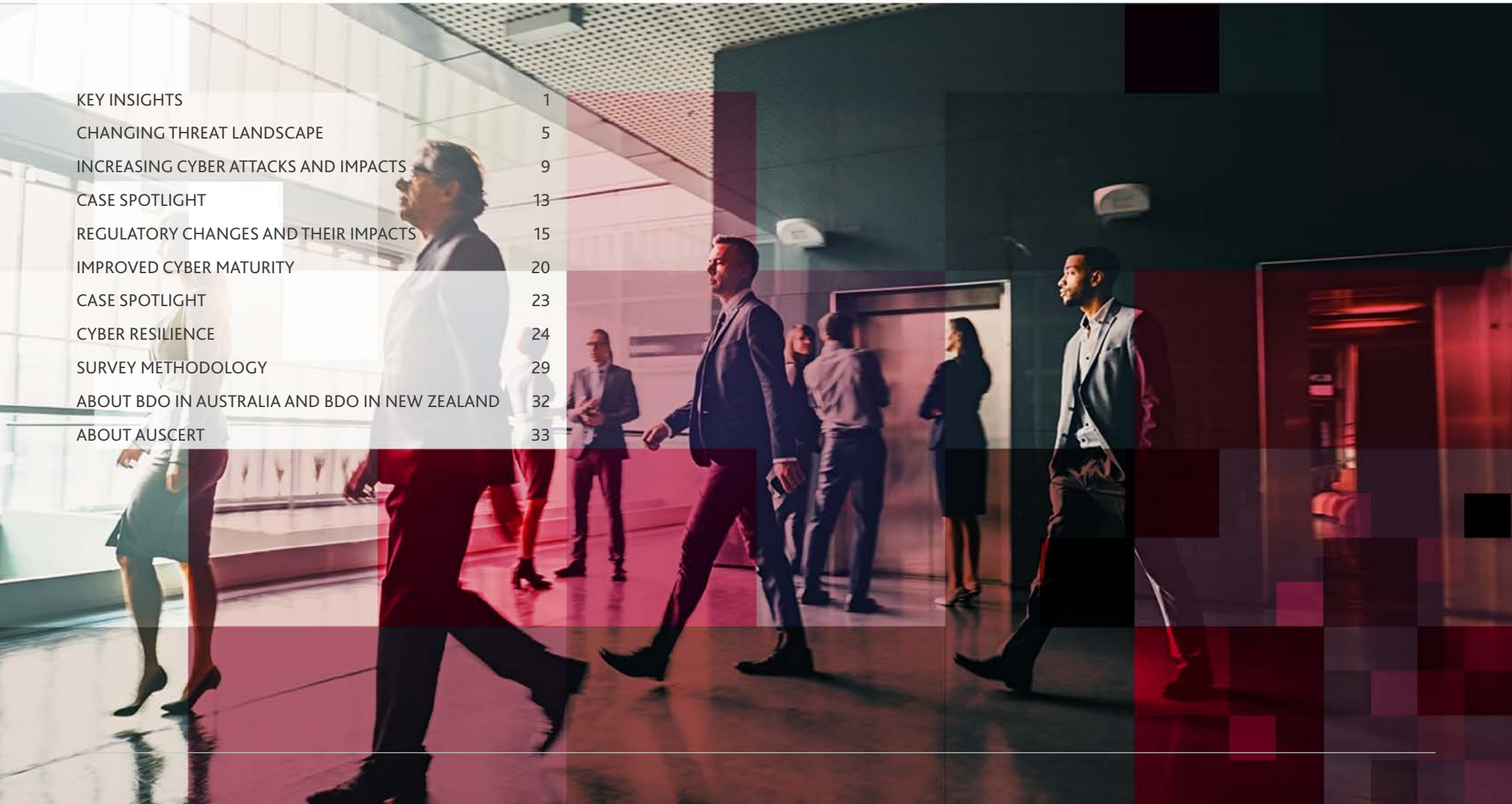
This year's report delves into these topics and many more, providing you with a wealth of valuable benchmarking data and threat intelligence insights. By taking a proactive approach to learning more about the cyber landscape and how it could impact your business, you are taking a vital first step in instilling a culture of continual improvement and transparency about cyber security within your organisation.

Thank you to all the participants in this year's survey, and also to those who took part in our 2016 and 2017 surveys. Without your honest input and ongoing support, we couldn't ascertain the long term data trends that have shed light on many important issues in this year's report. We greatly appreciate the effort you put into supporting the survey and look forward to continuing the education journey with you into the future.

Leon Fouche
National Cyber Security Leader,
BDO

David Stockdale
Director,
AusCERT

CONTENTS



KEY INSIGHTS

At BDO, we strongly believe an organisation's approach to cyber security planning and management is set from the tone at the top. With this in mind, this year's results are music to our ears! A key theme running through the 2018 findings is that there has been a genuine uplift in leadership awareness of cyber security and improved reporting to these senior levels. It is action like this that allows organisations to strengthen their cyber security resilience.

- **Increased cyber awareness across respondent organisations, with management getting more involved**
- **Enhanced cyber maturity and improved security posture, likely as a result of compliance with regulatory changes**
- **More work is needed to manage the impact of incidents, particularly developing breach response plans and adopting cyber insurance.**

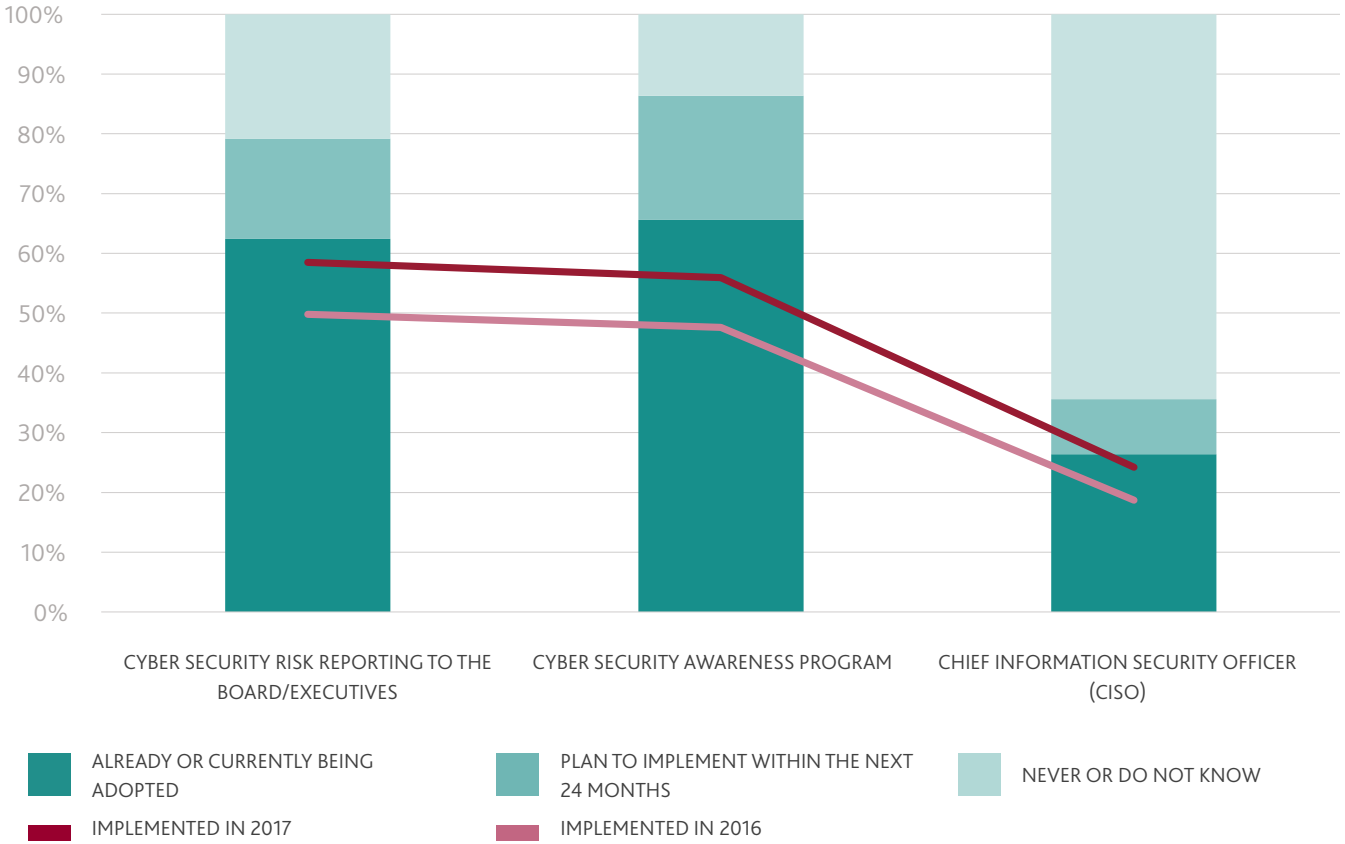
Many could argue this uplift in leadership engagement is simply the result of regulatory changes – the Notifiable Data Breaches Scheme and General Data Protection Regulation – and it would be hard to disagree entirely. What is clear though is that these changes are not the sole reason for Australian and New Zealand businesses taking a more proactive approach. High levels of respondent commitment to roll out activities such as cyber security awareness training and cyber security risk assessments demonstrates this.

What is still missing though, is a stronger focus on reducing the impact of cyber incidents. The regulations and leadership support have clearly had a positive impact on helping respondents prevent a cyber attack, but many still appear vulnerable once an attack happens.

LEADERSHIP IS INCREASINGLY AWARE OF CYBER RISK

In 2018, survey respondents demonstrated a clear increase in cyber security awareness. This shift in attitude has come directly from the top, with risk reporting to the Board and Executive Leadership Team (ELT) increasing. Where the Board and ELT have greater oversight and understanding of their organisation's cyber security risks, greater support and implementation of proactive cyber security controls is reported. These activities include cyber security training and awareness programs for staff within the organisation, establishing the requirement for cyber security risk assessments and standardising approaches to managing cyber security.

CYBER RESILIENCE — LEADERSHIP AND TONE AT THE TOP



CYBER RISK MANAGEMENT IS MATURING

Respondents have begun defining their risk management frameworks, but these exist in varying states of maturity. A BDO and Australian Institute of Company Directors study of Australian organisations in 2018 on Enterprise Risk Management[1] found that while the majority of organisations have partially defined risk thresholds and risk statements, only 6% have fully defined their risk posture.

In contrast, when we consider cyber security risk management, as opposed to the broader risk management definition, the data is more positive. This year's survey found that by 2020, 84.8% of respondents plan to implement regular cyber security risk assessments, while 86.4% of respondents expect to have a cyber security awareness program in place. This demonstrates that when the Board and ELT understand the risk landscape, they are willing to assign resources to address cyber security risk. We expect this sentiment to permeate further with respondents' risk management frameworks naturally being refined and maturing over time with a posture towards continual improvement.

DATA PRIVACY REGULATIONS HAVE RAISED VISIBILITY OF CYBER RISK

A notable driver for change across industries in 2018 has been the implementation of the Privacy Amendment (Notifiable Data Breaches) Act 2017 (NDB) in Australia and the General Data Protection Regulation (GDPR) in Europe. With these new regulations, organisations face greater risk of significant financial (fines for non-compliance) and reputational damage associated with a data breach. These additional consequences, coupled with the immediate impact of data breaches, are leading to many respondents implementing preventative controls. This fact is reflected in the trend of increased IT security budgets for the third year running. In part due to this increase in budget, organisations appear more confident in setting and achieving their cyber security outcomes.

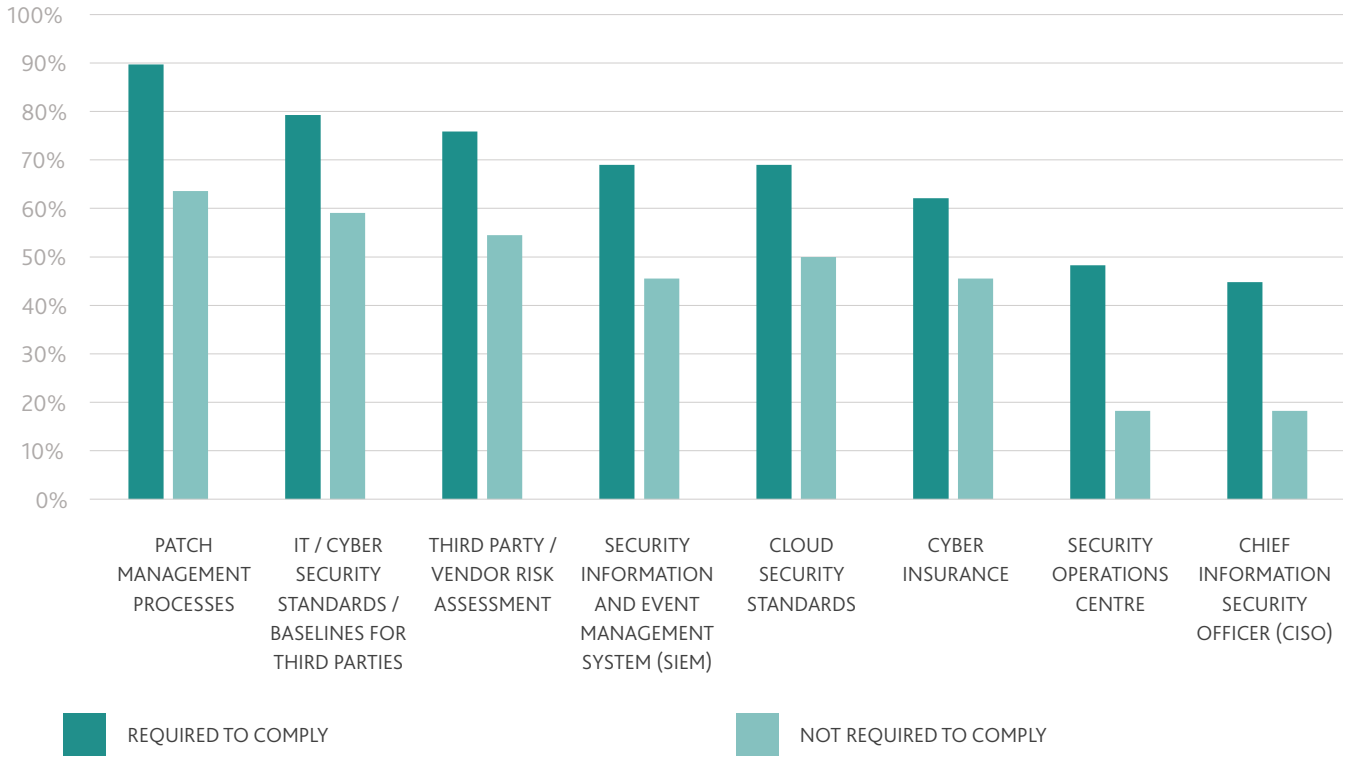
TOO MUCH FOCUS ON PREVENTION, NOT ENOUGH ON RESPONSE

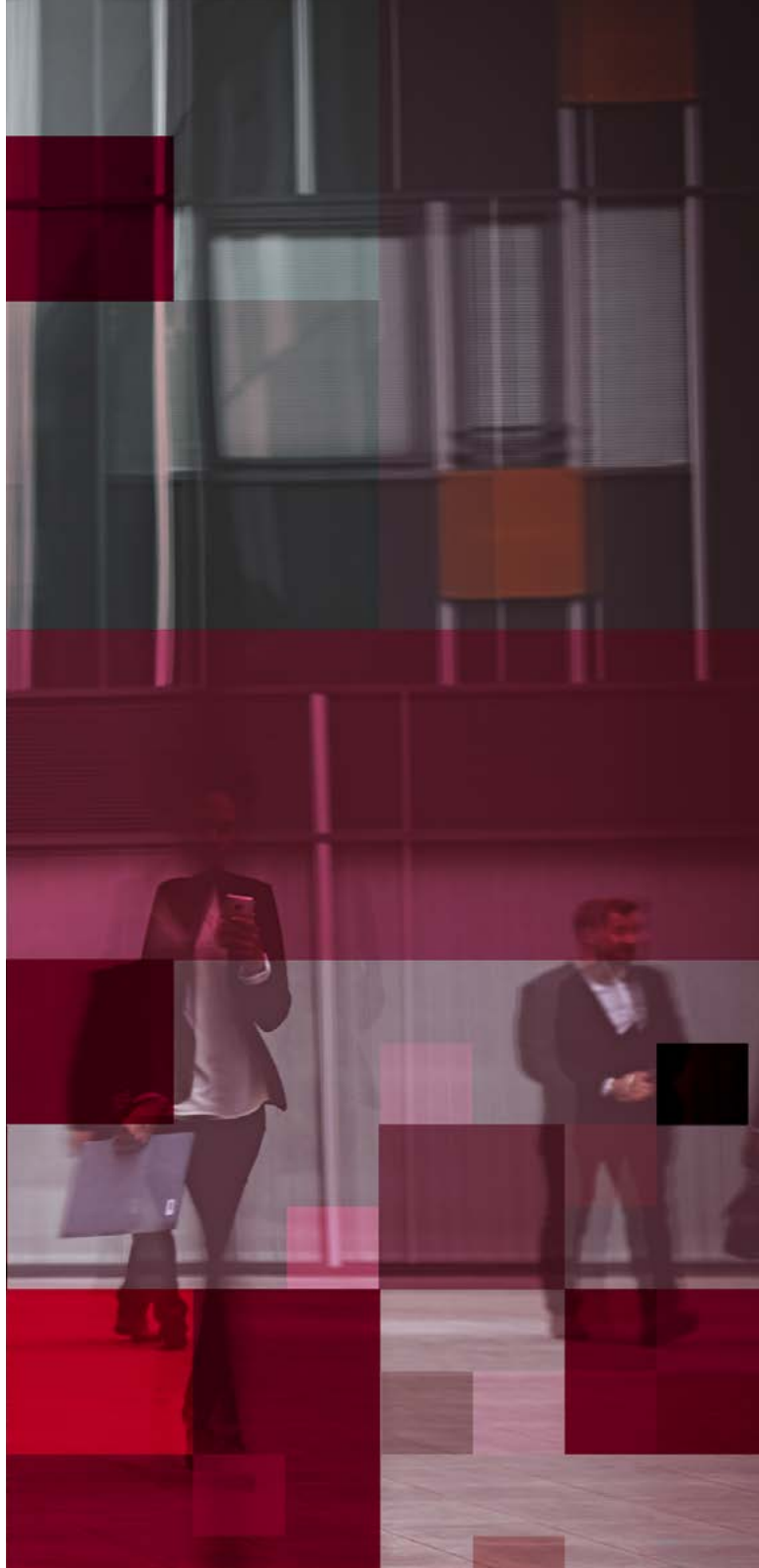
Even with this overall trend, further work is required to reduce the impact of cyber security incidents. In previous years, the BDO and AusCERT Cyber Security Survey has found that proper planning and preparation for cyber incidents resulted in greatly reduced impacts to the organisation following an incident. The importance of cyber resilience has been highlighted again in 2018.

Where organisations are required to comply with NDB or GDPR, the adoption and maturity of security controls is significantly higher than those who are not required to comply. Despite this, the focus of this compliance is on preparedness, not response or incident management. We are hopeful that over the next 12 to 24 months, organisations will focus on implementing strategies to assist with reducing or lowering the impact of cyber security incidents, on the back of the work they've done to comply with the new regulations. Areas of focus should include the development of data breach response plans and the adoption of cyber insurance, as these controls can afford organisations the opportunity to minimise the impact of breaches, while ensuring rapid investigation can occur.

[1]https://aicd.companydirectors.com.au/advocacy/research/aicd-bdo-enterprise-risk-management-report-2018

HOW DATA BREACH COMPLIANCE REQUIREMENTS AFFECT ADOPTION OF SECURITY CONTROLS - 2018





CHANGING THREAT LANDSCAPE

CYBER REMAINS A TOP GLOBAL RISK

According to the World Economic Forum Global Risks Perception Survey 2019[2], cyber attacks and data fraud or theft are rated in the Top Five risks assessed in terms of likelihood. It is noteworthy, and indicative of the changing threat landscape, that cyber attacks and data breaches are rated amongst the most impactful risks, alongside weapons of mass destruction, climate change, natural disasters and water crises.

Cyber risk remains a pertinent and ever present consequence of society's pervasive adoption of technology. It therefore follows that as we increase our consumption of technology, our risk profile, exposure and susceptibility to risks that could compromise the confidentiality, availability and integrity of information naturally increases.

INCREASED SOPHISTICATION, MAGNITUDE AND COST OF CYBER ATTACKS

Cyber attacks are increasing in sophistication and magnitude of impact across all industries, on a global scale. A recent study from the Ponemon Institute's recent Cost of a Data Breach Study[3] found that the average cost per lost or stolen record as a result of a data breach was USD$148 and Australia's average organisational cost for a data breach was USD$1.99 million. Irrespective of industry sector, all organisations possess valuable information assets, which may include sensitive IP, financial payment information, client information, supply chain partners' information, personally identifiable information (PII), protected health information (PHI), and/or payment card information (PCI).

EDUCATION, HEALTHCARE AND INFORMATION, MEDIA AND TELECOMMUNICATION SECTORS MOST AFFECTED BY DATA BREACHES

While all organisations are potential targets of cyber attacks, industries that possess the highest volumes of valuable data are typically the most frequent targets. Results from the 2018 survey found that respondents in the healthcare and education sectors were highly targeted in Australia and New Zealand. The Office of the Australian Information Commissioner's (OAIC's) Q4 (Oct – Dec 2018) Report[4] noted that 54 (20%) healthcare and 21 (8%) education sector organisations reported data breaches during this period, with 64% of them the result of malicious or criminal activity and 33% from human error.

Organisations seeking to enhance their cyber security capabilities will need to understand the sources of cyber incidents (refer to pages 8 and 9 of the BDO and AusCERT 2017/2018 Cyber Security Survey for a summary of threat actor profiles and motives).

[2]http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
[3]https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf
[4]https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics/notifiable-data-breaches-quarterly-statistics-report-1-october-31-december-2018.pdf

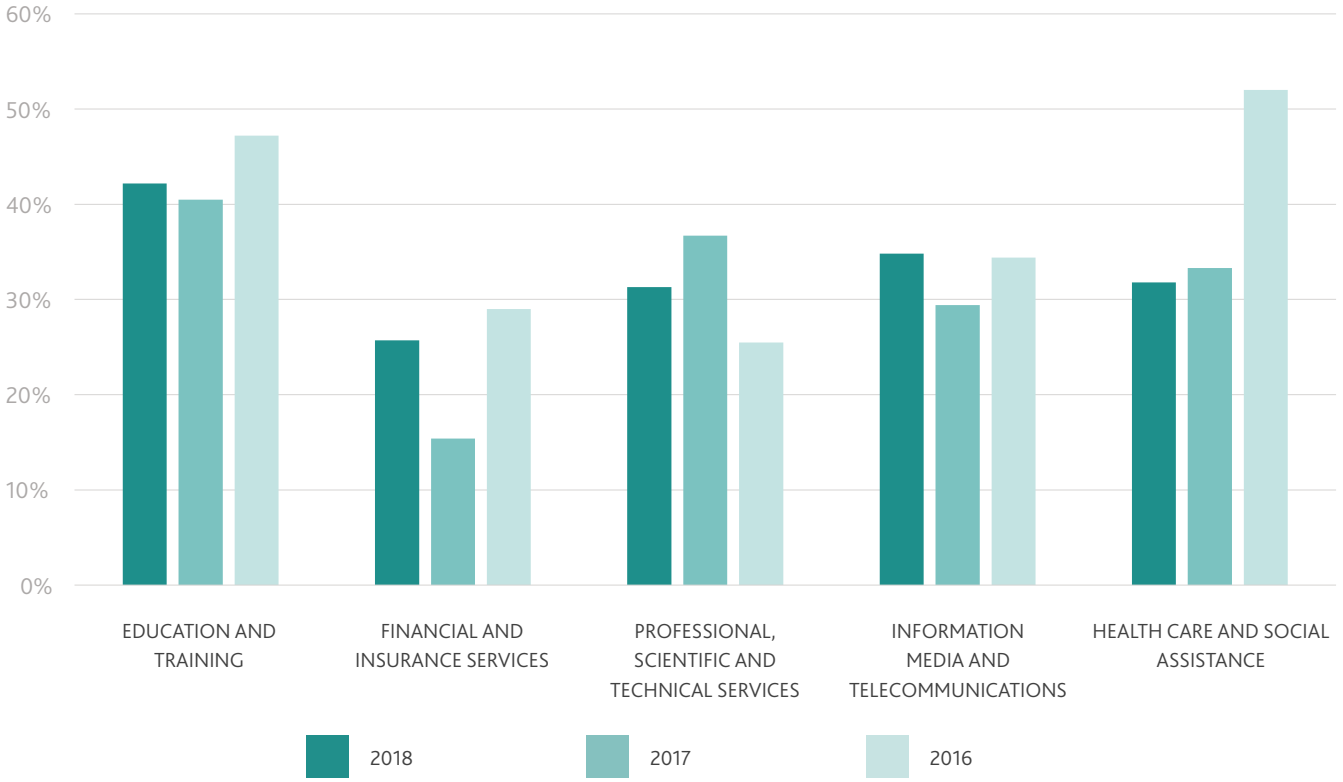
CYBER CRIMINALS ARE THE MOST COMMON SOURCES OF CYBER ATTACKS

In 2018, respondent organisations overwhelmingly reported that cyber criminals were responsible for cyber attacks. Respondents also reported a significant increase in suspected attacks from foreign governments/nation states. Although there are clear differences in the motivations (and resources) between foreign government/nation state level groups and individuals or criminal groups, there is a degree of fluidity and commonality between the two classes of threat actor. In numerous cases, the same (or very similar) tools, techniques and procedures are used by different classes, perhaps because those are the best tools available. Consider the WannaCry malware link to North Korean state sponsored actors (see BDO 2017/2018 Cyber Threat Insights Report[5]).

MANAGED SERVICE PROVIDERS ARE TARGETED FOR ACCESS TO THEIR CUSTOMERS' ENVIRONMENTS

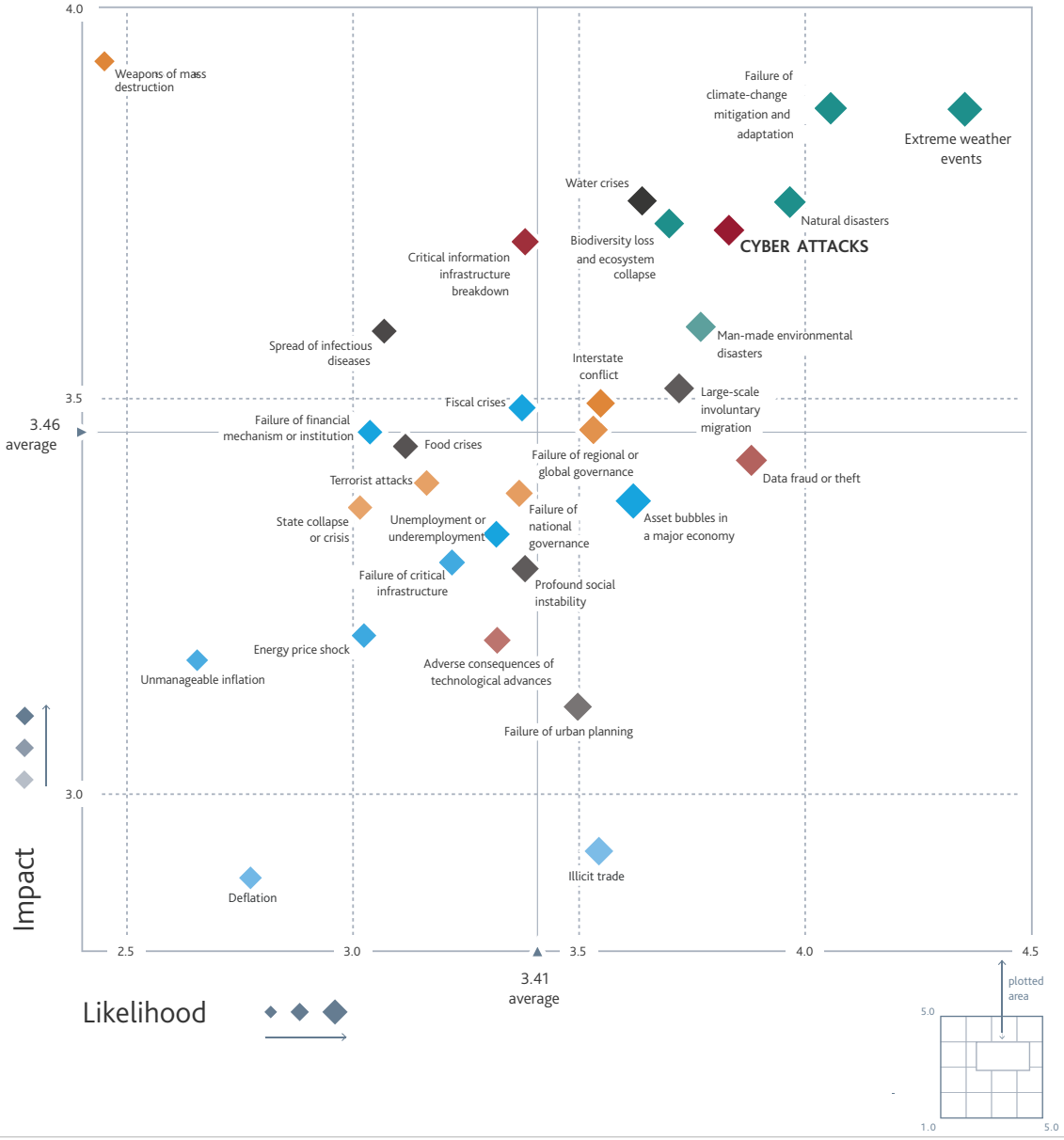
Managed Service Providers (MSPs) are engaged by organisations to manage their IT services and infrastructure. MSPs require remote access to their customers' systems to deliver these services, making MSPs attractive targets for state actors and cyber criminals. A notable example of this was the recently published campaign targeting MSPs worldwide, and which included Australian organisations, in a concerted effort to steal commercial secrets from the customers of MSPs for commercial advantage. It is important to note that the attributed threat actor's (APT10, also known as MenuPass, StonePanda or CloudHopper) activities in this campaign commenced as far back as 2014 and were comprehensively tracked and attributed in 2017 – however only recently had its impacts and the Australian Government's public response become well publicised.

ORGANISATIONS THAT EXPERIENCED AN INCIDENT - 2016 TO 2018



[5]https://www.bdo.com.au/en-au/insights/cyber-security/publications/bdo-cyber-threat-insights-report-2017-2018

THE GLOBAL RISKS LANDSCAPE 2019



Top 10 risks in terms of Likelihood

1. Extreme weather events
2. Failure of climate-change mitigation and adaptation
3. Natural disasters
4. Data fraud or theft
5. Cyber-attacks
6. Man-made environmental disasters
7. Large-scale involuntary migration
8. Biodiversity loss and ecosystem collapse
9. Water crises
10. Asset bubbles in a major economy

Top 10 risks in terms of Impact

1. Weapons of mass destruction
2. Failure of climate-change mitigation and adaptation
3. Extreme weather events
4. Water crises
5. Natural disasters
6. Biodiversity loss and ecosystem collapse
7. Cyber-attacks
8. Critical information infrastructure breakdown
9. Man-made environmental disasters
10. Spread of infectious diseases

Categories

- Economic
- Environmental
- Geopolitical
- Societal
- Technological

HACKTIVIST ATTACKS EXPECTED TO BE NEARLY TWICE AS COMMON IN 2019

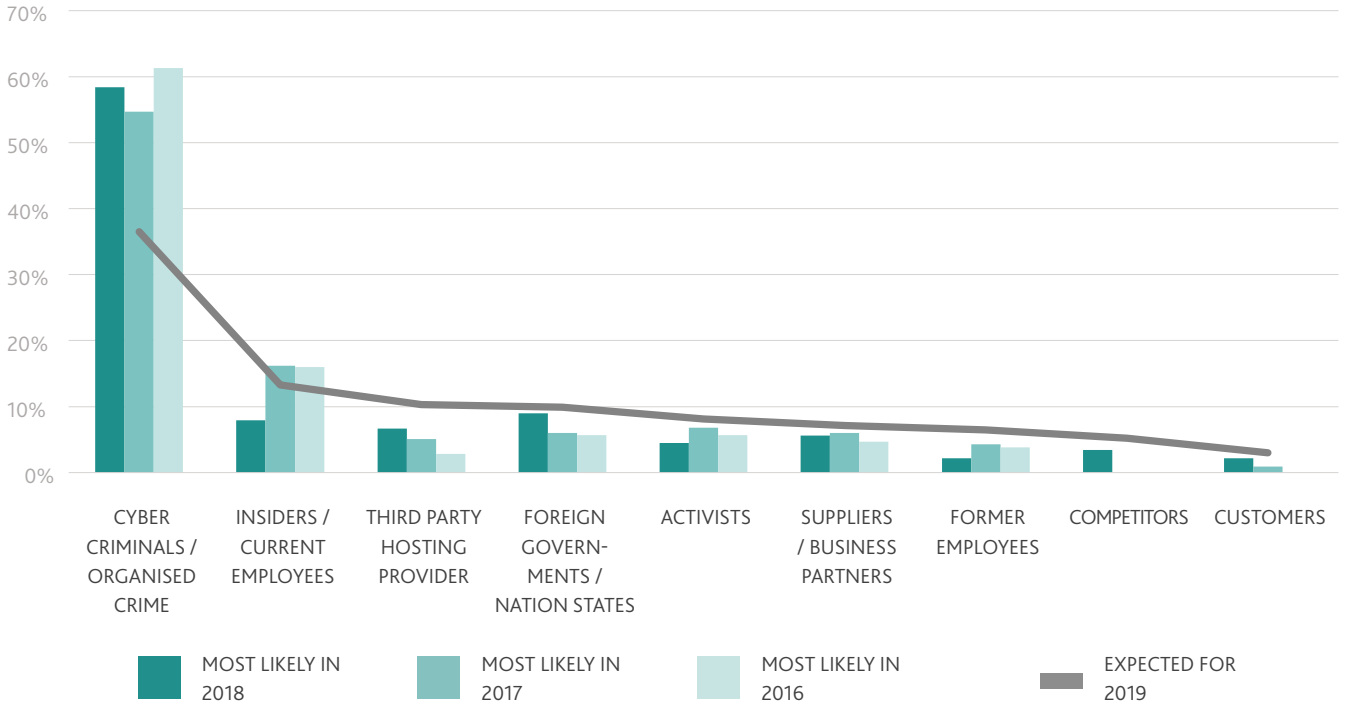
The adjacent graph shows the types of attackers respondents felt were most responsible for cyber attacks, compared to the attackers they expect to be most prevalent in 2019. Respondents perceive that cyber criminals will be perpetrating less attacks in 2019, but surprisingly they feel that activists/ hacktivists are going to be nearly twice as likely to be sources of cyber security incidents than the previous year.

Organisations may be underestimating the prevalence of cyber security criminals and insiders, and overestimating the frequency of attacks launched by other actors. This could be symptomatic of a limited understanding of the relevant cyber security threat risk landscape. In order to effectively defend against most likely cyber risks, organisations must have a clear understanding of who is targeting which assets, and how they are likely to do so.

LIMITED PERCEPTION OF CYBER THREAT RISK LANDSCAPE

These findings indicate that respondents may be inaccurately assessing their relevant cyber security risk landscapes. When organisations perceive that different threat actors are targeting them compared to reality, security control investments are not commensurate with the real risk. This means organisations could be over or under protecting the wrong assets, from the wrong adversaries, in the wrong ways and for the wrong reasons. In general, this misinterpretation of the cyber threat landscape is likely symptomatic of limited comprehension of cyber risk more generally.

MOST LIKELY SOURCES OF INCIDENTS - 2018 vs 2019



INCREASING CYBER ATTACKS AND IMPACTS

The 2018 survey data supports the common observation that adversaries are continually evolving their tactics and strategies. Cyber adversaries are rapidly evolving and adopting new tactics to better suit both their targets and the technology solutions they choose.

Data trends between 2017 and 2018 indicate that some exploits seem to be targeted for a period of time and possibly then become uneconomical for attackers to invest effort into as organisations' defence layers improve. The decline in ransomware and malware attacks from 2017 to 2018 demonstrates this. Conversely, some exploits have continued to grow year-on-year, such as phishing.

In 2018, the survey results have highlighted the following cyber attack trends:

- Phishing has consistently increased to become the most common incident experienced by survey respondents
- Adversaries are moving away from ransomware and malware exploits as there has been a significant fall in the number of attacks between 2017 and 2018. Looking at year-on-year, ransomware experienced a 44.27% drop in frequency. Ransomware, which involves unauthorised modification of information, can partially explain the more dramatic 70.90% drop in unauthorised modification of information incidents
- Data loss/theft of confidential information has risen rapidly since 2017. Respondents also reported an increase in the data breach via third party provider/supplier category
- Denial of service attacks have decreased from 2017
- In the 2018 survey we saw an increase in the number of attacks classified as 'None of the above', indicating that new incident types are occurring.

THE CONTINUED RISE OF PHISHING

Our trend data from survey results since 2016 outlines a consistent rise in phishing incidents through to 2018. In fact, it remains the most common incident experienced. Adversaries continue to target the human psyche, our inquisitiveness and general position of trust. Humans are continuing to prove to be a weak link in the layers of defence.

We have seen many businesses slowly implementing phishing awareness training across their workforce, but educating all employees about the dangers of phishing is a slow process. While education continues to improve, we expect phishing to remain the most popular attack vector.

Phishing can also be considered a method through which other incidents can occur – for example, ransomware can be delivered through phishing, or credential compromise can be used to gain unauthorised access to information or perform Business Email Compromise (BEC) fraud.

Over the past 12 months, we have seen adversaries specifically target a number of industry sectors with BEC attacks. Organisations that manage the transfer of large sums of money have been specifically targeted, such as conveyancing firms.

INCREASING DATA BREACH ATTACKS OR JUST MANDATORY REPORTING?

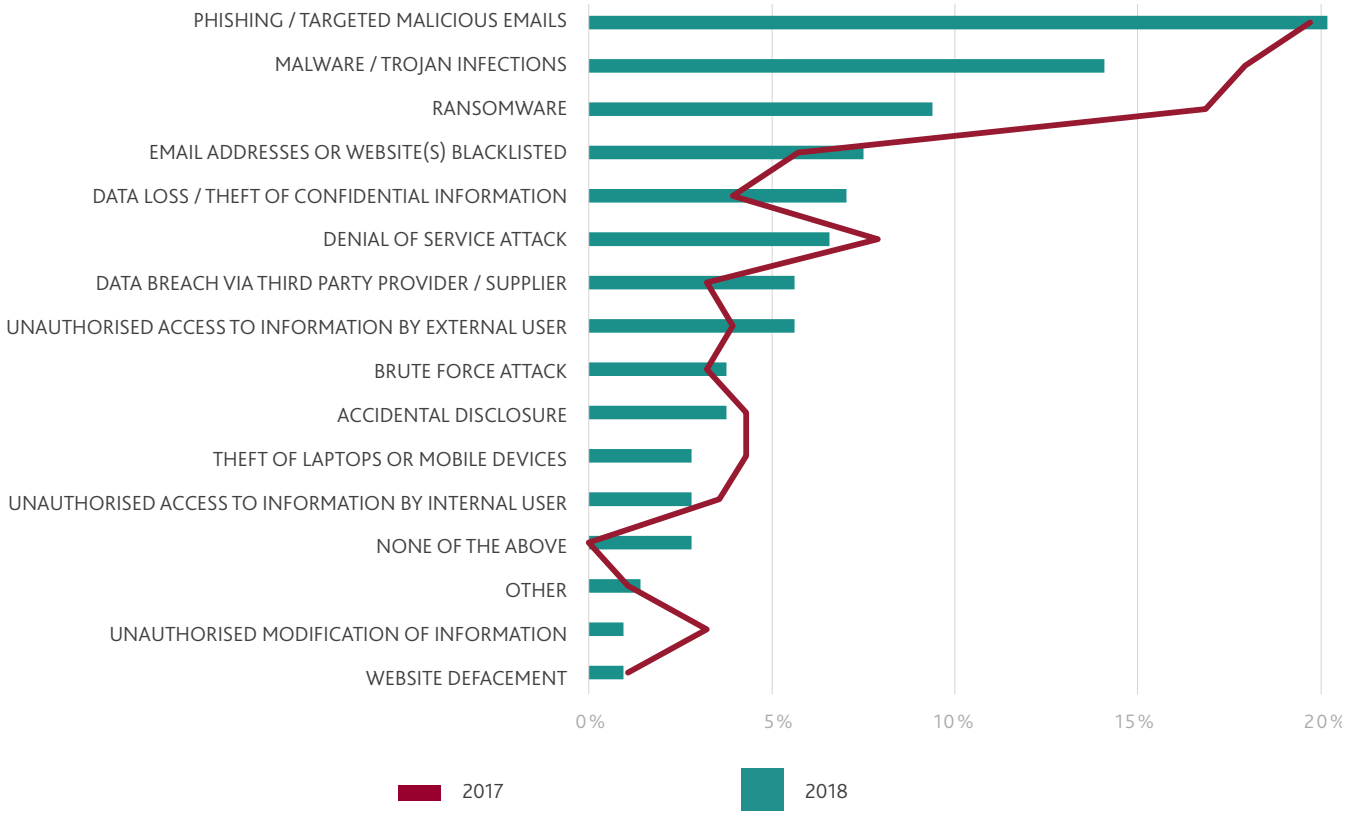
Data loss/theft of confidential information incidents rose by 78.68% in 2018 compared to 2017. Equally as alarming is the rise in data breaches experienced through third party providers and suppliers, which rose by 74.30%.

This increase in data may be related to implementation of the NDB Scheme by the Office of the Australian Information Commissioner in early 2018. The introduction of mandatory reporting could have contributed to respondents reporting a significant increase in these attacks between 2017 and 2018.

LOOKING AHEAD...WHAT ARE RESPONDENTS EXPECTING?

When considering incident types experienced and future expectations, some interesting results came to the fore. Respondents are anticipating a significant increase in data loss/theft of confidential information in 2019, compared to what they actually experienced the prior year. Conversely, they expect to experience a sharp decrease in phishing incidents moving forward, yet this does not align with the trends we have observed over the past three years for this attack type. The expected reduction in malware and ransomware incidents in 2019 aligns with the trends presented in survey data.

INCIDENTS EXPERIENCED - 2017 vs 2018

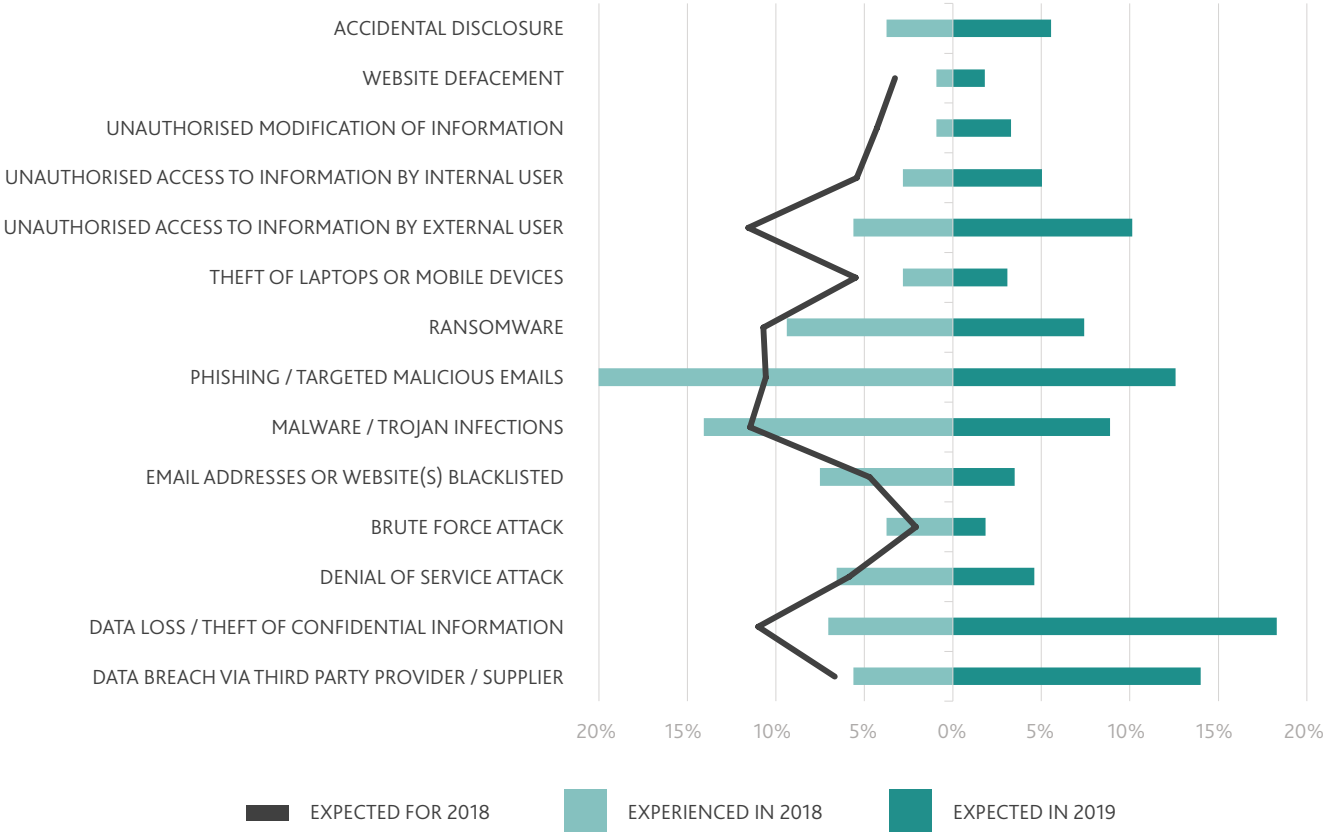


INCREASE IN PHISHING ATTACKS AND APPLICABILITY OF INDICATORS OF COMPROMISE

AusCERT members have witnessed an increase in phishing, which is now more prominent than all other types of incidents. "Bullet proof" and lax processes within hosting providers are challenges for AusCERT and, as a result, AusCERT has invested in bespoke systems that integrate with its open source incident ticketing system, to facilitate tracking and faster recovery for its members suffering phishing attacks.

In AusCERT's established intel sharing groups (such as the CAUDIT ISAC for Australia and New Zealand higher education and research), the organisation targets its threat intelligence to suit members' utilisation patterns. This includes determining the type of threat indicators members are able to readily detect or prevent, such as email based indicators. For example, "email subject" is a readily detected and/or blocked indicator of compromise for most organisations, which has led to members utilising AusCERT's intelligence to configure their environments to increase their ability to prevent and/or detect phishing.

INCIDENTS EXPERIENCED IN 2018 vs INCIDENTS EXPECTED IN 2019



WHO EXPERIENCED AN INCIDENT

While the past three years of survey data show a downward trend in the number of respondent organisations experiencing a cyber incident, almost a third of all respondents in 2018 still experienced one. The reduction in the number of incidents may be due to greater defences and awareness being adopted by organisations, as the importance of cyber resilience has increased over the past two to three years.

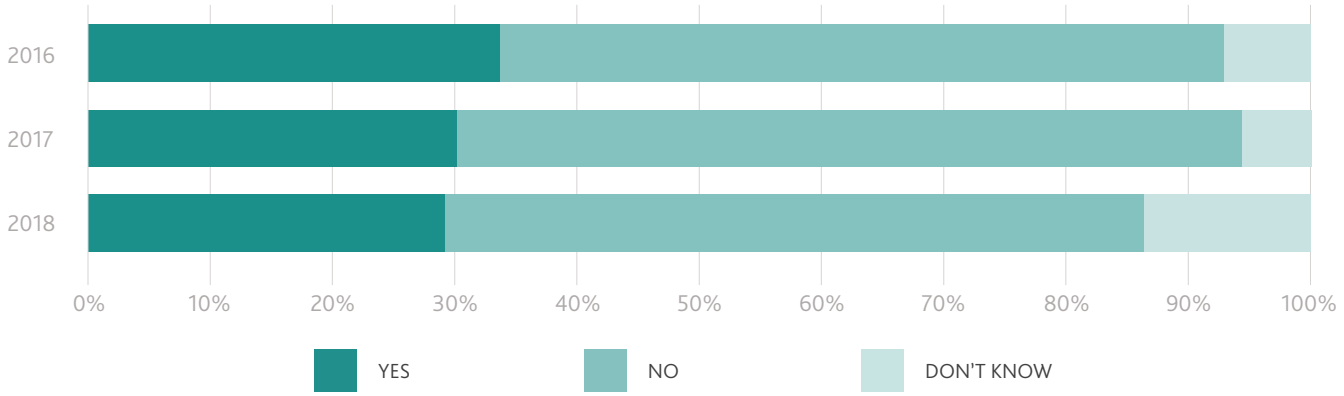
Interestingly, the 2018 survey saw a significant increase in the number of respondents who did not know whether an incident had occurred, an increase from 5.7% in 2017 to 13.6% in 2018. This change could be related to the decrease in the prevalence of ransomware, which by its very nature ensures the business knows they have been compromised.

INCIDENT IMPACT

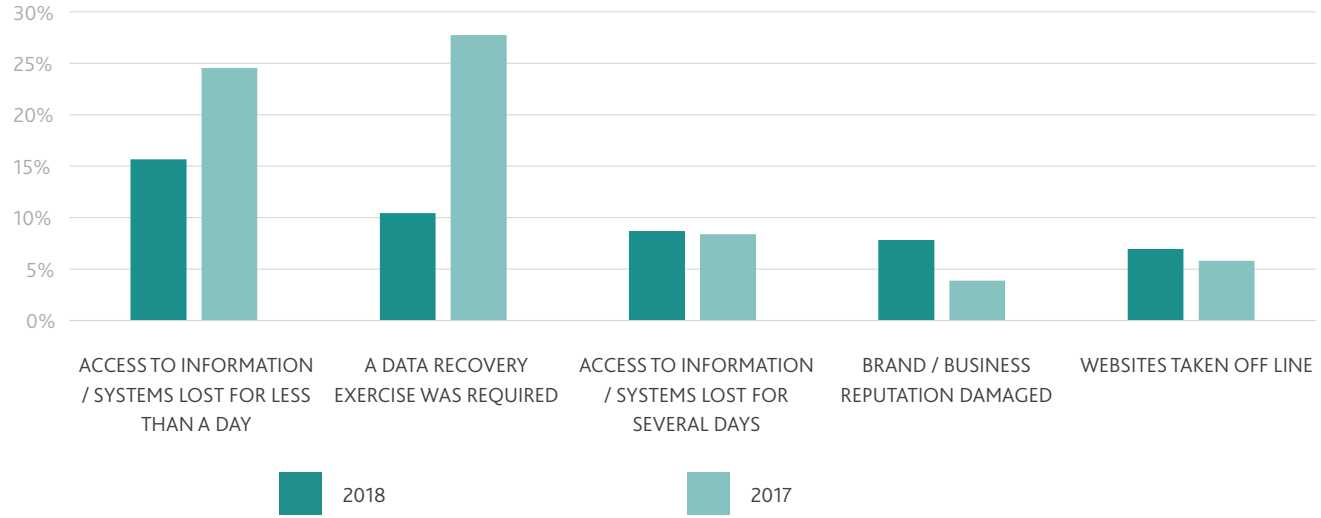
The impact of an incident on a business can vary considerably and data from 2017 to 2018 shows some stark changes in these impacts over just one year. There has been a considerable drop in both 'access to information/systems lost for less than one day' and 'a data recovery exercise was required'. One could argue this is the result of a drop in ransomware attacks, which generally require a data recovery process because data is encrypted and held to ransom by the cyber criminal/s.

In contrast, this focus on preparedness has not filtered through to a reduction in the impact on an organisation's brand/reputation, nor their website. Both factors experienced an increase between 2017 and 2018. Business websites that have been taken offline also increased between the years.

ORGANISATIONS THAT EXPERIENCED AN INCIDENT - 2016 TO 2018



IMPACTS OF CYBER SECURITY INCIDENTS - 2017 vs 2018



CASE SPOTLIGHT

MALWARE ATTACK ON GERMAN FOREIGN MINISTRY

In early September, Antivirus and Internet Security Solutions (ESET) published a follow-up investigation report about the attack on the German Foreign Ministry[6] attributed to Russian nation-state actors. The attack was notable for the unique backdoor that was used, which does not require a direct Internet connection to operate. Instead, the backdoor can leverage the ability to send emails from workstations and compromise controlled environments that maintain a highly filtered Internet connection. The backdoor mainly targets users of Microsoft Outlook, a widely used mail client, but also targets The Bat!, an email client used across Eastern Europe.

OVERVIEW OF THE EVENT

The attack, which began in 2016 and was identified by the German authorities only in late 2017, resulted in the exfiltration of sensitive data for more than a year and is attributed to Turla (sometimes referred to as Snake), a Russian cyberespionage threat group. The actor obtained access to the German Foreign Ministry's computer infrastructure via malware that communicates with its command-and-control server through specially crafted PDF documents attached to emails. It's worth noting that the backdoor operates on common protocols; however, it does not exploit any actual vulnerabilities in PDF Reader or Outlook. Rather, the malware is able to decode data from the PDF documents and interpret it as commands for the backdoor.

PENETRATION VECTOR

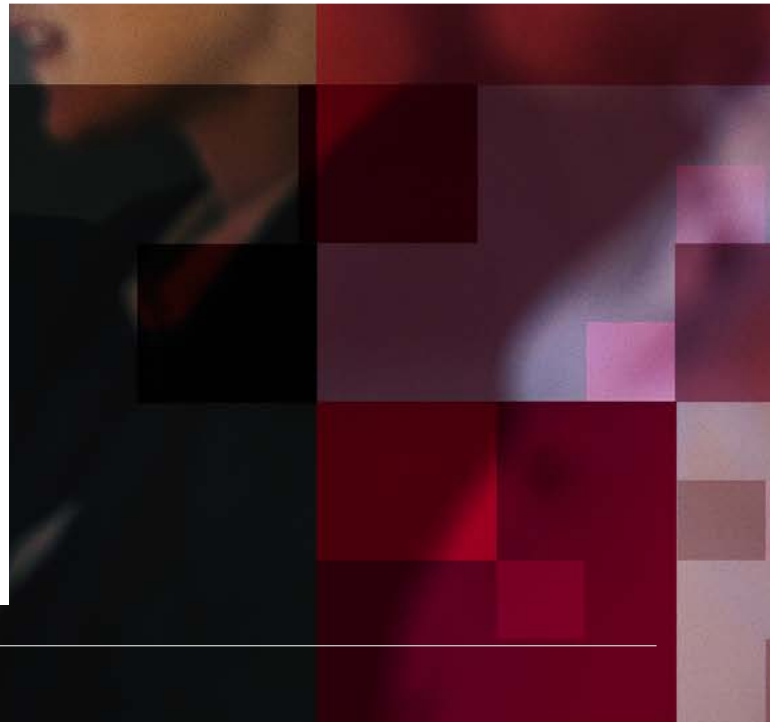
Initially, the attackers infected the network of the Federal Academy of Public Administration (Hochschule des Bundes), a federal administrative university. The attackers then laterally moved across the network until they successfully achieved persistency in March 2017. The most notable tool in the attack is the aforementioned Turla backdoor, which appears to have been used since 2013 and was created as early as 2009. In addition to the attack on the German Foreign Ministry, this backdoor was involved in attacks on two additional European governmental institutions and a major defence contractor. We assess with moderate certainty that one of the targets was the French government. This is based on a string found within the malware that contained the official French government top-level domain (TLD), *gouv.fr*.

[6]https://www.welivesecurity.com/wp-content/uploads/2018/08/Eset-Turla-Outlook-Backdoor.pdf

DECREASE IN RANSOMWARE INCIDENTS

AusCERT has speculated that ransomware is less effective than it used to be (other than commodity, run-of-the-mill malware that locks end user PCs) because enterprises have potentially hardened their incident response strategy, including keeping regular, tested backups.

Incidents that previously would have left an organisation unrecoverable (or in a recovery state for days) can potentially be recovered in approximately one hour, for example the recent Weather Channel ransomware attack in the United States took 90 minutes.



CASE SPOTLIGHT *CONTINUED*

MALWARE ANALYSIS

The backdoor has a number of variants, several of which target Outlook's email client, while others target The Bat!. The command-and-control protocol is based on sending and receiving emails from the attackers' email addresses. These emails are attached with PDF files containing commands for the malware or data taken from the compromised systems and siphoned off to the attackers. The commands are compressed with bzip2 and encrypted with a modified MISTY1 algorithm. The communication with the malware is fully transparent to the user, and the emails are timed and sent to the attackers at the same time the user sends a legitimate email—reducing the chances of detection.

In 2018, the backdoor gained the ability to run PowerShell commands via a tool named Empire PSInject,[7] which injects PowerShell commands into the process. Due to the design of the command and protocol, the backdoor does not require direct access to the Internet—only a workstation capable of sending emails. Accordingly, this malware poses a risk to controlled environments with highly filtered Internet connections. Moreover, shutting down the attacker's email address does not hinder the malware's command-and-control capabilities as it does not verify the identity of the sender. Accordingly, it can be controlled from any email address. This does mean, though, that more than one group may be using it.

Moreover, Turla created a different email address for the command-and-control function of each target. This was done via the free email service GMX by using real employees' names based on the following format: *firstname.lastname@gmx[.]com*

The use of GMX and employees' names presents several mitigation issues. Firstly, most organisations would prefer not to block the domain gmx.com. Secondly, it can be difficult to tell the difference between the malicious emails and legitimate private email accounts of the employees. Thirdly, the backdoor does not exploit a vulnerability in Outlook, but rather uses the software in a legitimate way via Microsoft's API – MAPI.[8] It manages to avoid authenticating the user's email account by exploiting his or her previous open session.

PERSISTENCY

In the case of the Outlook variants, the malware hijacks the COM[9] to maintain persistence, while modifying certain CLSID[10] values in the Windows Registry. This results in the execution of the DLL during each reboot of the client's software. It should be noted that in Windows OS, there is a security mechanism designed to prevent the redirection of COM objects to malicious DLL files based on the integrity level of the process. Namely, if the integrity level of a process is higher than medium, the COM runtime ignores per-user COM configuration and accesses only per-machine COM configuration. Nevertheless, in this scenario, this feature fails, as Outlook's process runs at medium-integrity level. Moreover, COM referrals do not require Admin authorisation.

In the case of The Bat!, the threat actors registered a plugin to the client's software that executed the malicious DLL file each time it was opened. The registration of a plugin for The Bat! consists of modifying the following configuration file: %appdata%\The Bat!\ Mail\ TBPlugin.INI. There is no preset path for the Turla Backdoor's DLL file. As such, it can be located anywhere on the hard drive.

RECOMMENDATIONS

Create alerts for anomalies by:

- Blocking emails with PDF attachments sent from the domain gmx.com
- Monitoring and flagging emails with certain subjects sent simultaneously from the same user
- Statistically examining abnormal email sending patterns from the organisation's email address, attached with PDF files
- Disabling the option of sending encrypted emails (creating an alert for emails containing bzip2 compressed data, or data encrypted by modified algorithms associated with Turla: MISTY1, CAST-128, RSA and ThreeFish)
- Creating a rule in the email filter system that blocks and alerts on any email that does not contain a pre-defined character or feature (e.g. a specific file attachment or special notes/characters).

[7] https://github.com/EmpireProject/PSInject
[8] Messaging Application Programming Interface.
[9] Microsoft Component Object Model - a platform-independent, distributed, object-oriented system for creating binary software components.
[10] Class Identifier – a unique global identifier of COM objects, which is comprised of a 128-bit long number and coded in Hexadecimal and recorded on Windows Registry.

REGULATORY CHANGES AND THEIR IMPACTS

PUBLIC DISCLOSURE OF DATA BREACHES WILL LIKELY INCREASE IN 2019

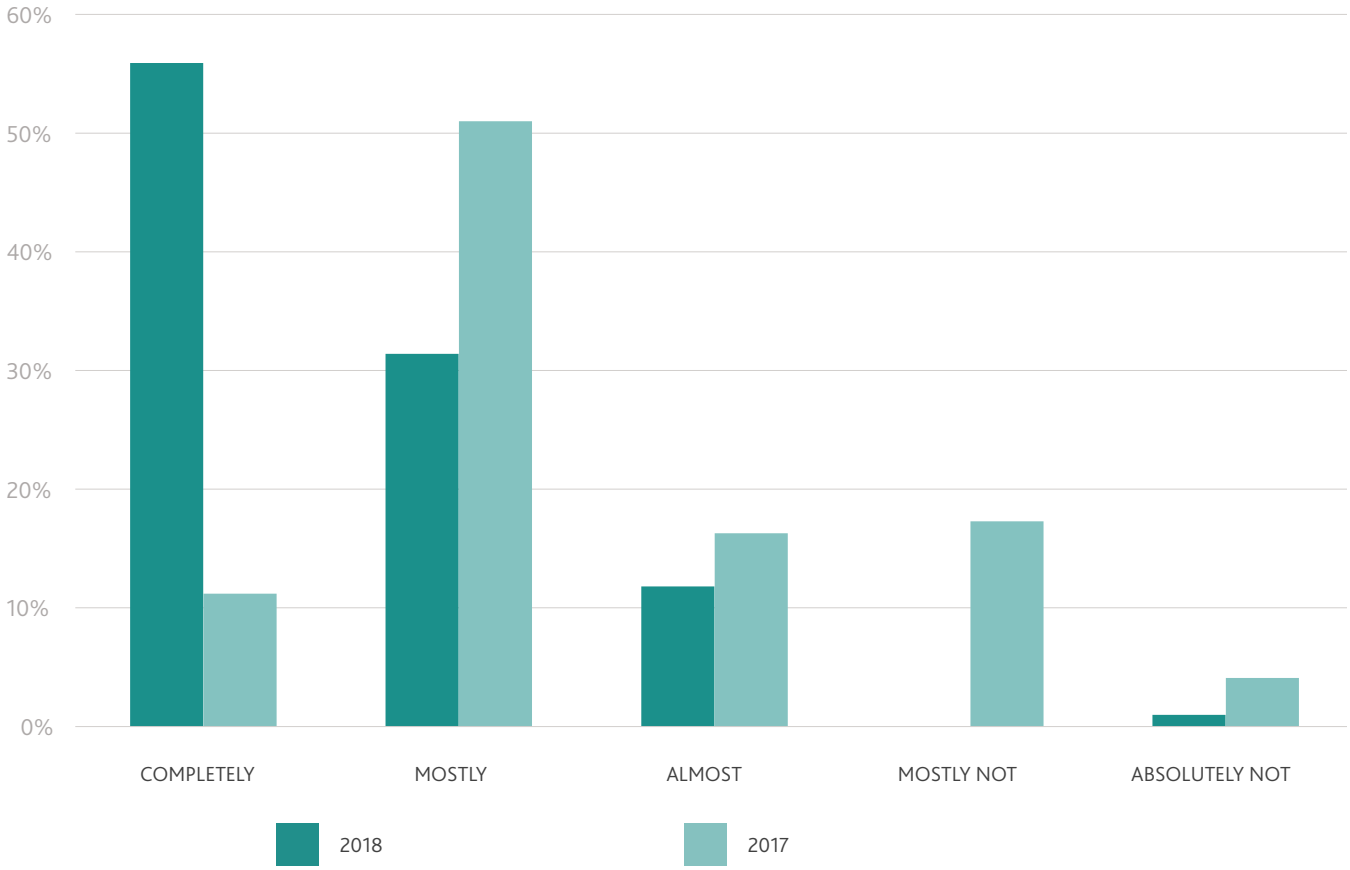
As governments become increasingly agile in responding to the ever-changing nature of cyber security threats, the regulatory landscape also continues to evolve. Naturally, with this increased focus on legislation regarding both cyber security and data privacy, the role of data breach detection, public disclosure and reporting has become significantly more prominent.

HIGH CONFIDENCE IN MEETING NDB OBLIGATIONS

On 22 February 2018, the Privacy Amendment (Notifiable Data Breaches) Act 2017 took effect in Australia. This legislation makes data breach notifications mandatory for organisations subject to the Privacy Act 1988 or with a turnover greater than $3 million per year. Furthermore, this scheme requires organisations to notify affected individuals at risk of serious harm by a data breach within 30 days of discovering the breach. There are significant financial penalties for non-compliance with this legislation of up to $420,000 for individuals and $2.1 million for organisations.

In the 2017 survey, we asked respondents to rate their confidence in meeting NDB compliance obligations. That survey also asked whether organisations who were required to comply with the scheme, had actually planned or implemented key controls necessary to prepare for it. We re-assessed respondents' preparedness for NDB in the 2018 survey and found that organisations were significantly more confident and prepared to meet their NDB obligations (55.9% completely confident in meeting NDB obligations in 2018, up from 11.2% in 2017).

CONFIDENCE IN MEETING NDB OBLIGATIONS - 2017 vs 2018



ORGANISATIONS ARE READY TO COMPLY WITH THE NDB SCHEME

Correspondingly, respondent organisations have placed much greater emphasis on NDB preparation activities such as developing notification processes, response plans and other preparatory controls. Notwithstanding this beneficial uplift and apparent increased commitment to meeting NDB obligations, less than half of these organisations had actually tested their data breach response plans. Our experience is that the activity of exercising response plans commonly reveals simple, yet significant and often overlooked, gaps, allowing them to be adequately identified and remedied before they hinder actual data breach response efforts.

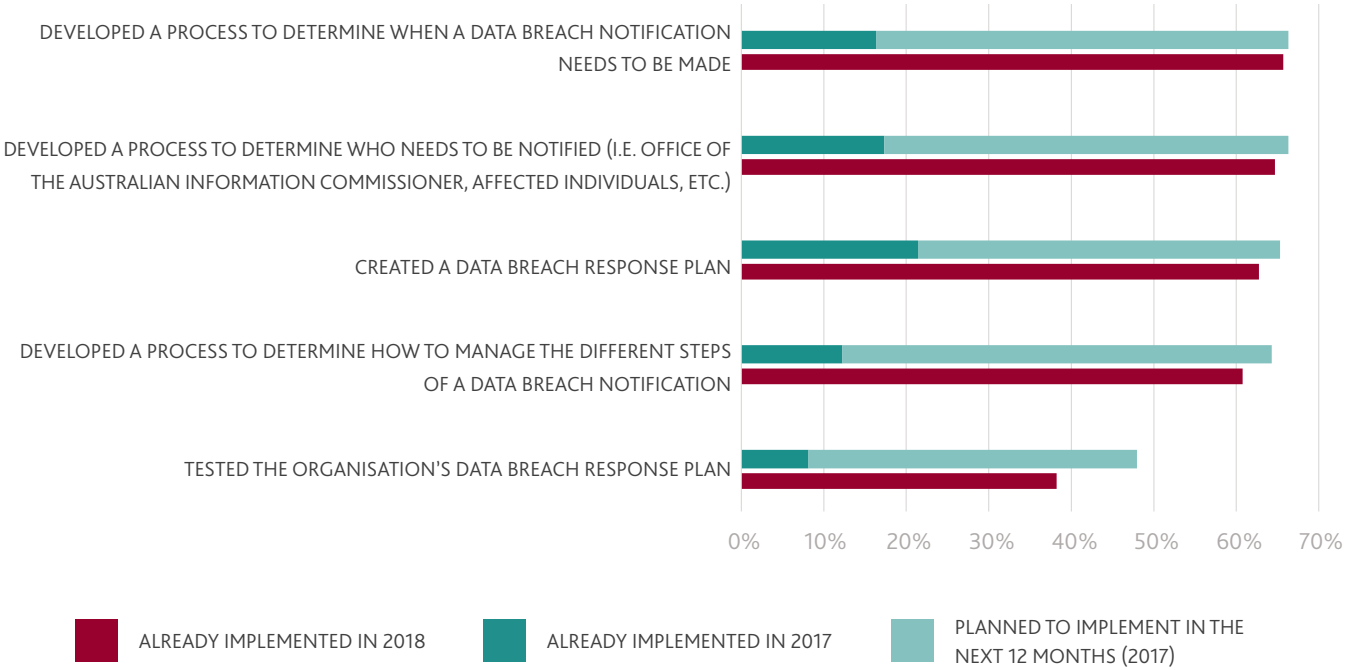
UNCERTAINTY OF GDPR COMPLIANCE REQUIREMENTS

The GDPR introduced new requirements for data protection that took effect on 25 May 2018. The purpose of this legislation is to harmonise data protection regulations across the European Union (EU) and, as described by the OAIC, help "build legal certainty for businesses and enhance consumer trust in online services". GDPR seeks to protect all natural persons in the EU, whether they are citizens of a European country or not.

Some Australian organisations covered by the *Australian Privacy Act 1988 (Cth) (the Privacy Act)* (known as APP entities), may need to comply with the GDPR if they:

- Have an establishment in the EU (regardless of whether they process personal data in the EU)
- Do not have an establishment in the EU, but offer goods and services or monitor the behaviour of individuals in the EU.

NDB PREPARATION ACTIVITIES - 2017 vs 2018



Similar to the Australian NDB scheme, there are significant financial sanctions applicable to organisations for non-compliance, including fines of up to €20 million or 4% of annual worldwide turnover (whichever is higher).

While 18.8% of this year's respondents indicated they were required to comply with the GDPR, 38.8% responded that they did not know whether they were required to comply at all. This uncertainty is somewhat anticipated where a European data privacy regulation is imposed on organisations outside of the European Economic Area (EEA).

LESS THAN HALF OF ORGANISATIONS REQUIRED TO COMPLY WITH GDPR CAN DEMONSTRATE COMPLIANCE

Of respondent organisations that identified the requirement to comply with the GDPR, less than 40% had implemented controls to meet their GDPR obligations. With the GDPR now enshrined in law, this indicates that the majority of organisations required to comply may not be capable of actually meeting their compliance requirements.

DATA BREACH REPORTING BECOMING MORE FREQUENT

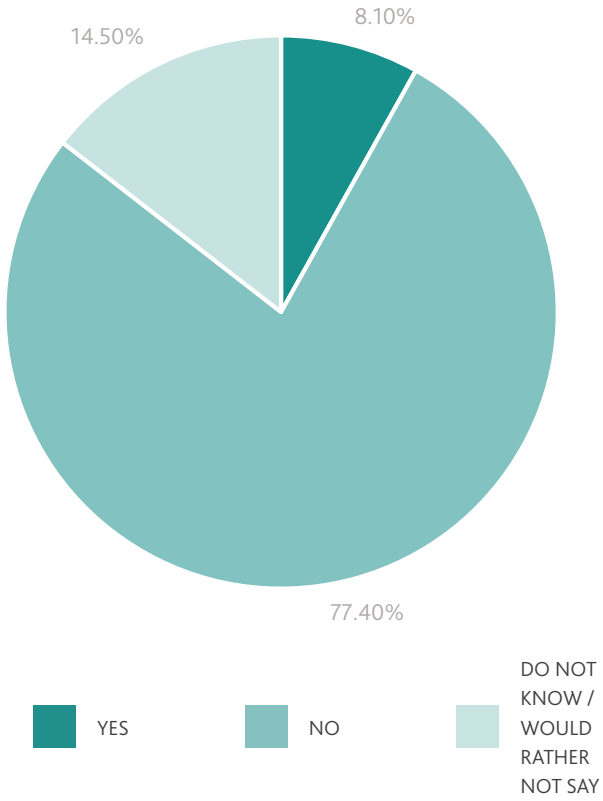
Since the NDB scheme commenced, there has been an increase in the number of data breach notifications made to the Office of the Australian Information Commissioner (OAIC) quarter-on-quarter, resulting in a total number of 812 data breach notifications for 2018[11].

As was seen in 2017, the OAIC's Q4 Report identified that the most common sectors making data breach notifications included health service providers (163), legal, accounting and management services (87), finance (119) and education (62). To a lesser extent, this also included business and professional associations (15), mining and manufacturing organisations (12) and charities (4). It is important to note that notifications made under the *My Health Records Act 2012* are not included in these figures, as they are subject to specific notification requirements set out in that Act.

DATA BREACHES ARE RISING, REPORTING MAY NOT BE KEEPING UP

Examining the 2018 survey results reveals the rising frequency of data breach incidents. Of key interest is that almost 1 in 10 respondent organisations that have experienced a data breach in 2018 and are required to comply with the NDB scheme, have notified the OAIC. Given their prevalence and frequency, this may indicate that some notifiable data breaches have remained unreported. We also note that most occurrences of data breach incidents, with the exception of accidental disclosure, have increased significantly since 2017.

RESPONDENTS THAT HAVE MADE A BREACH NOTIFICATION TO THE OAIC - 2018



[11]https://www.oaic.gov.au/media-and-speeches/news/anniversary-of-notifiable-data-breaches-scheme

CYBER CRIMINALS CHANGED TACTICS AND PREFER DATA BREACHES TO RANSOMWARE

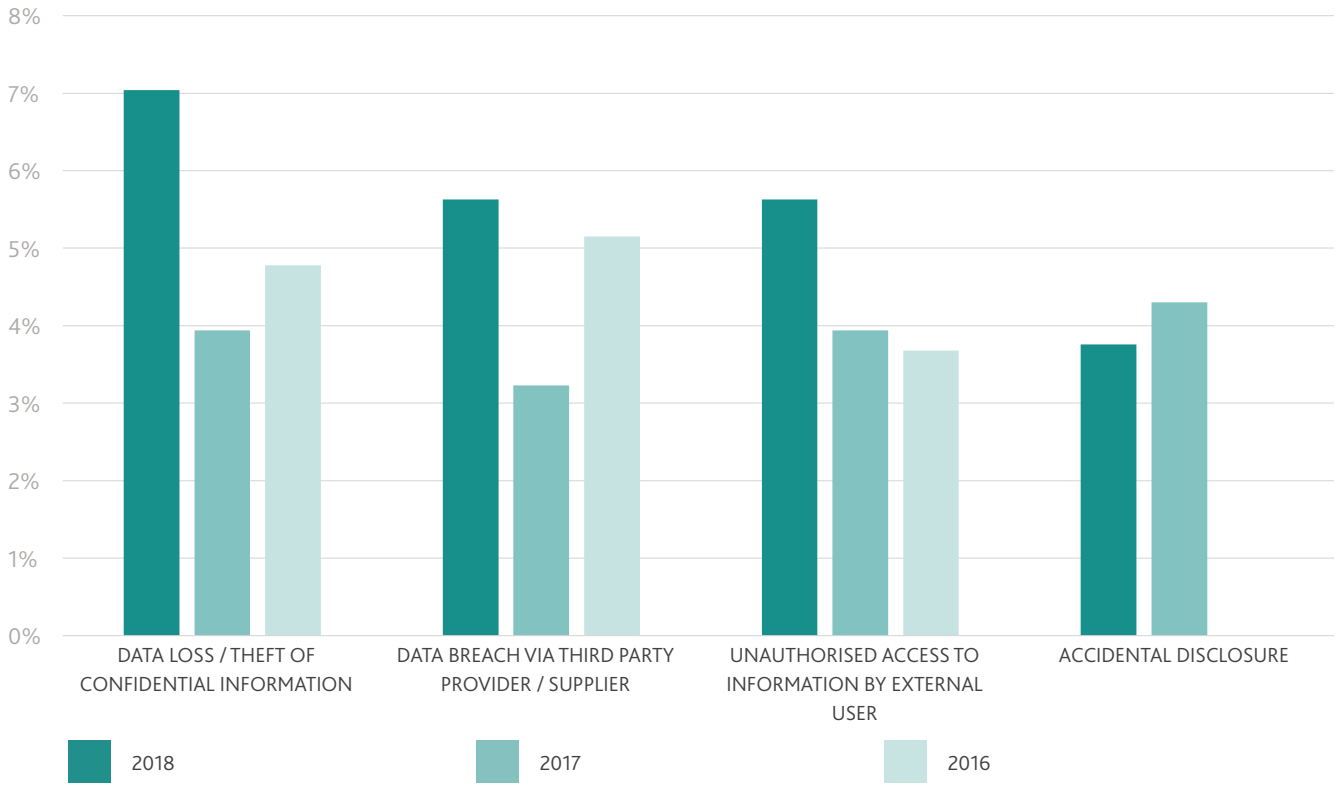
Our analysis of survey results from the past two years suggests that cyber criminals are changing their tactics, with contributing/causal factors that are two-fold:

- Cyber adversaries are changing tactics and realising the value of stolen identity and payment information (as distinct from the potential profits achievable through ransomware as seen in previous years)
- Regulatory changes requiring heightened visibility of data breach incidents have resulted in higher detection/ reporting rates.

MOST DATA BREACHES ARE DELIBERATE AND MALICIOUS

Analysing why data breaches occur, the 2018 survey found the majority of data breaches are reportedly caused by deliberate, malicious attacks. This aligns to the OAIC's latest Q4 NDB Report, which indicated that 64% of data breaches were caused by malicious or criminal attacks. Similarly, our 2018 survey found that one in three data breaches were caused by internal staff inadvertently disclosing information over email (i.e. by emailing the wrong recipient or by using the "Carbon Copy [CC]" feature instead of the "Blind Carbon Copy [BCC]" feature). This precisely mirrors the OAIC's reports, that 33% of data breaches were due to human error.

DATA LOSS FREQUENCY - 2017 vs 2018



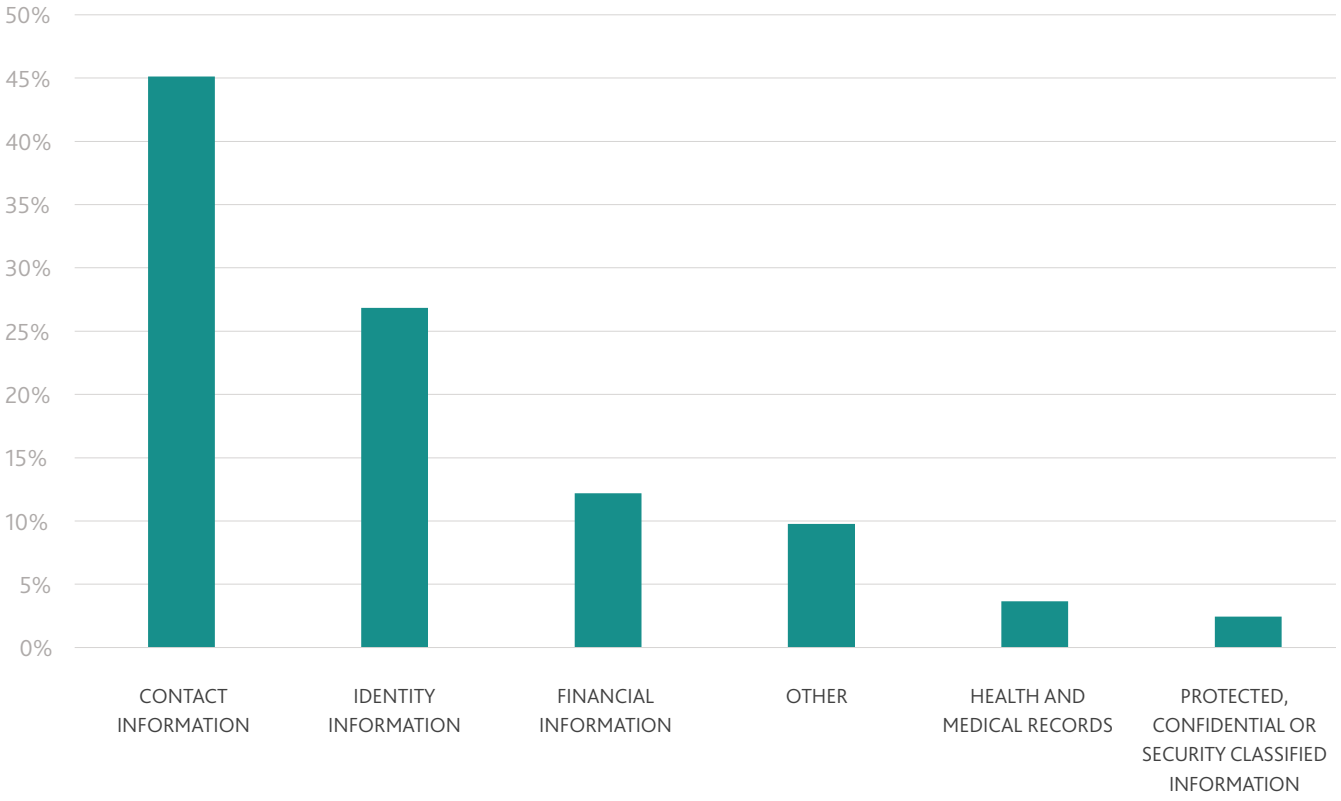
ONE IN FOUR DATA BREACHES FACILITATE IDENTITY THEFT

The 2018 survey found the most commonly breached information type is contact information. Contact information include names (full or partial), physical addresses, telephone numbers, email addresses and usernames. Contact information was impacted in almost half of all data breaches. Alarmingly, more than one in four data breaches involved the compromise of identity information. This is information that can directly enable identity theft and fraud, allowing threat actors to (for example) take out financial loans under the victim's identity. This information includes artefacts such as passport details, birth certificates, drivers' licenses and tax file numbers.

ONE IN TEN DATA BREACHES DIRECTLY ALLOW THEFT OF VICTIM'S FUNDS

More than one in ten data breaches reported in 2018 involved the direct compromise of financial information (including credit card details), in some cases allowing threat actors to directly and rapidly steal funds from the victim's financial institutions. In addition, 2.44% of data breaches involved security classified information, indicating that government information is not immune from data breaches, and it is being actively accessed and exfiltrated by cyber adversaries.

CATEGORIES OF INFORMATION BREACHED - 2018



IMPROVED CYBER MATURITY

REDUCES THE LIKELIHOOD OF SUCCESSFUL ATTACKS

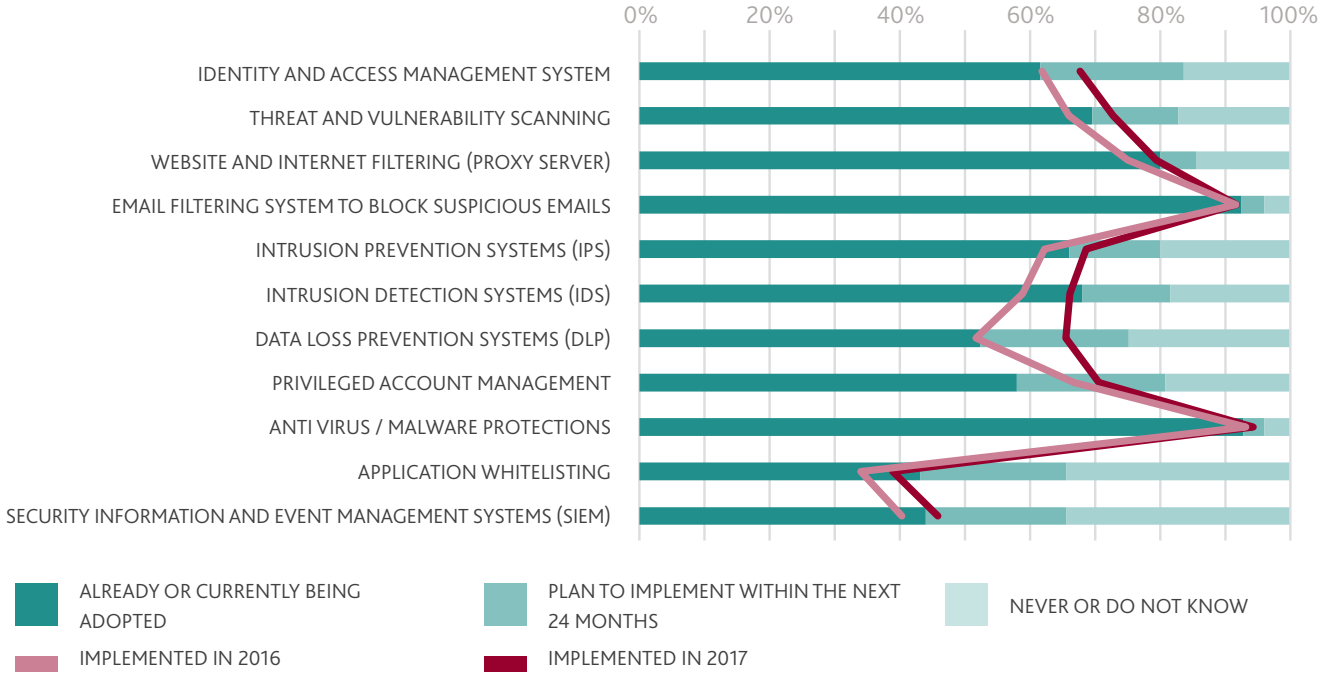
INVESTMENTS IN CONTROLS HAVE CHANGED SIGNIFICANTLY

As seen with incidents, investments in controls have changed and shifted significantly since 2017. There are two likely primary drivers for this:

- Previously discussed significant changes in the regulatory environment, such as the NDB and the GDPR have arguably required organisations to maintain heightened visibility of cyber risk across their organisation, including into their own supply chains. This results in an increased investment in procedural and governance focused cyber security risk management practice
- Organisations are taking proactive steps to implement preventative, predictive, detective and reactive controls to meet the changing tactics, techniques and procedures (TTPs) that are being employed by cyber adversaries, across all classes of threat actor.

In light of the above, it's not surprising that we have witnessed a general shift away from investments in cyber security technology, and a honed investment lens towards those controls that could be more accurately considered procedural and governance based.

IMPLEMENTATION OF TECHNICAL CONTROLS - 2016 TO 2018

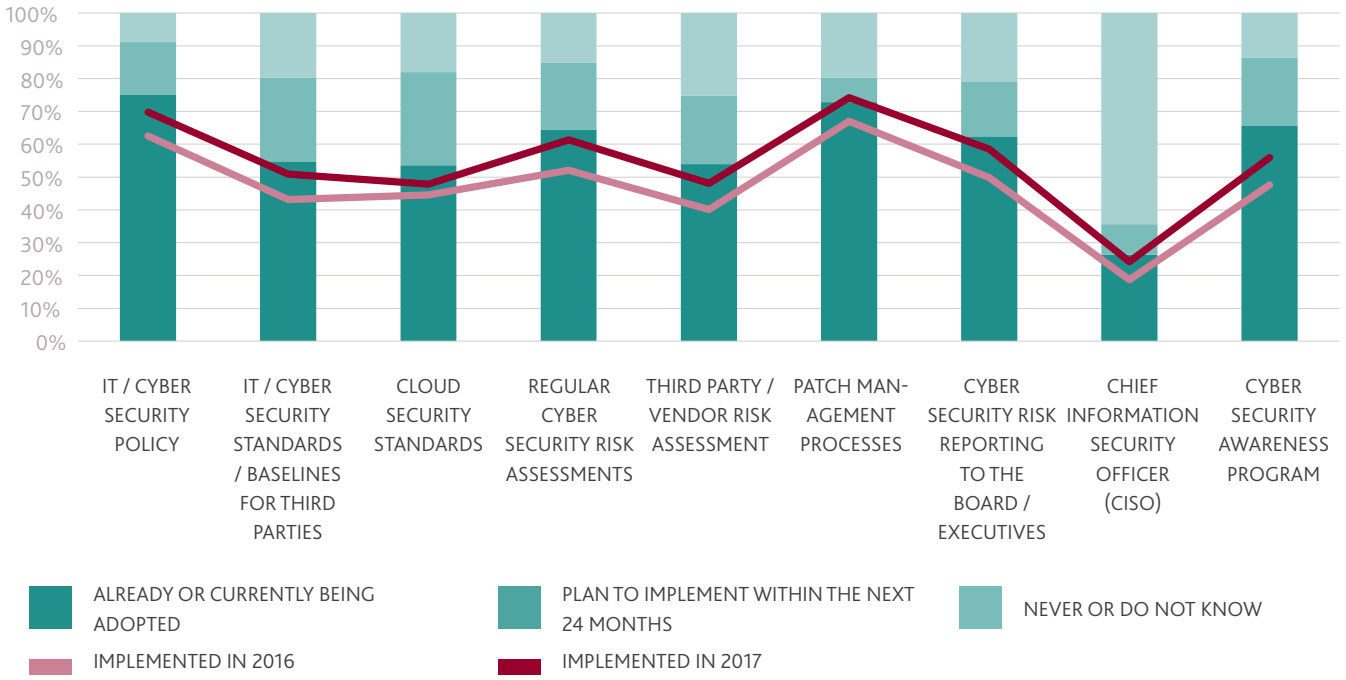


As we specifically examine the survey responses concerning the implementation of technical controls from 2016 to 2018, two downward trends and one upward trend are immediately noted:

- 65% of survey respondents indicated they had implemented a Data Loss Prevention system (DLP) in 2017, versus only approximately 52% in 2018, representing an approximate 20% year-on-year reduction
- 70% of survey respondents indicated they had implemented a privileged account management technical control in 2017, compared to approximately 58% in 2018, representing an approximate 17% year-on-year reduction
- 39% of survey respondents indicated they had implemented application whitelisting in 2017, whereas approximately 43% had put in place the same control the following year, representing an approximate 10% year-on-year improvement.

As an aside, we note that both privileged account management and application whitelisting are considered part of the Australian Signals Directorate (ASD)/Australian Cyber Security Centre (ACSC)'s Strategies to Mitigate Cyber Security Incidents Essential Eight[12]. These prioritised mitigation strategies are designed to assist organisations in protecting their systems against a range of cyber threats.

IMPLEMENTATION OF PROCESSES AND STANDARDS - 2016 TO 2018



[12]https://acsc.gov.au/infosec/mitigationstrategies.htm

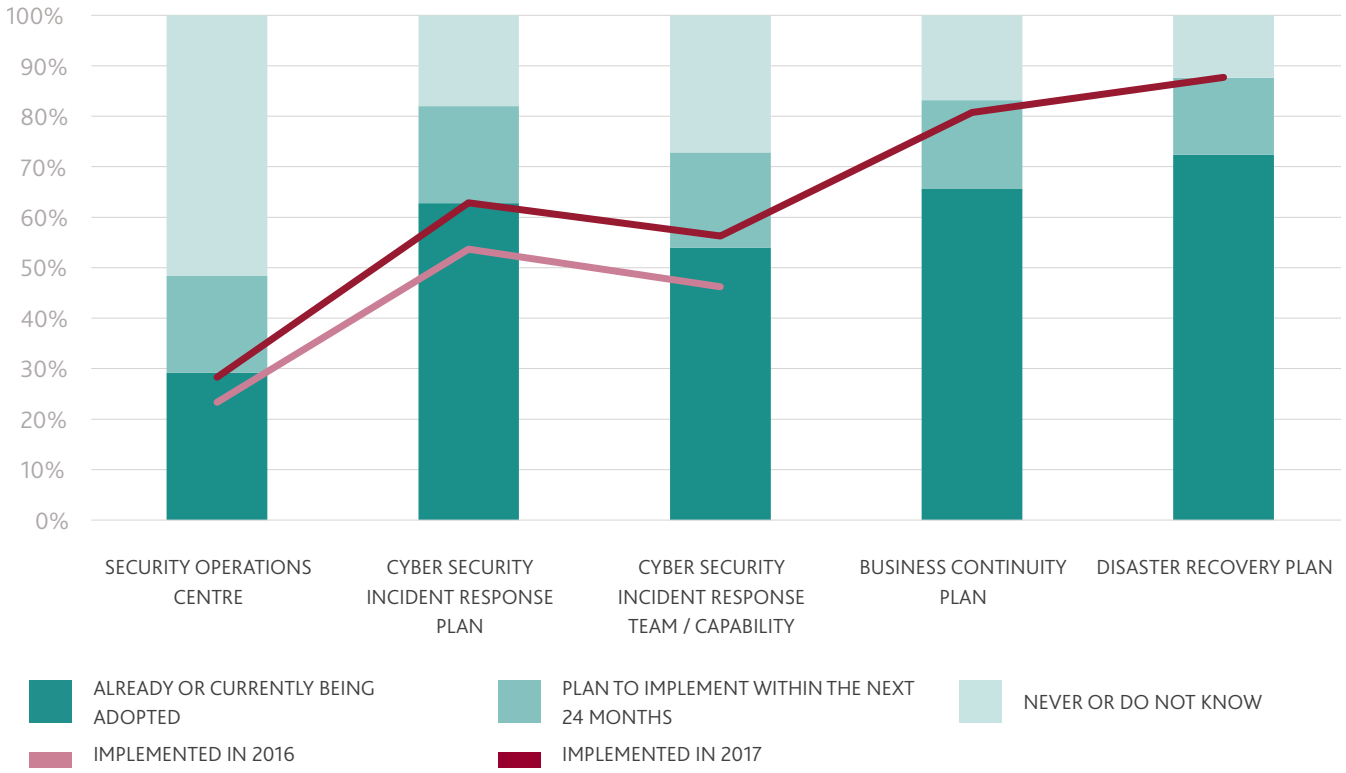
When we examine respondents' implementation of processes and standards from 2016 through to 2018, we observe further evidence of these shifts away from specific cyber security technologies and towards more general processes and standards.

We note with positive interest that:

- Cyber security awareness programs have been adopted nearly 20% more often as compared to 2017
- There was a 12% year-on-year increase in both third party vendor risk assessments and cloud security standards as compared to 2017.

The benefits to organisations seeking to improve both their resilience and improve their maturity through the implementation of a cyber security awareness program cannot be understated. In short, if they lessen the likelihood of their organisation being breached, they will likely be more capable of meeting regulatory requirements and experience an uplift in the organisation's overall cyber security culture.

IMPLEMENTATION OF INCIDENT RESPONSE CAPABILITIES - 2016 TO 2018



AN INCREASED FOCUS ON PREPARATORY AND PROTECTIVE CONTROLS

Managed detection and response functions with advanced capabilities are being more frequently sought by organisations seeking to acquire the necessary resources and skills to detect data breaches. Trend data between 2017 and 2018 highlights this. During this period there has been:

- A 15% year-on-year increase in the number of respondents stating they have already adopted, or are currently adopting, a security operations centre
- An 11% year-on-year increase in the number of respondents stating they have already adopted, or are currently adopting, a cyber security incident response plan.

We also note with some concern that certain aspects of planning and preparation for cyber security incidents have decreased.

Incident response capabilities such as a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) have actually decreased, by approximately 10% year-on-year and 8% year-on-year correspondingly. This may suggest fewer organisations are developing, refining and, most importantly, rehearsing these plans. This is a critical point to note in the event of a real world cyber security incident.

As discussed elsewhere in this report, these specific incident response capabilities are critical and can directly contribute to detection capabilities and also reduce the potential impact of data breaches and cyber security incidents.

CASE SPOTLIGHT

BUSINESS EMAIL COMPROMISE (BEC)

The work details of 30,000 Victorian public servants were stolen in a data breach, after part of the Victorian Government staff directory was downloaded by an unknown party.

What happened?

In December 2018, an unauthorised third party accessed and downloaded what is believed to be a 'partial copy' of the Victorian state government employee directory, identifying approximately 30,000 public service staff and contractors. The investigation revealed that it appears the third party was able to illicitly access this information after initially compromising an employee's email account.

What was targeted?

The employee directory/list is available to government employees and contains work emails, job titles and work phone numbers. Additionally, users affected by the breach were informed via email that their mobile phone numbers may have also been accessed if this information had been entered into the directory. It is worth noting that while it did not appear highly personal or sensitive information had been stolen, the dataset as a whole could be useful for a more targeted attack or as part of other broader cyber-criminal activities.

What was the impact?

It is likely affected users would experience increased phishing, spam and social engineering attempts using the leaked information, particularly via the work email address and any telephone numbers disclosed. A major data breach such as this will also impact the reputation of the Victorian Government and its ability to adequately protect information. The case was referred to Victoria Police and specialist agencies including the Australian Cyber Security Centre for further investigation.

CYBER RESILIENCE

MORE WORK REQUIRED TO REDUCE IMPACTS

PRIOR PLANNING AND PREPARATION INCREASES DETECTION OF DATA BREACHES

The 2018 survey found that organisations with a cyber security incident response plan and capability detected and responded to more data breach incidents than those without. In 2018, organisations with planning and preparation were 3.5 times more likely to detect data breaches via third party suppliers and providers when compared to organisations without planning and preparation.

It is unlikely organisations experience more data breaches because they have established plans and preparations. Rather, those with incident response plans and preparations are likely reporting more data breaches than those without because of their improved capability to detect them. Following from this, a confronting prospect is to be considered; that data breaches are occurring more frequently, and detected less often, than many organisations realise.

PRIOR PLANNING AND PREPARATION REDUCES INCIDENT IMPACTS

Prior planning and preparation allows organisations to adopt an ever forward-leaning posture in the face of cyber attacks. Where incidents occur, organisations that have planned and prepared ahead of time understand how to respond immediately and effectively. This capability to rapidly detect and analyse, contain, eradicate and recover from cyber security incidents is a key contributor to reducing their impacts.

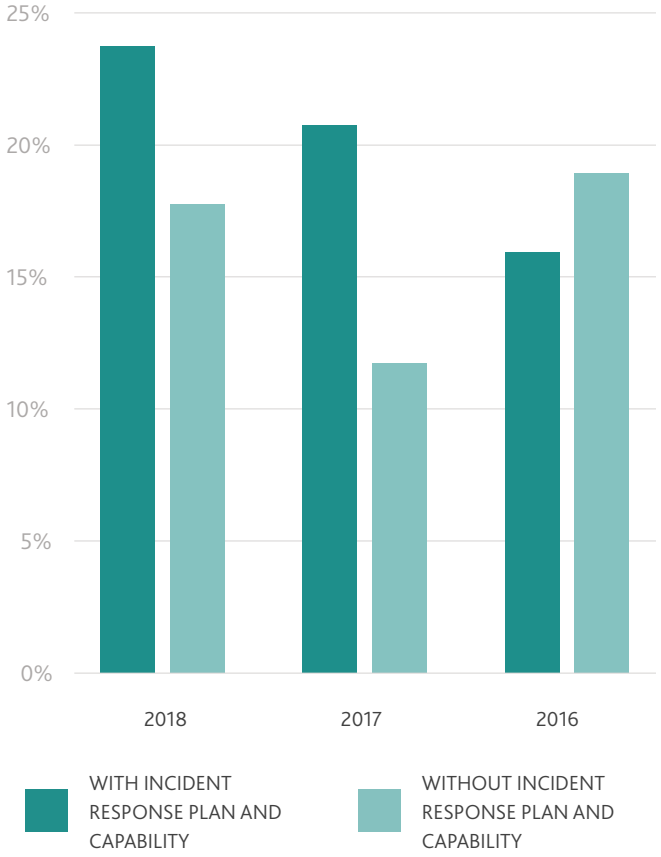
INCIDENT RESPONSE PLANS AND CAPABILITIES REDUCE THE DISRUPTION, DURATION AND REPUTATIONAL DAMAGE OF CYBER SECURITY INCIDENTS

Across both 2017 and 2018, organisations with plans and preparations in place have experienced reduced incident impacts. These include:

- Less disruption and downtime
- Shorter incident durations
- Minimised reputational damage.

To be effective in not only preventing incidents, but reducing their impact and damage when they do occur, organisations need to be proactively establishing, rehearsing and optimising incident response plans and capabilities.

DATA BREACH INCIDENTS DETECTED - WITH AND WITHOUT PLANNING AND PREPARATION - 2016 TO 2018



DATA BREACHES HAVE LESS TANGIBLE IMPACTS THAT CANNOT BE INSURED

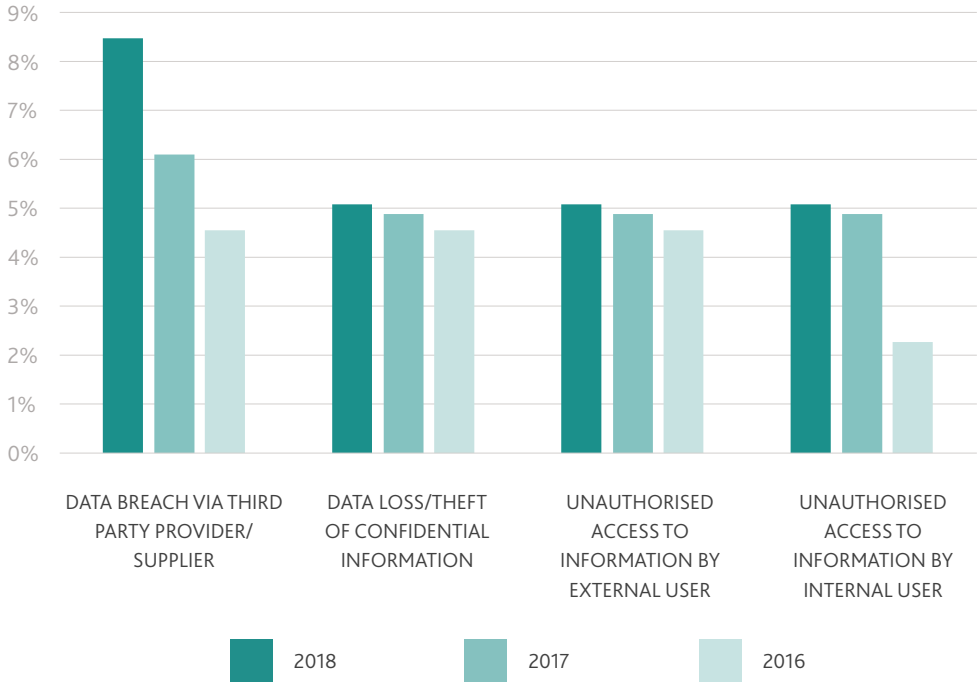
Directly linked to higher generation of profits, a brand's value is often considered one of its most important, yet intangible assets. The general makeup of an organisation's brand can be understood through the key contributors to its reputation – which include its perceived trust and strength. As a double-edged sword, the public's awareness of information security has generally increased, largely driven by high profile data breaches and global cyber security incidents with intense media coverage. As this awareness increases, it has also engendered a sense of public distrust. Numerous academic studies have cited distrust of information security as a hindrance to the adoption of services by consumers, which translates to an opportunity cost for organisations.

Information security and cyber security risk management is inextricably linked to the health of an organisation's reputation, and therefore brand (a powerful contributor to any organisation's bottom line). To strengthen the reputation is to support the brand – and to do so, organisations globally (and across all industries) have quickly recognised the returns on information security investments. The costs of a data breach, both direct and intangible, now often outweigh the cost of their mitigation.

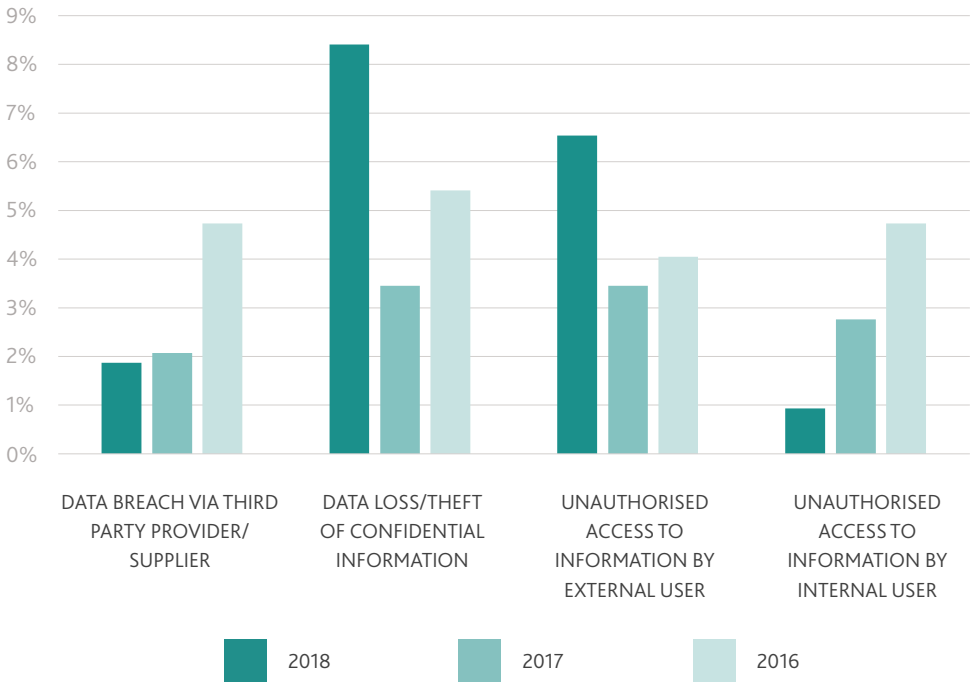
REPUTATIONAL DAMAGE PUSHES THE BOTTOM LINE DOWNWARDS

The costs of an information security incident have, traditionally, been difficult to quantify. In recent times, numerous sources provide estimates and averages for the cost of data breaches specifically (most notably research work from Ponemon Institute's Cost of a Data Breach Study). Typically, these evaluations quantify the cost of a data breach in terms of 'cost per record'. Often, these estimates are based on simple calculations of the average direct costs attributed to responding to a data breach, such as third-party specialist advice, forensics, the cost of purchasing new systems, the cost of priority response from services providers, and the average size of the data breach. While these are simple estimations of the direct costs of cyber security incidents, wider reputational impacts can have even heavier (and traditionally more difficult to quantify) costs attributed to them.

DATA BREACH INCIDENTS DETECTED - WITH PLANNING AND PREPARATION - 2016 TO 2018



DATA BREACH INCIDENTS DETECTED - WITHOUT PLANNING AND PREPARATION - 2016 TO 2018



INCIDENT IMPACTS - 2018

INCIDENT IMPACTS - 2017

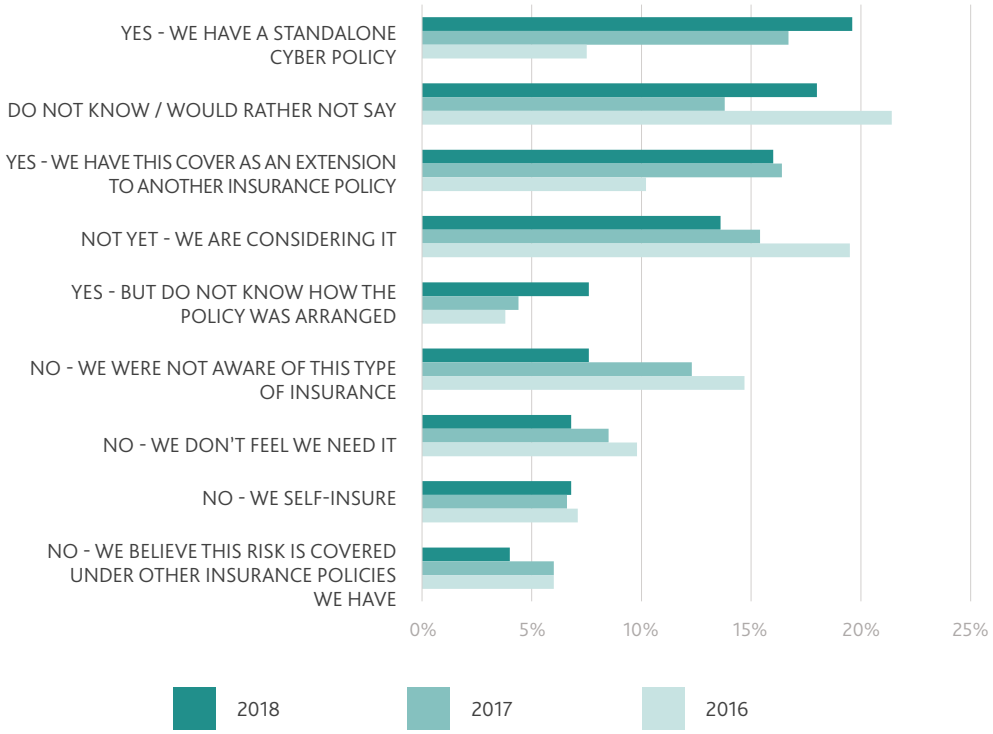
INCREASING ADOPTION OF CYBER INSURANCE

The number of respondents indicating they have adopted cyber insurance has increased. Similarly, less organisations perceive that cyber risks are covered by other insurance policies.

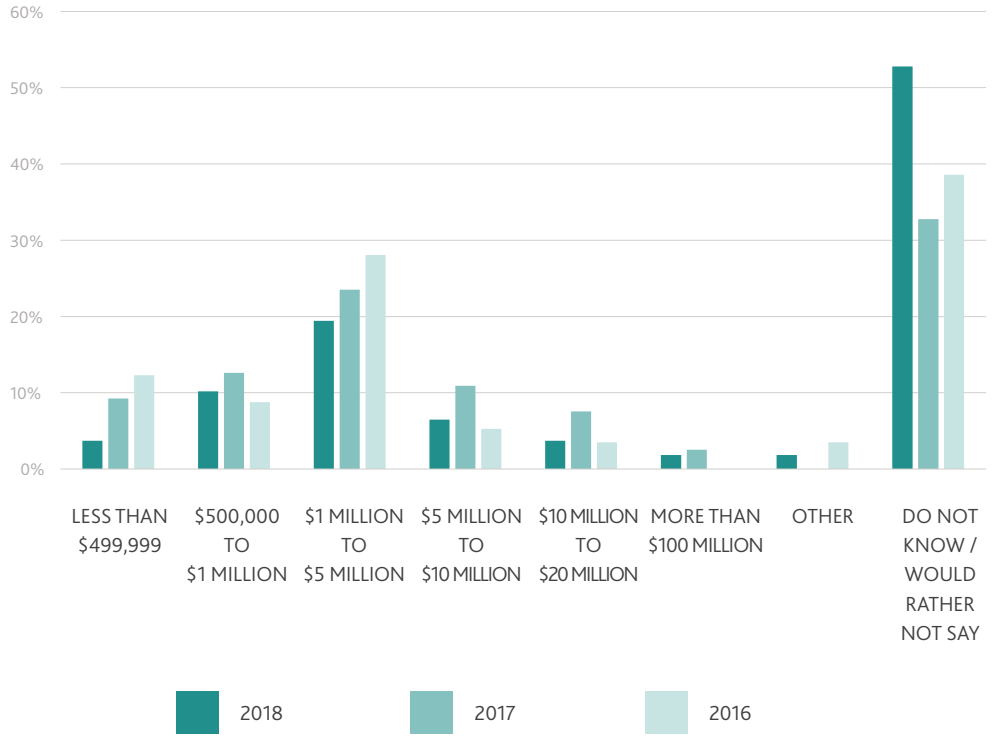
UNCERTAINTY OF CYBER INSURANCE COSTS AND COVER

The 2018 results suggest organisations are becoming increasingly confident in the decision to adopt cyber insurance. Despite this, they also seem less certain on their premium costs and levels of cover compared to previous years. This could be indicative of an emerging awareness of and appreciation for cyber insurance, and its subsequent adoption without deeper levels of consultation.

UPTAKE OF CYBER INSURANCE - 2017 vs 2018



LEVEL OF CYBER INSURANCE COVER - 2017 vs 2018



SURVEY METHODOLOGY

BDO and AusCERT deliver annual cyber security surveys to identify industry trends across private and public small to medium sized organisations across the Asia Pacific region.

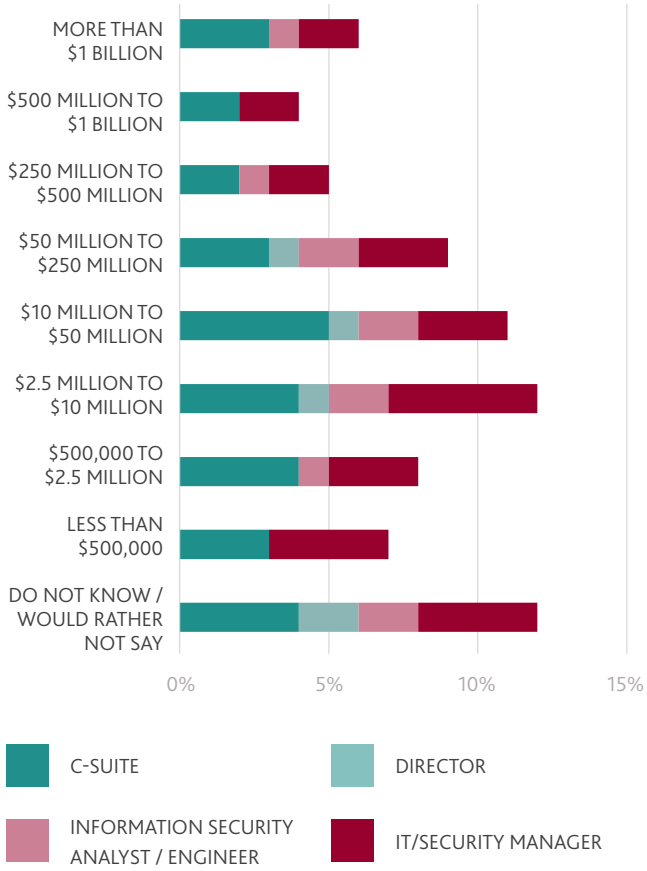
Prior to launching the BDO and AusCERT Cyber Security Survey in 2016, we found that most existing cyber security benchmarking data focused on multinational organisations in other global regions, making it difficult for Australian and New Zealand organisations to contextualise the findings and realise value through relevant, actionable insights. The data collected within this Survey Report provides a more relevant benchmark for organisations in Australia and New Zealand, who are not necessarily subject to the international legislations that have driven cyber security growth in the United States and Europe.

In 2018, we conducted the third annual BDO and AusCERT Cyber Security Survey. We received strong support from industry, with almost 500 respondents across a variety of industry sectors. Of these respondents, 74.4% were based in Australia, 20% were based in New Zealand, while 5.6% were based internationally.

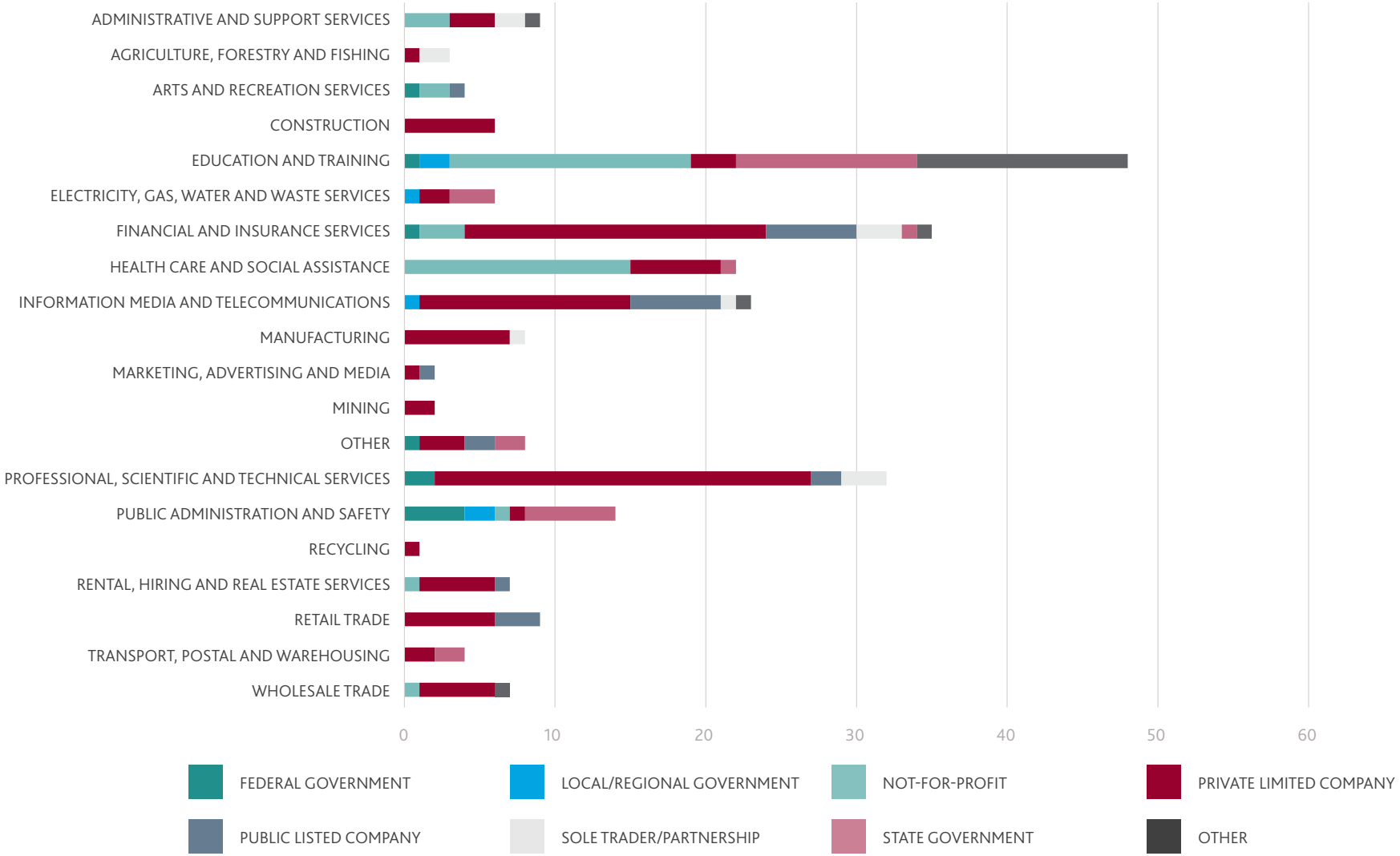
Our survey covered a wide variety of organisation types across a range of industry categories, now demonstrating a greater percentage of respondents from the education and financial sectors compared with previous years. The data set contained all industry sizes, but particularly focused on small and medium sized businesses. The individuals completing the survey were closely connected to cyber security and their organisation's risk management responsibilities:

- 40.4% were C-level executives
- 28% were IT/Security Managers
- 7.6% were Security Analysts/Engineers
- 1% were Internal Auditors
- 23% were in other roles.

RESPONDENTS BY ORGANISATIONS' ANNUAL REVENUE



RESPONDENTS BY ORGANISATION TYPE AND SECTOR



ABOUT BDO IN AUSTRALIA AND BDO IN NEW ZEALAND

BDO is one of the world's leading accountancy and advisory organisations, with clients of all types and sizes, in every sector. Our global reach and strong collaboration across countries allows our cyber experts to keep abreast of industry developments and the emergence of new and evolving cyber security threats.

BDO's Cyber Resilience Framework allows us to work alongside our clients to ensure they take a strategic view of their entire cyber security risk management lifecycle. As a result, they can better understand the evolving cyber risk landscape, potential impacts on their business, and build their cyber resilience over the long term with expert guidance along the way.

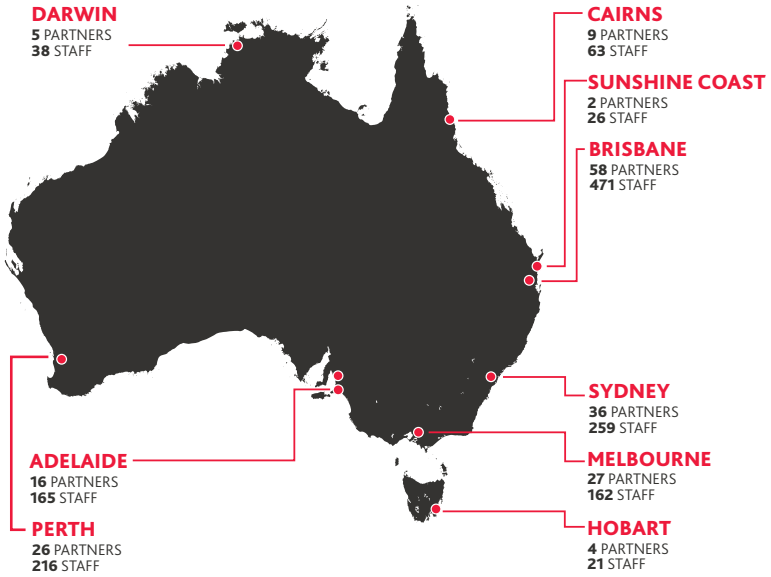
As a result of our client partnership approach, our cyber teams develop strong insight into their clients' business, enabling them to find innovative ways to help clients maximise their growth opportunities, improve processes and avoid pitfalls.

BDO has 1,500+ partners and staff across Australia, making us one of the country's largest associations of independently owned accounting practices. We have offices in New South Wales, Northern Territory, Queensland, South Australia, Tasmania, Victoria and Western Australia.

In New Zealand, BDO has more than 800 partners and staff in 15 offices across the North and South Islands, and BDO is the fastest-growing business services firm in the country.

For more information about BDO services, visit www.bdo.com.au or www.bdo.co.nz.

1,642 PEOPLE
10 OFFICES
183 PARTNERS
FIGURES TAKEN AS AT 01 APRIL 2019



800+ PEOPLE
15 OFFICES
88 PARTNERS
FIGURES TAKEN AS AT 01 APRIL 2019

Growth
The fastest growing business services firm in New Zealand.

Backing smart NZ business
We support over 28,000 SME, mid-market and corporate clients across New Zealand, helping them achieve their business success.

ABOUT AUSCERT

AusCERT (the Australian Cyber Emergency Response Team) is a membership-based, independent, not-for-profit security team, which is part of The University of Queensland.

AusCERT has a national focus across industry and government and has a national and global reach.

Established in 1993, AusCERT is one of the oldest cyber emergency response teams in the world. AusCERT services help organisations prevent, detect, respond and improve their resilience to cyber attacks.

For more information about AusCERT services, visit www.auscert.org.au.

AUSCERT

1300 138 991
www.bdo.com.au

Distinctively different - it's how we see you
AUDIT • TAX • ADVISORY

NEW SOUTH WALES
NORTHERN TERRITORY
QUEENSLAND
SOUTH AUSTRALIA
TASMANIA
VICTORIA
WESTERN AUSTRALIA