2019 CYBER SECURITY SURVEY

AUSCERT

FOREWORD

Organisations and individuals alike are readily embracing the opportunities presented by technology. Our physical world is intrinsically bound to its digital counterpart. No longer are we just sensing or perceiving the world around us with technology, we are actively changing it. This capability has been driven further with the rise of ubiquitous technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI). As the complexity and extent of digital capabilities grow, so too does our reliance on them. While we seek to capitalise on the opportunities of 2020 and beyond, we must also be prepared to defend against the threats that emerge from the use of such technology.

The 2019 BDO and AusCERT Cyber Security Survey Report highlights the cyber security trends, changes, challenges and risks faced by Australian and New Zealand businesses. The survey results present an interesting contrast in terms of both recurring themes and shifting investments. Businesses are moving away from vendor technology as 'silver bullet' solutions, instead, they are investing more on security governance processes. We learnt that when respondents adopt a set of key controls, they face significantly fewer incident impacts and less complex cyber risk management challenges. Yet, while the adoption of key controls has empowered some organisations to understand their cyber risks, most respondents continue to misinterpret who is attacking them and how they are doing so.

Interestingly, the report findings also pinpoint a continual disparity between the types of incidents respondents expect versus the types of incidents they actually experience. Similarly, the survey data highlights that respondents continue to underestimate the cause of most incidents – with insider threats two times more common than expected.

As phishing once again takes the lead as the most common incident, we are reminded of the importance of cyber security education, training and awareness among employees. This goes hand-in-hand with our report's findings on the prevalence of Business Email Compromise and Payment Redirection Fraud – the first time we've surveyed respondents on these kinds of attacks.

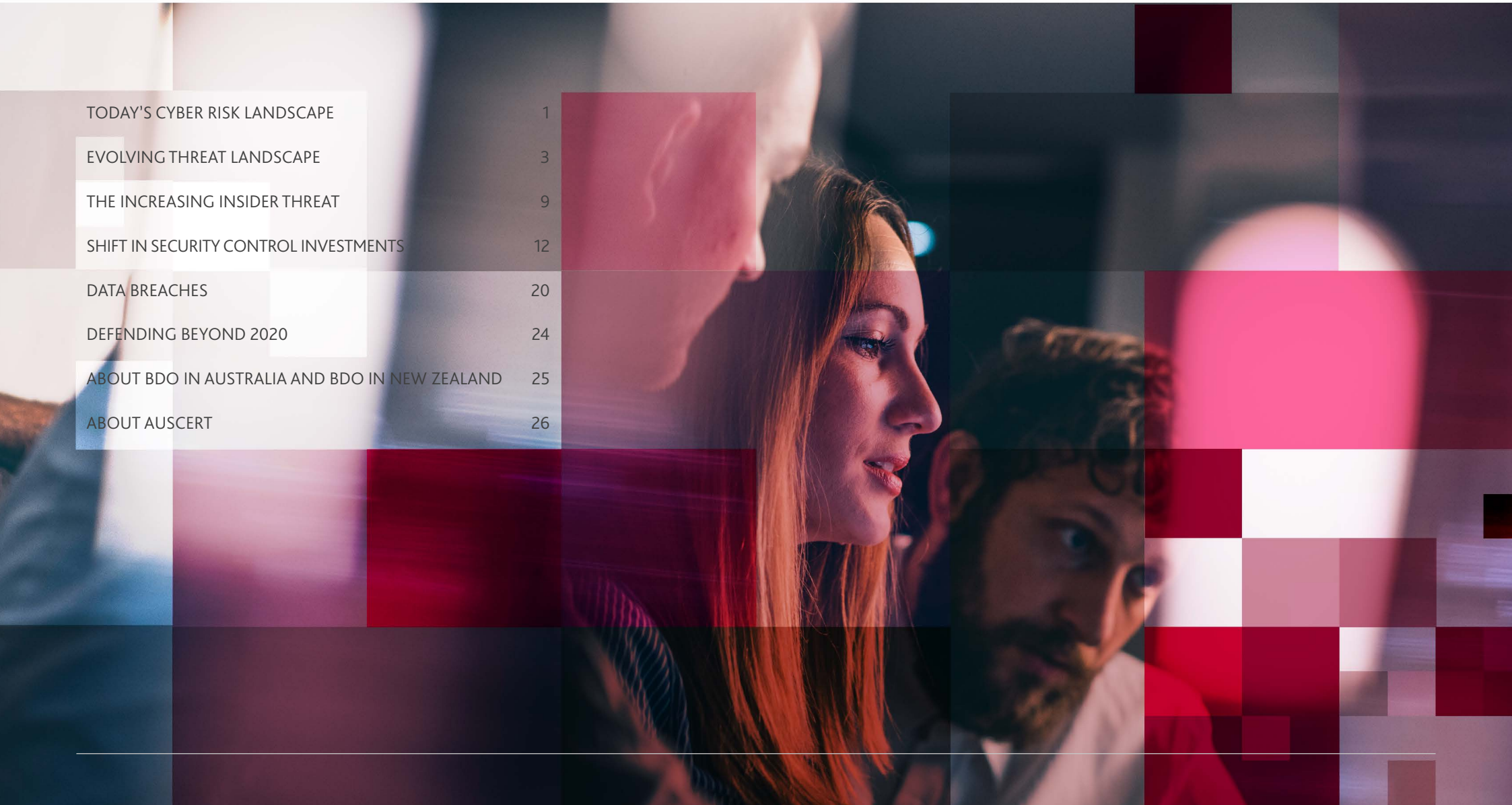
This detailed survey report dives into these findings, providing you with insights into what cyber risks Australian and New Zealand businesses are facing, and where they are investing time, resources and funds to manage them. By leveraging the insights of this report, organisations can take a proactive approach to threat-based cyber security in their mission to establish resilience.

Thank you to all participants in this years' survey, and also those who took part in our previous surveys since 2016. Without your honest input and ongoing support, we couldn't obtain and analyse the data that represents the collective state of cyber risk management efforts across our region. We greatly appreciate the effort you put into supporting the survey and look forward to furthering our understanding of the cyber threat risk landscape for Australian and New Zealand businesses with you.

Leon Fouche
National Cyber Security Leader,
BDO

David Stockdale
Director,
AusCERT

CONTENTS



TODAY'S CYBER RISK LANDSCAPE

There is no escaping technology in today's modern economy. Whether it be for personal, organisational or social means, the reliance on technology is constantly increasing. Consider this, to access online services today we need a computer, an email address and a mobile device for multifactor authentication. At work, most staff receive a computer or mobile device as standard. Technology is a pervasive element of our daily lives in Australia and New Zealand. Every day, new devices are introduced to the global ecosystem and more people join the online community. This permeation of technology across all elements of society has also seen the digitisation of information (enter 'The Cloud'), making it easier than ever to access. As a result, organisations and businesses have moved online, not only to meet customer demand but to give their staff efficient access to organisational information.

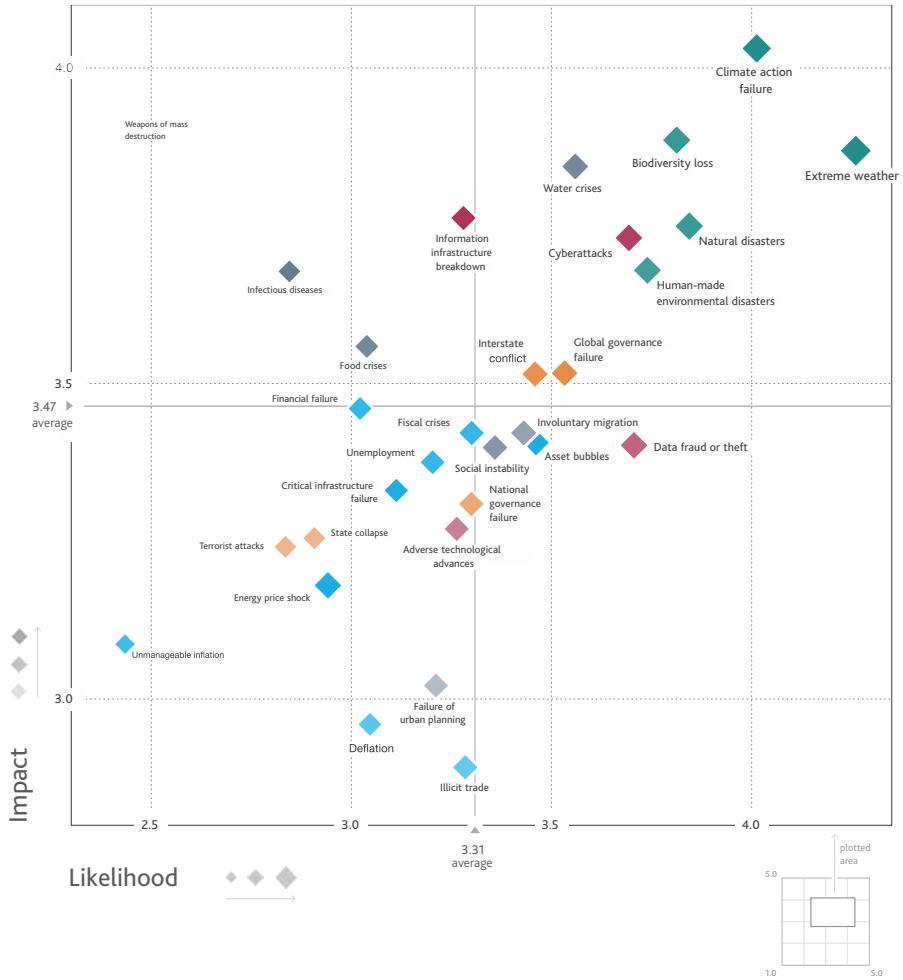
This adoption of cloud technology provides benefits to organisations beyond the realms of the Information Technology (IT) team. It decreases the reliance on staff attending a traditional office setting, allowing them to work remotely with flexible working arrangements. This operating model results in an overlap between the work and personal lives of staff, and it has a flow-through effect on the threat and risk profiles for organisations and data exchange. The willingness and capability for organisations to recognise and adjust to this modern way of operating is a key theme of this report. As the way we work changes, the complexities in identifying and addressing information security risk can be difficult, not just for individuals and small to medium businesses, but also for larger organisations as well.

TECHNOLOGY RISK IS A GLOBAL PRIORITY

Organisations are recognising that technology and cyber security risk is a critical concern. The World Economic Forum's (WEF's) Global Risk Report 2020 analyses organisations' forward perceptions of risk until 2030. Since 2012, cyber security attacks and data fraud have appeared in the top five global risks in terms of likelihood, with increasing regularity. This trend demonstrates an understanding by organisations of the potential impact of cyber security breaches and attacks. In 2020, with climate change at the forefront of public discussion, it is unsurprising to see wide-scale natural disasters and other climate change associated concerns become the highest-rated risks in terms of likelihood. Immediately following these though are data fraud or theft and cyber attacks. The fact cyber security risk rates so highly, despite so many pressing global concerns, highlights the likely view of many organisations that cyber attacks and data loss are inevitable in the current global landscape.

When it comes to impact, information infrastructure breakdown and cyber attacks remain in the top 10, listed at sixth and eighth respectively. For Australian and New Zealand businesses, this means a shift in focus towards building cyber resilience is required. While it's getting harder to maintain total control over the likelihood of a cyber event due to the changing technology landscape, managing the impact of an incident is becoming more important. By implementing the right controls and testing them thoroughly to ensure they are sufficient, organisations have a better chance of recovering from an incident and ensuring continuity. The WEF's Global Risk Report highlights that, as a global community, the consequence of information and cyber security risk is increasing. This leads us to ask whether this understanding is reflected by Australian and New Zealand businesses. Are we doing enough?

THE GLOBAL RISK LANDSCAPE 2020



Top 10 risks in terms of **Likelihood**

1. Extreme weather
2. Climate action failure
3. Natural disasters
4. Biodiversity loss
5. Human-made environmental disasters
6. Data fraud or theft
7. Cyberattacks
8. Water crises
9. Global governance failure
10. Asset bubbles

Top 10 risks in terms of **Impact**

1. Climate action failure
2. Weapons of mass destruction
3. Biodiversity loss
4. Extreme weather
5. Water crises
6. Information infrastructure breakdown
7. Natural disasters
8. Cyberattacks
9. Human-made environmental disasters
10. Infectious diseases

Categories

- Economic
- Environmental
- Geopolitical
- Societal
- Technological

Source: World Economic Forum Global Risks Perception Survey 2019–2020.

Note: Survey respondents were asked to assess the likelihood of the individual global risk on a scale of 1 to 5, 1 representing a risk that is very unlikely to happen and 5 a risk that is very likely to occur. They also assessed the impact of each global risk on a scale of 1 to 5, 1 representing a minimal impact and 5 a catastrophic impact. To ensure legibility, the names of the global risks are abbreviated; see Appendix A for the full name and description.

EVOLVING THREAT LANDSCAPE

LIMITED UNDERSTANDING OF THE RISKS

Last year's BDO and AusCERT Cyber Security Survey Report found that cyber security risk management was maturing. This year, the adoption of regular information security risk assessments has continued to increase, but the data also indicates Australian and New Zealand organisations still have a work to do to fully understand the relevant cyber security threats and risks they could face, as shown by the graph on the right.

To be fair, in the cyber domain certainty is limited and complexity is increasing. One of the reliable constants is that the threats an organisation faced yesterday will not be the threats experienced tomorrow. Maintaining an adequate degree of resilience requires an organisation to constantly assess the threat landscape and improve its cyber readiness posture. So, what is it that Australian and New Zealand organisations could be missing when looking to understand and contextualise the risk?

CYBER SECURITY INCIDENTS: 2016 - 2019

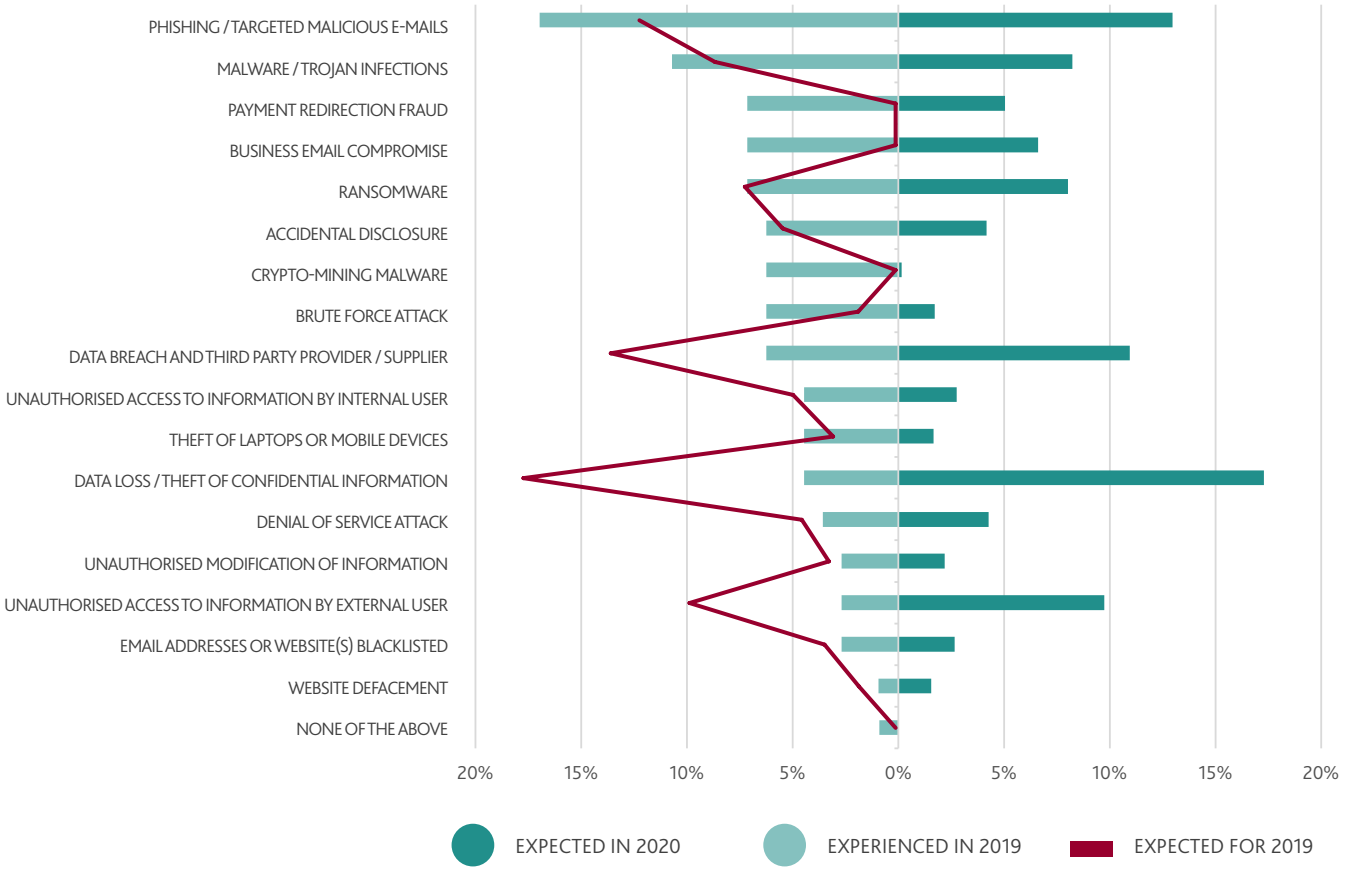
CYBER ATTACKS ARE UNDERESTIMATED

In Australia and New Zealand, it is clear the prevalence of different attack vectors may not be well understood. When asked in 2018 which attacks were most likely to be experienced in 2019, respondents held the firm view that data loss and theft of confidential information would be the most common attacks they face. Looking at the data for incidents experienced in 2019, respondents highlighted that phishing and targeted malicious emails remained the most prevalent cyber security incident.

This data highlights an important disparity between expected versus actual incidents experienced. Respondents also underestimated the prevalence of accidental disclosure in 2019, with data breaches due to insider threats experienced more than twice as frequently than expected. This increased concern about data breaches is likely a symptom of the Privacy Amendment (Notifiable Data Breaches) Act 2017 (NDB scheme), which came into effect in 2018.

The evident shortcomings for organisations to understand the prevalence and likelihood of incidents raise questions about their cyber security priorities and readiness. Organisations tend to invest to combat the risk as they perceive it. If there is such a disparity between perception and the reality of the risk, organisations may not be investing in ways that will help them meet defined risk tolerance goals.

INCIDENTS EXPERIENCED IN 2018 VS INCIDENTS EXPECTED IN 2019



MISINTERPRETATION OF THE THREAT RISK LANDSCAPE

Since 2016, a key trend emerging from the survey data is the consistent misinterpretation or attribution of the cyber threat risk landscape. Such misinterpretation is likely the result of two key factors. Firstly, governance and risk reporting is not effective in communicating the cyber security risk, which means executive leaders do not have visibility of the organisation's information and cyber security risk, so it cannot make appropriate decisions to combat it. The benefit to be gained by opening up these lines of communication is great, as the survey data shows that organisations with better cyber risk reporting were 33% more accurate in predicting most likely incidents.

The second factor is that organisations find it difficult to assess their threat profile, and identify threat actors who would seek to compromise their information assets or determine how these adversaries are likely to do so. The tendency for organisations to consistently raise concerns for data breaches via the supply chain highlights this. Contrasting this lack of having a true understanding of supply chain risks.

PHISHING TAKES THE LEAD

This year, as with most of the years we have run this survey, phishing is the most commonly experienced cyber security incident. Phishing is prevalent because of its low complexity and high success rate to execute. Phishing is also often the gateway for other forms of attacks, as phishing emails can result in both Business Email Compromise (BEC) and the dissemination of malware into an organisation's systems. With the rising adoption of anti-virus/anti-malware solutions, malware is less successful, and threat actors are beginning to move towards BEC attacks. In June 2019, the Australian Competition and Consumer Commission (ACCC) reported an increase in BEC attacks by 42% compared to the prior year's losses.

PAYMENT REDIRECTION FRAUD

Financial gain has proven a prominent driver for threat actors conducting a cyber attack, so it is not surprising many use BEC attacks to redirect legitimate payments into accounts they control. These subsequent attacks are known as Payment Redirection Fraud. Due to the increasing commonality of this attack, we surveyed BEC and Payment Redirection Fraud data for the first time in 2019. Our analysis of this new data shows that despite being a new category for the survey, these types of attacks were the top fourth and fifth incident types reported.

BEC attacks with a financial motive typically target employees working in roles with financial responsibilities and executives with large financial approval authorities. The apparent targeting of these attacks suggests threat actors are actively using social engineering techniques and Open Source Intelligence (OSINT) methodologies to harvest public information to guide attacks where financial theft is the objective. This information is then used by criminals to craft emails to trick employees to authorise payments of finalised invoices.

RANSOMWARE DECREASING, BUT VARIANTS EMERGING

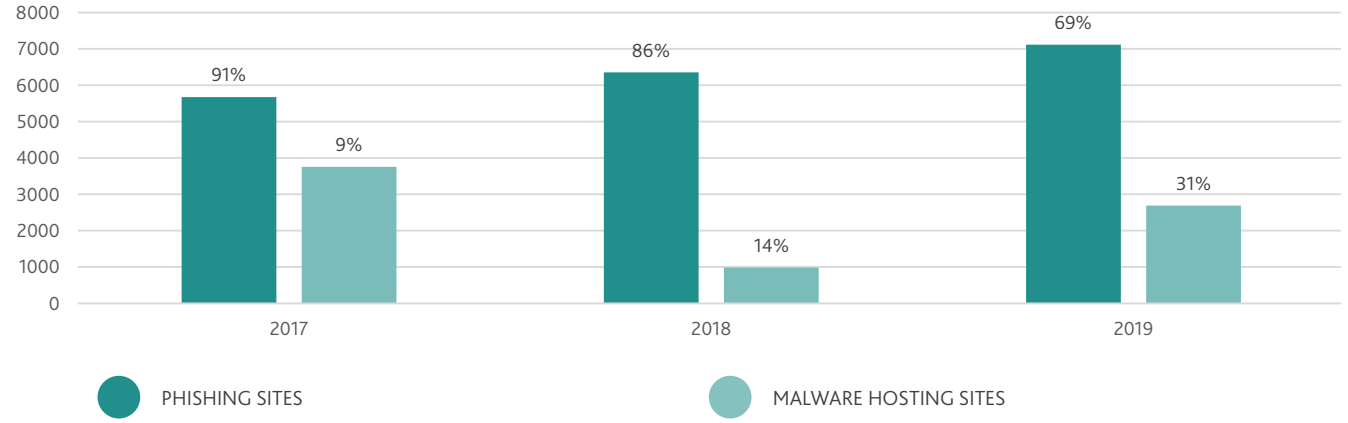
Ransomware was at its peak in 2017 and Australian and New Zealand organisations were some of the hardest hit by ransomware infections. A single strain of ransomware, known as WannaCry, resulted in significant public awareness with healthcare organisations infected and critical systems damaged in more than 150 countries. In subsequent years, the number of reported ransomware incidents has declined, as organisations have improved their defences against the known threat. Our 2019 data demonstrates a continuation of this trend with the number of ransomware attacks dropping by 37% compared to the previous year. This decrease in incidents does not mean ransomware no longer poses a threat, instead it highlights that new variants of ransomware are being developed. It only takes a quick scan of the media reporting on cyber security incidents to know ransomware attacks are still a serious concern. In fact, ransomware attacks are becoming more sophisticated themselves, with the introduction of cryptographic techniques to evade detection from anti-virus software and variants that take a copy of the data before it locks organisations out. Respondents seem cognisant of this threat, expecting ransomware attacks to rise by 11% in 2020. Given our observations of what is happening across Australia and New Zealand's threat landscape, we agree with this expectation.

PHISHING AND MALWARE

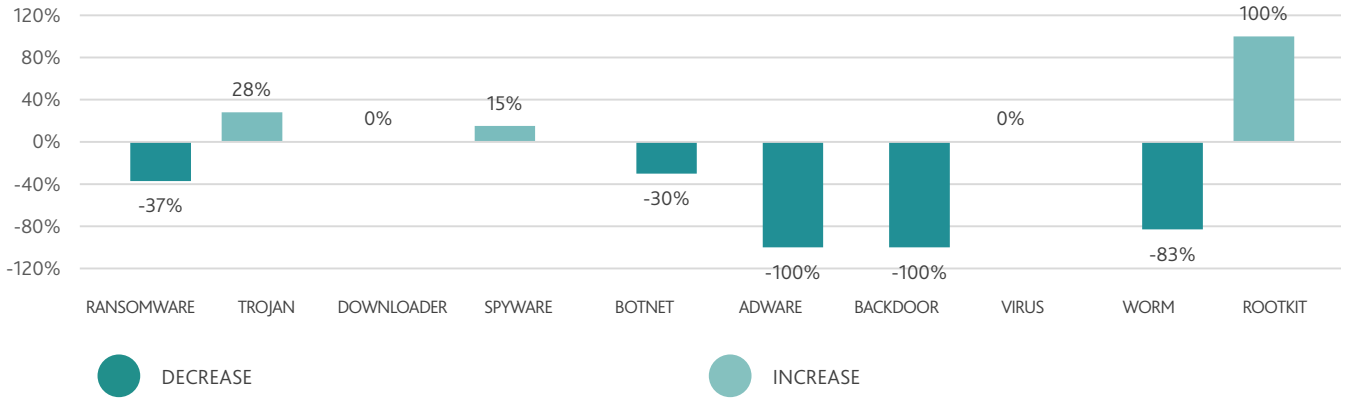
In alignment with this year's survey results, AusCERT technical incident analysis statistics are demonstrating that phishing attacks are on the rise. Over the last 3 years, AusCERT has taken down 19,151 malicious phishing sites and 7,434 malware hosting sites. This number is only expected to rise in the coming year.

Additionally, AusCERT's members are continuing to report a wide array of incidents, often revealing changes in trends. In 2019, AusCERT saw an increase in Trojan, Spyware and Rootkit samples (28%, 15% and 100% respectively) compared to 2018. This suggests that attackers continue to develop new threat tactics and techniques to exploit organisation's computer systems. There is also some good news. Similar to the data recorded in this survey, AusCERT members reported a decline of 37% in Ransomware since 2018. This decrease suggests that organisations have improved their defences and are following improved redundancy practices, which may have helped drive a decline in the prevalence of ransomware attacks. 2019 also saw declines in Botnet, Adware, Backdoor and Worm attacks which suggests that organisations are getting better at applying security patches to their environments. The increased uptake of security controls is further examined in the shift in security control investments section of this report.

PHISHING SITE TAKEDOWNS VS MALWARE SITE TAKEDOWNS



2018 - 2019 (% CHANGE)



CASE STUDY: AIRLINE'S CUSTOMER DATA BREACHED

In July 2019, a threat actor compromised two employees of an Asia Pacific based airline via a phishing attack. The threat actor gained access to internal documents relating to the airline's loyalty scheme and the data of 70,000 customers. The information included customers' names and email and mailing addresses. A small number of customers also have had passport details exposed. While the threat actor did not steal highly personal or sensitive information in this particular attack (excluding possible identity documents), the data could be used for future targeted attacks or as part of broader cyber criminal activities.

Even though the country in which the airline was headquartered at the time of the attack did not have a mandatory data breach notification scheme, the airline still chose to make a privacy breach notification to the Privacy Commissioner's office. The airline also made contact with all affected customers and advised those affected to be aware of the possibility of an increase in spam, phishing and other social engineering attempts.

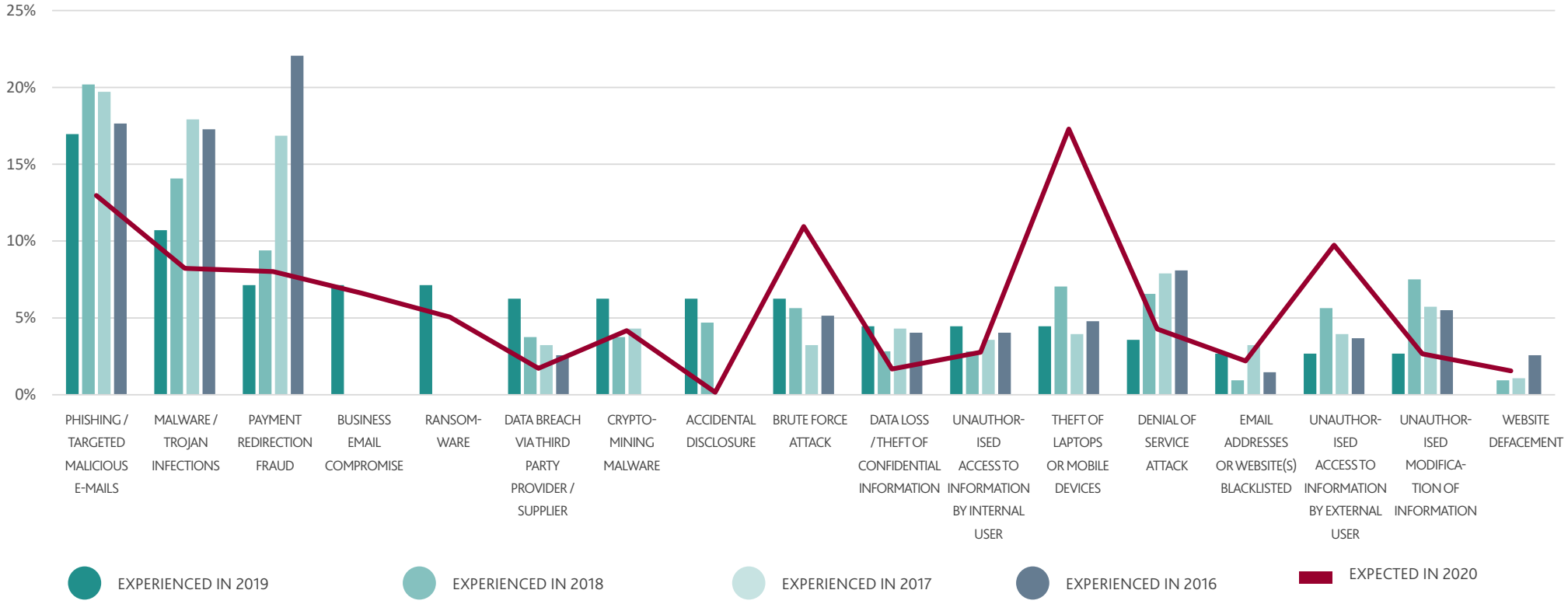
CASE STUDY: WHEN AN OFFER TO DO BUSINESS ISN'T WHAT IT SEEMS

In January 2019, an international engineering group disclosed that it was the victim of a highly targeted cyber attack – one of the largest successful BEC incidents in history. Impersonating the CEO, cyber criminals sent a number of emails to the head of another information technology organisation, all under the guise of discussing a secret business venture in a foreign country.

The cyber criminals went beyond just using emails, facilitating conference calls and impersonating various legitimate stakeholders, including lawyers and senior executives. The cyber criminals successfully convinced the international technology organisation to transfer $18.6 million USD into offshore accounts. Most of the money was then transferred out of the accounts almost instantly.

SINCE 2016 RESPONDENTS HAVE BEEN CONSISTENTLY MISINTERPRETING THEIR THREAT RISK LANDSCAPE.

CYBER SECURITY INCIDENTS: 2016 - 2019

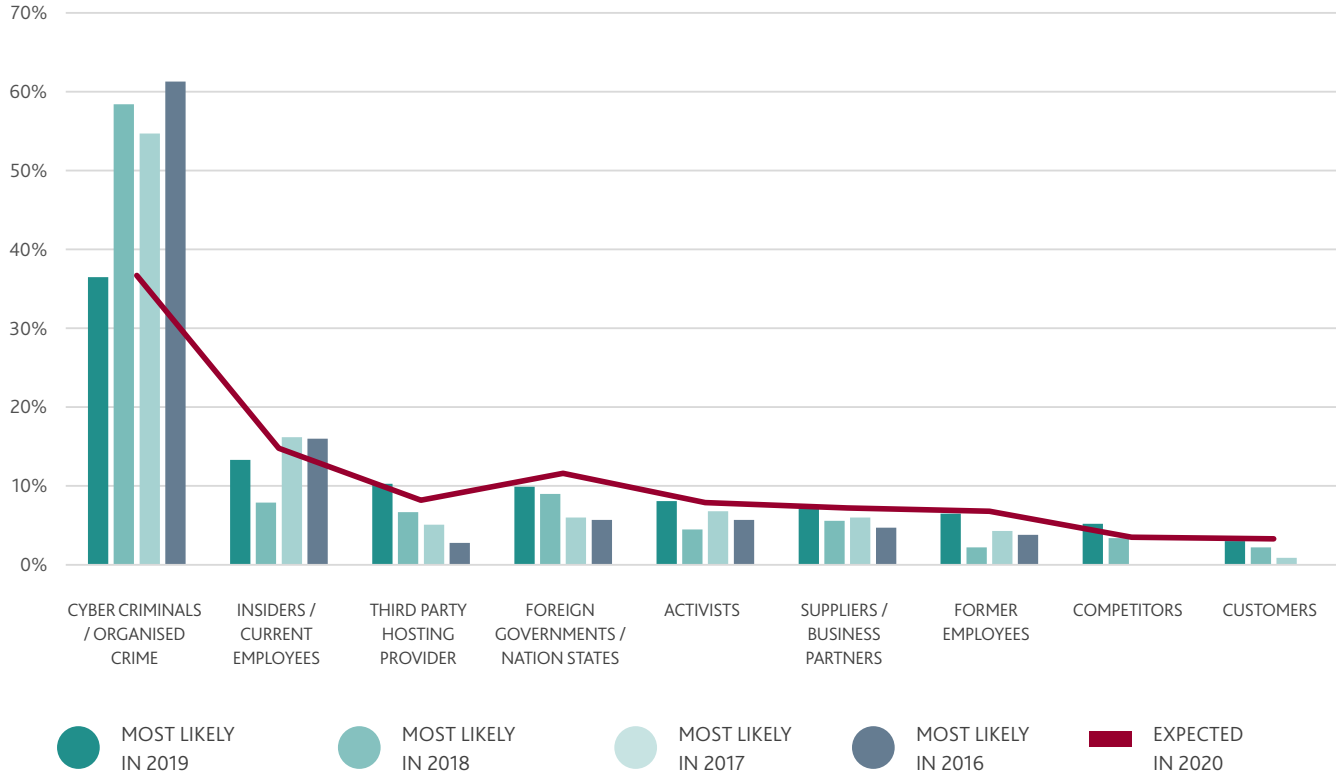


THE INCREASING INSIDER THREAT

In 2019, respondents became increasingly aware of the current employee insider threat, slightly shifting their concern away from external cyber criminals alone. When asked what the most likely source of incidents they had experienced was, respondents increasingly identified different types of insiders. The increase in attribution to sources that can be grouped as the "insider threat" is likely due to organisations better understanding incidents following NDB preparation activities. These sources include:

- Current employees
- Suppliers
- Former employees
- Customers.

MOST LIKELY SOURCE OF INCIDENTS - 2016 TO 2020



CYBER CRIMINALS HERE TO STAY, BUT INSIDERS ON THE RISE

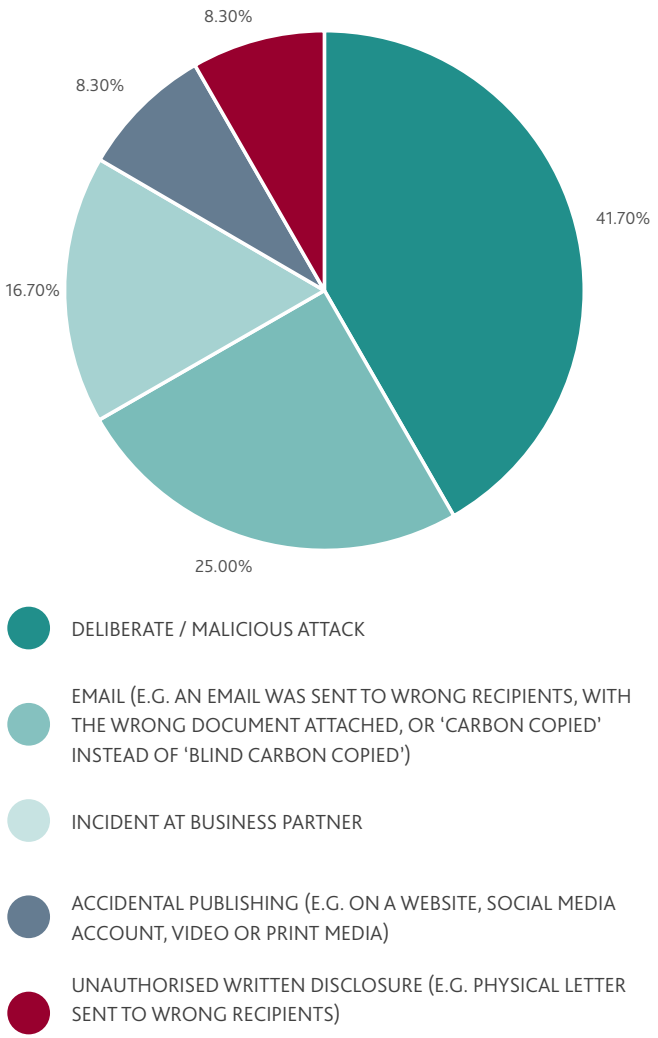
In 2019, cyber criminals (those operating outside the organisation) were 50% more active than expected. Such heightened activity demonstrates why cyber criminals remain a concern, but what is of importance to note is that insiders/current employees were considered the second-largest sources of incidents in 2019.

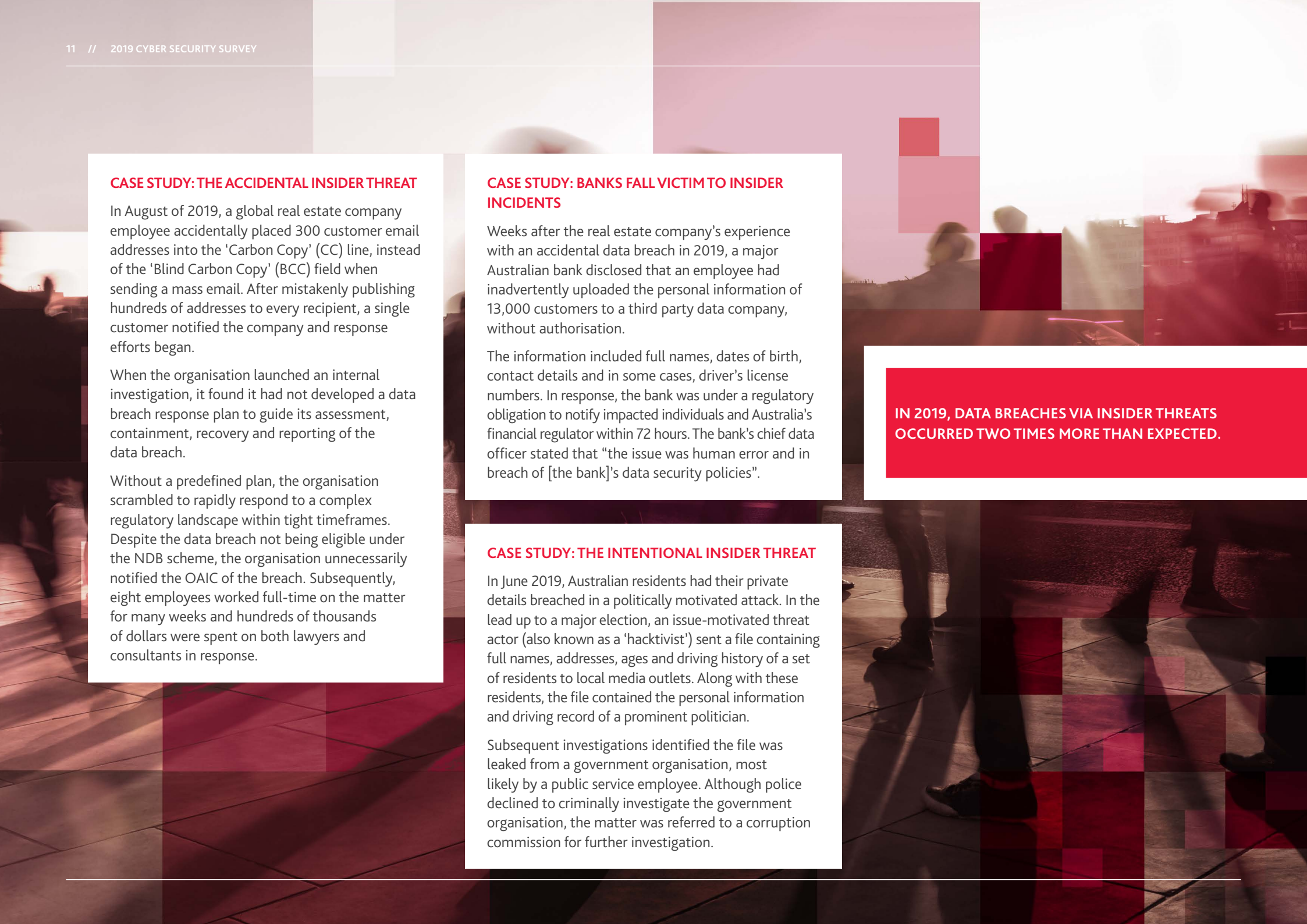
Respondents indicated there is likely to be more than a 10% year-on-year rise in insider incidents over the coming year. When the insider threat is grouped to include current and former employees, suppliers and customers, 40.2% of incidents can be attributed to this source. This exceeds the 36.5% of attribution afforded to cyber criminals. The rise of insider threats may be a symptom of organisations becoming increasingly aware of cyber security incidents as they occur and having the opportunity to investigate and define attribution. Regardless, it's imperative organisations don't underestimate this internal source.

HOW INSIDER THREATS ARE CAUSING DATA BREACHES

Though there has been a rise in the incidents involving insiders, we should not take this to imply an insider threat is necessarily malicious. It would not be unreasonable to anticipate that human error would account for a considerable number of these incidents. The Office of the Australian Information Commissioner (OAIC) Notifiable Data Breach Scheme – 12 month Insights Report 2019 suggests that 35% of breaches are attributable to human error. This data mirrors our 2019 findings, which show that 41.7% of breaches were attributable to accidental emails or inadvertent online publishing. This highlights that organisations must look to their cyber security training and awareness programs. Accidents happen, but when organisations are running a comprehensive program, it may be a sign of the failure of the program itself.

CAUSES OF DATA BREACHES - 2019





CASE STUDY: THE ACCIDENTAL INSIDER THREAT

In August of 2019, a global real estate company employee accidentally placed 300 customer email addresses into the 'Carbon Copy' (CC) line, instead of the 'Blind Carbon Copy' (BCC) field when sending a mass email. After mistakenly publishing hundreds of addresses to every recipient, a single customer notified the company and response efforts began.

When the organisation launched an internal investigation, it found it had not developed a data breach response plan to guide its assessment, containment, recovery and reporting of the data breach.

Without a predefined plan, the organisation scrambled to rapidly respond to a complex regulatory landscape within tight timeframes. Despite the data breach not being eligible under the NDB scheme, the organisation unnecessarily notified the OAIC of the breach. Subsequently, eight employees worked full-time on the matter for many weeks and hundreds of thousands of dollars were spent on both lawyers and consultants in response.

CASE STUDY: BANKS FALL VICTIM TO INSIDER INCIDENTS

Weeks after the real estate company's experience with an accidental data breach in 2019, a major Australian bank disclosed that an employee had inadvertently uploaded the personal information of 13,000 customers to a third party data company, without authorisation.

The information included full names, dates of birth, contact details and in some cases, driver's license numbers. In response, the bank was under a regulatory obligation to notify impacted individuals and Australia's financial regulator within 72 hours. The bank's chief data officer stated that "the issue was human error and in breach of [the bank]'s data security policies".

CASE STUDY: THE INTENTIONAL INSIDER THREAT

In June 2019, Australian residents had their private details breached in a politically motivated attack. In the lead up to a major election, an issue-motivated threat actor (also known as a 'hacktivist') sent a file containing full names, addresses, ages and driving history of a set of residents to local media outlets. Along with these residents, the file contained the personal information and driving record of a prominent politician.

Subsequent investigations identified the file was leaked from a government organisation, most likely by a public service employee. Although police declined to criminally investigate the government organisation, the matter was referred to a corruption commission for further investigation.

IN 2019, DATA BREACHES VIA INSIDER THREATS OCCURRED TWO TIMES MORE THAN EXPECTED.

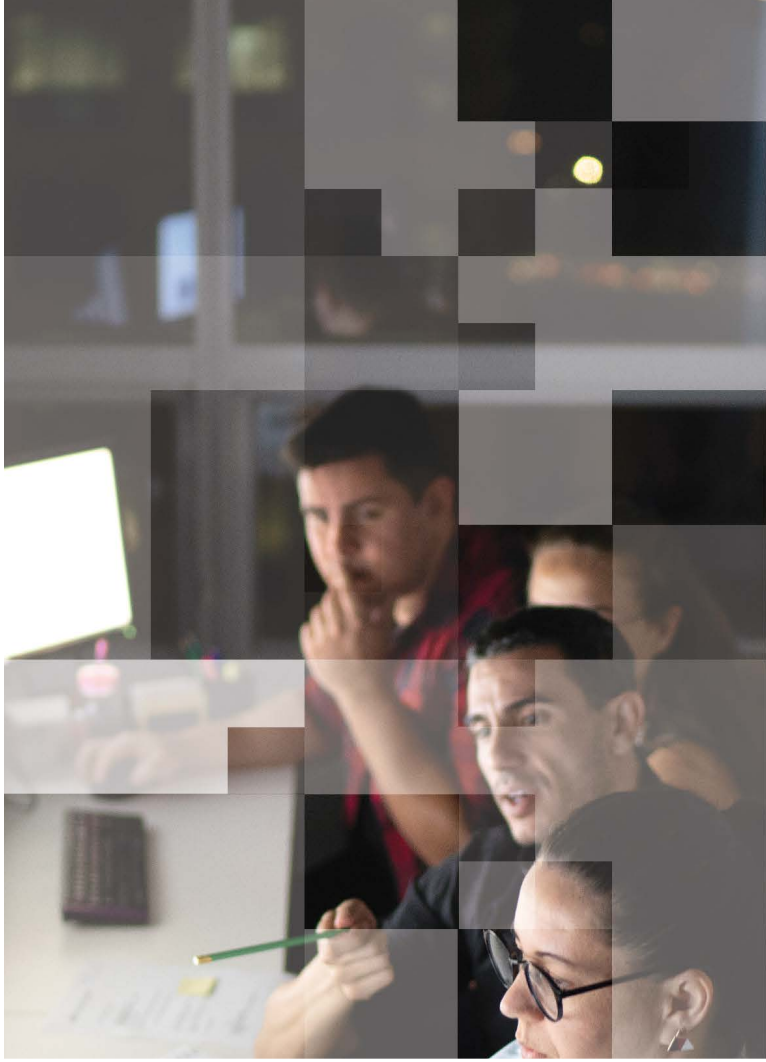
SHIFT IN SECURITY CONTROL INVESTMENTS

Cyber security risk does not discriminate against industry, region or size. It will exist wherever technology resides but can manifest itself in different ways. Some adversaries prefer highly sophisticated targeted attacks, where others prefer to focus on the lowest hanging fruit. Overt attacks, like ransomware, are highly disruptive, whereas others are more silent and insidious.

Just as we see differences in the ways cyber risk presents itself, we see different options to reduce its likelihood and impact. For decision-makers, this typically means investing in either technology-driven security solutions (such as software tools) or governance and process related based efforts to reduce specific risks. There is no single 'silver-bullet' approach or toolset to mitigate cyber risk, and control investments need to prevent, detect and respond to incidents the organisation is most likely to face. When organisations ignore or misinterpret the threat landscape, they tend to adopt security controls that may not be effective in mitigating their cyber risks, which makes demonstrating a return on security investment a challenging exercise. Therefore, it is essential these investment decisions are informed by the organisation's threat profile.

During 2019 there was a shift away from technology security controls and an increase in the adoption of security governance and supporting processes. Historically, respondents have underestimated the threat landscape and relied on a limited visibility of threats to make security investment decisions. Historically, respondents reported lower levels of maturity in understanding their specific threat profile. This may have resulted in making security investment decisions that may not be addressing their specific risks.

2019 started to see that organisations started taking threat-based cyber security approaches to direct their investment decisions. This trend shows that mature respondents are focussing less on 'silver-bullet' technology and more on establishing enterprise-wide processes to be better prepared for cyber incidents.



IT WAS TWICE AS COMMON FOR A RESPONDENTS IN 2019 TO HAVE A CISO ROLE IN PLACE, COMPARED TO 2016.

CYBER RESILIENCE CONTROLS - 2016 TO 2019

MANAGING THE 'NOT IF BUT WHEN' FACTOR

There's a common saying in the cyber security industry: "it's only a matter of time until your organisation will experience a cyber attack". Decision-makers are starting to be more proactive; taking stock of the cyber threats in their industries and reflecting when their industry peers or competitors face disruptive cyber attacks. As board directors and C-suites ask themselves how to manage the 'not if, but when' factor, a core tenet of cyber security risk management provides the answer: build resilience.

CYBER RESILIENCE THE KEY TO BEING PREPARED

In the cyber domain, resilience is the capability to reduce the impacts of cyber incidents when they occur (rather than focussing on likelihood alone). This involves accepting the high likelihood, or even certainty, of cyber incidents occurring in the future that will negatively impact your organisation. Efforts to establish resilience are most successful when there is clear visibility of the threat landscape. This means the organisation understands its crown jewels, which adversaries seek to compromise them, and what their methods involve. As organisations accept specific incidents will occur and subsequently tailor their plans to recover from them, we see a shift in controls. The 2019 survey results show this shift as a reduced focus on technical controls and heightened efforts in enterprise-wide processes, procedures and governance. In 2019, respondents reported a 16% increase in the adoption of Business Continuity Plans (BCPs) and a 17% increase in security awareness programs. Investment in recovery processes and empowering staff to respond to cyber incidents indicates recognition of the importance of entrenched organisational resilience and defence for specific, relevant threats and risks.

PROCESS AND PEOPLE

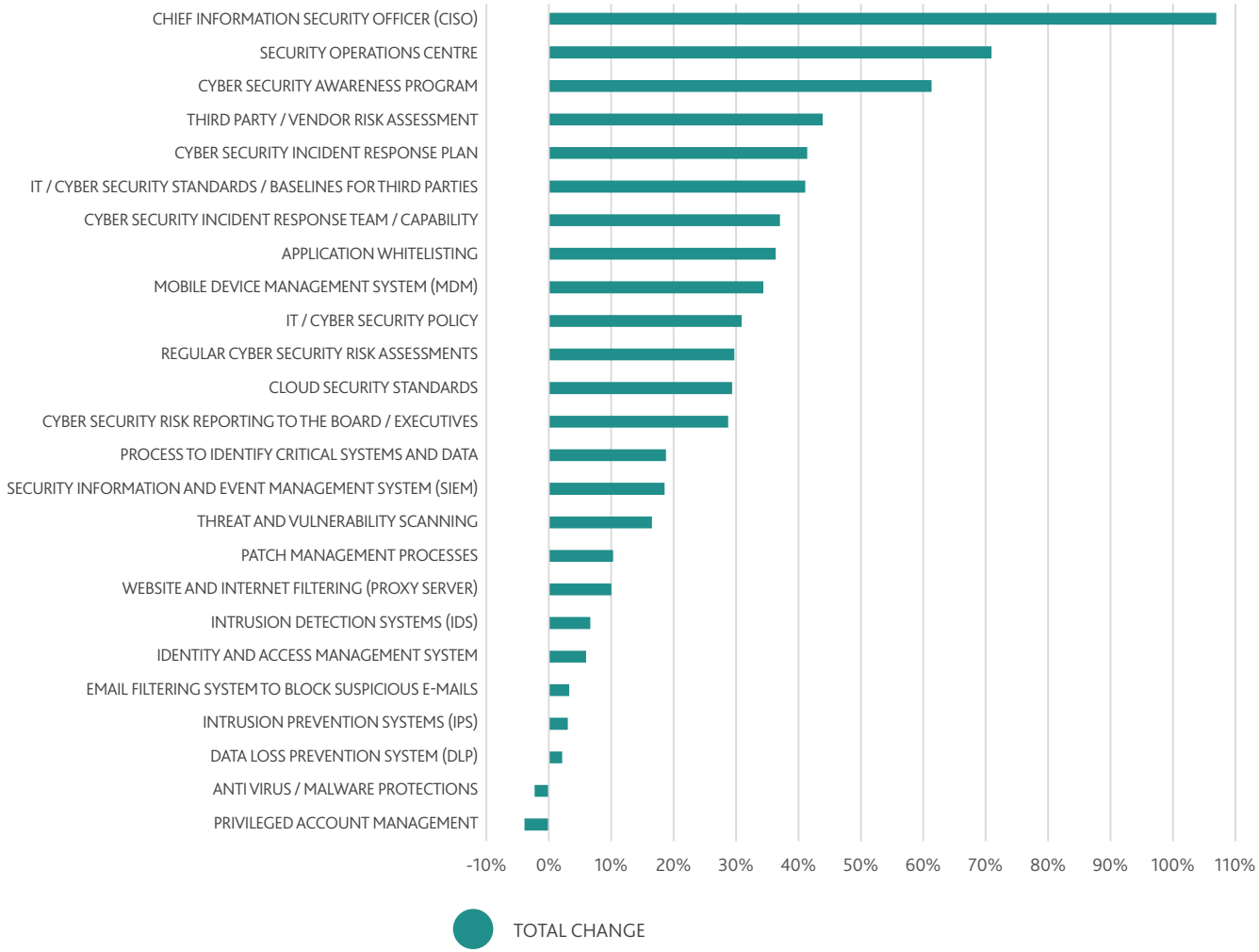
As resilience shines a light upon the cyber threat landscape, organisations realise the importance of clearly communicating and representing relevant risks to decision-makers. Our survey data supports this, showing that the number of respondents with CISOs increased by 46% in 2019 compared to 2018. Looking further back, the data shows the adoption of CISO roles has more than doubled since 2016. The uptick in governance controls in 2019 also saw a 31% increase in cyber insurance, as businesses sought to avoid the financial damage inflicted by disruptive cyber security incidents.

TOP FIVE CONTROLS

As 2019 shows a shift towards the adoption of governance practices, longer-term data provides insights into the top five most frequently adopted controls are:

- **CISOs** – Dedicated senior executive responsible for cyber security who are committed to setting and ensuring the effectiveness of the organisation's approach to defending its information assets against cyber threats
- **Security Operations Centres** (SOCs) – Decentralised hubs of unique cyber security operations capabilities focussed on detecting, containing, eradicating and recovering from cyber security incidents
- **Cyber security awareness programs** – Initiatives to uplift the awareness of employees to detect and defend against cyber attacks by engaging them to learn about relevant attacker tactics, techniques and risks
- **Third party/vendor risk assessments** – the effectiveness of security controls at assessments of third party vendors
- **Cyber security incident response plans** – Procedures to mobilise the entire organisation in managing incident detection, containment, eradication and recovery.

RATES OF CONTROL ADOPTION - 2016 TO 2019



INCREASED ADOPTION OF GOVERNANCE CONTROLS

Examining the 2019 survey data shows that while most controls have increased in their rate of adoption over time, the slowest growing are technology solutions. This reiterates the focus businesses place on establishing enterprise-wide processes to manage the impacts of cyber risks. Interestingly, the adoption of both privileged account management and anti-virus/anti-malware protections has decreased over time. These two controls, and particularly anti-virus/anti-malware protections, are considered fundamental 'must-haves' in the management of cyber risk. As their adoption rates fall, we can expect the frequency of malware and unauthorised access to rise.

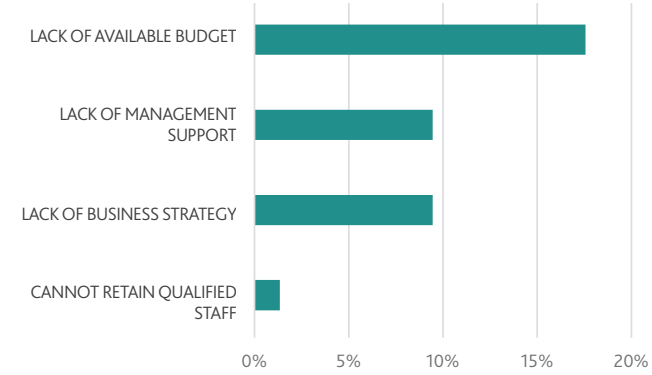
EXECUTIVE OVERSIGHT

Organisations with more senior stakeholders involved in cyber security adopt a more holistic approach to effectively managing cyber risk – and it's paying off. Survey respondents who adopted the top five most rapidly growing controls experienced 31% fewer incidents than their peers.

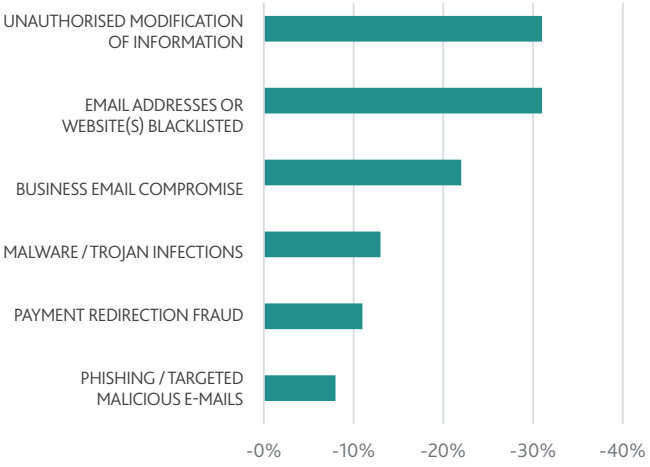
RISK VISIBILITY ALIGNS CYBER WITH ORGANISATIONAL OBJECTIVES

Organisations that adopt the top five controls will have established the capability to clearly identify, communicate and endorse the importance of cyber risk. This capability to assign ownership, champion, and manage cyber risk in an accountable way, has demonstrable benefits. Respondents who adopted the top five controls were more than three times more likely to have completely aligned their cyber capabilities with organisational objectives.

CYBER SECURITY CHALLENGES FACED WITHOUT TOP 5 CONTROLS



DECREASE IN INCIDENTS EXPERIENCED WHEN GOVERNANCE CONTROLS ARE IMPLEMENTED



RESPONDENTS THAT ADOPTED THE TOP FIVE MOST RAPIDLY GROWING CONTROLS WERE THREE TIMES MORE LIKELY TO HAVE COMPLETELY ALIGNED THEIR CYBER CAPABILITIES WITH ORGANISATIONAL OBJECTIVES.

INSTILLING CONFIDENCE TO MANAGE CYBER RISK

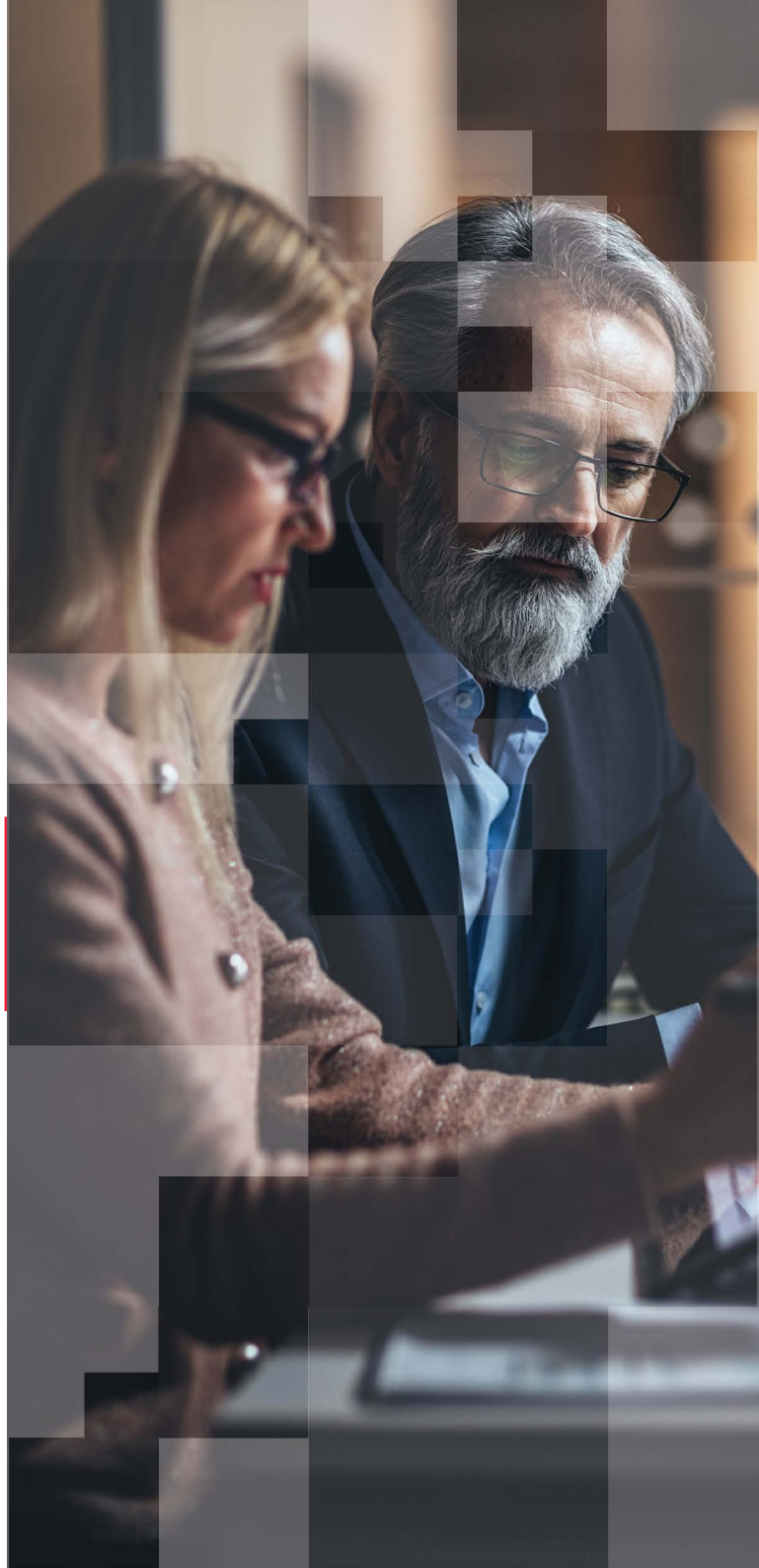
Organisations that effectively manage cyber risks can identify, assess, track and control them in a measured way. With this in mind, it is not surprising respondents who had adopted the top five controls were more than 50% more confident in responding to and recovering from cyber incidents.

REDUCING RISK MANAGEMENT CHALLENGES

Organisations face different challenges in managing cyber risk. These include balancing too many priorities, resource restraints, limited budgets and lack of management support. But one thing becomes clear when organisations build effective north/south pathways to communicate and manage risk within their organisations: they face fewer challenges than their peers. Respondents who adopted the top five controls faced no challenges related to acquiring talent, budget, management support or alignment to organisational strategy.

THREAT-BASED CYBER RISK MANAGEMENT

Businesses that have implemented focussed efforts on supporting security operations with well-structured governance controls have enabled their cyber security capabilities to act as headlights in the threat risk landscape. By directing efforts to understand relevant threats and risks, organisations that have adopted the top five controls are significantly more accurate in their predictions of which incidents will impact them. This results in smarter security investments with greater returns, reduced incident frequency and heightened confidence in cyber risk management capability. Increased confidence in the ability to interpret and respond to cyber risks, empowers decision-makers to safely take greater risks when determining how to exploit market opportunities. It is in this way that a threat-based approach to managing cyber risk can enable organisations to, for example, rapidly expand into regions with stringent data privacy regulations, without taking unacceptable risks.



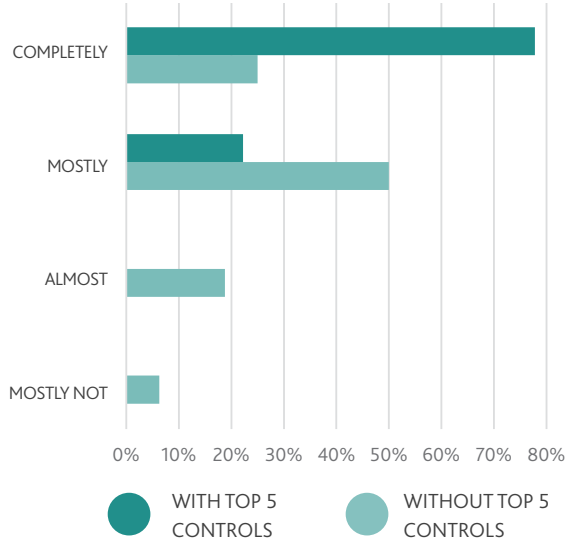
CONFIDENCE IN MEETING REGULATORY REQUIREMENTS

The Notifiable Data Breaches scheme came into force in Australia on 22 February 2018. It brought with it stringent requirements and timeframes for identifying and reporting data breaches of a particularly harmful nature, coupled with financial penalties for Australian organisations who fail to comply. Understanding the details of the NDB scheme's scope, whether a organisation does or does not need to comply, and what constitutes a notifiable data breach are complex topics. The next steps of determining how to respond to and notify impacted individuals of a data breach (including the Australian Government), is made more challenging by the very nature of the pressures and risks of an ongoing data breach incident.

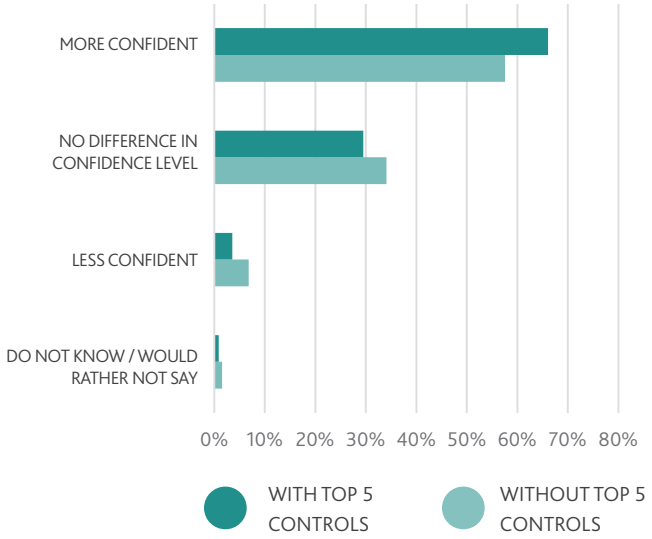
In 2020 it is expected that New Zealand will follow Australia and the United Kingdom in introducing mandatory data breach notifications. This update to the Privacy Act 1993 is expected late in 2020, and can be expected to follow a similar track as the legislation change in Australia.

Navigating the complex regulatory landscape requires a clear and continual model to appraise legislative change, identify gaps in compliance, and implement effective capabilities to meet new obligations. Respondents who have adopted the top five controls are more than twice as likely to be completely confident in complying with the NDB scheme.

CONFIDENCE TO COMPLY WITH NDB SCHEME



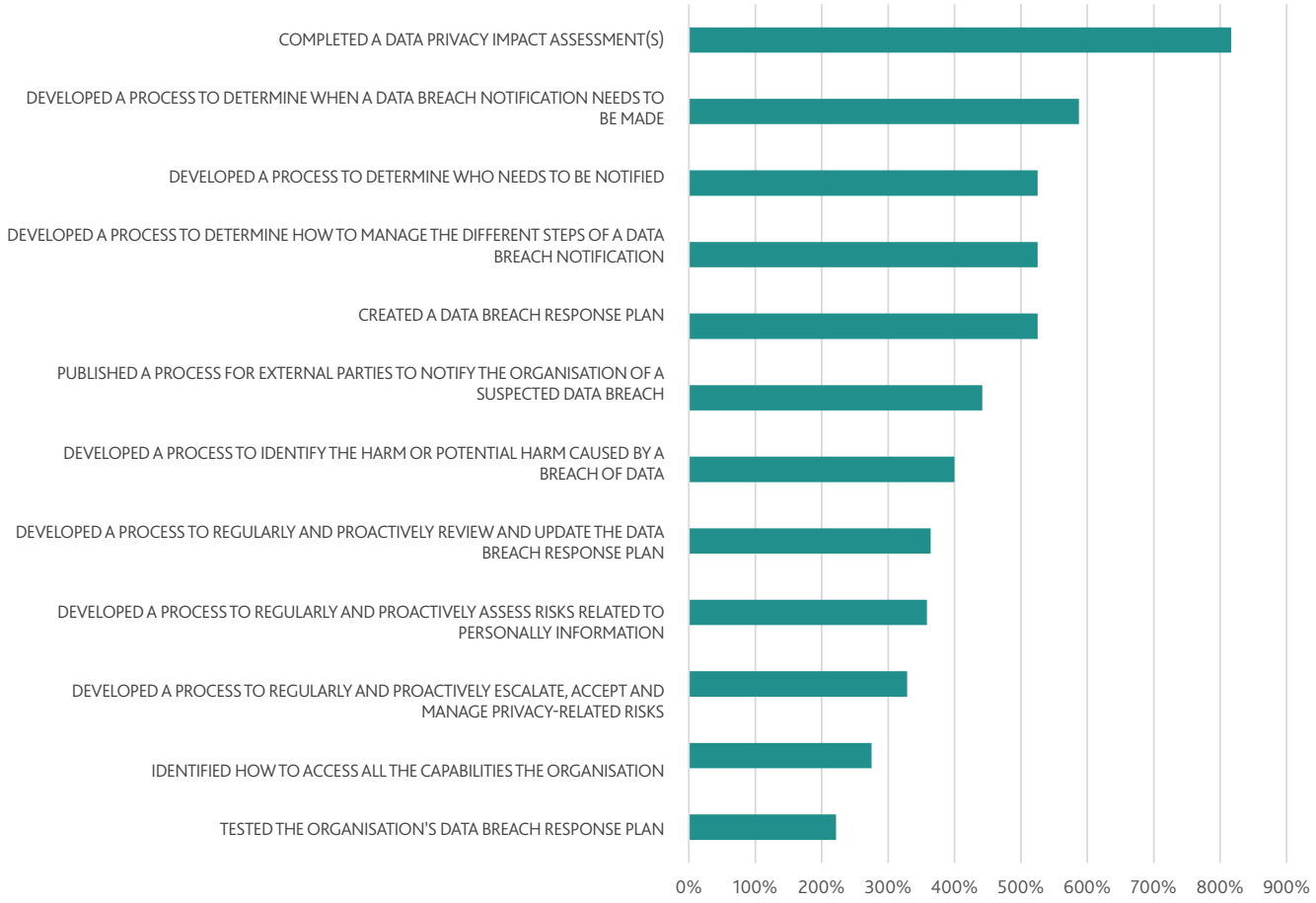
CONFIDENCE TO RESPOND AND RECOVER FROM AN INCIDENT COMPARED TO LAST YEAR



CAPABILITY TO COMPLY WITH THE NDB SCHEME

Many organisations have historically reported over-confidence in meeting NDB scheme requirements. Where respondents had been mostly or completely confident in their ability to comply, their implementation of pre-requisite controls and capabilities was lacking. This could be due to an inefficient regulatory risk management function that fails to accurately communicate the scope, impact or requirements of new regulations. Organisations effectively managing cyber risk have well-rehearsed pathways to identify and continually manage this type of risk. It is therefore fitting that respondents who had implemented the top five controls were, on average, more than four times more likely to have adequately prepared for meeting NDB obligations. An interesting commonality of true resilience between mature respondents who have adopted the top five controls is that they are eight times more likely to have tested their data breach response plans.

INCREASE IN NDB READINESS WHERE TOP 5 CONTROLS ARE ADOPTED



DATA BREACHES

Data breaches remain one of the more common 'nightmare scenarios' for decision-makers globally. As media saturation reinforces their often dire impact, it is now more clear that data breaches can push the bottom-line down at best, and at worst, bankrupt organisations or inflict real harm on people's lives.

DATA BREACHES REMAIN PROFITABLE FOR ADVERSARIES

In 2019, respondents reported a 35% year-on-year increase in the number of NDB notifications made to the OAIC. Interestingly, the number of respondents who reported being unsure or unwilling to disclose whether an eligible data breach occurred rose by almost 60%.

CONFIDENCE IN MEETING NDB OBLIGATIONS DROPS

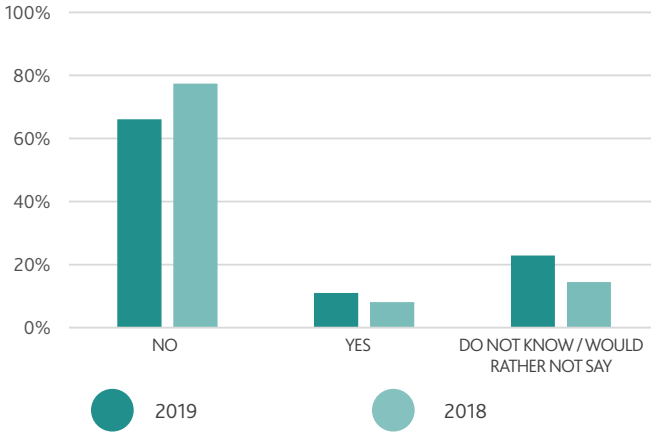
Earlier in this report, we highlighted that respondents who had adopted the top five most rapidly growing controls were more confident in meeting their NDB obligations. This is a positive trend to be expected as regulation ages and becomes more understood. However, across respondents generally, confidence in meeting NDB obligations has dropped. Most organisations now are less confident than last year and more are "absolutely not" confident in their capability to meet NDB obligations at all.

These statistics are likely to be indicative of a greater pool of respondents now understanding, as awareness of the NDB scheme grows, that they are required to comply and are unprepared to do so.

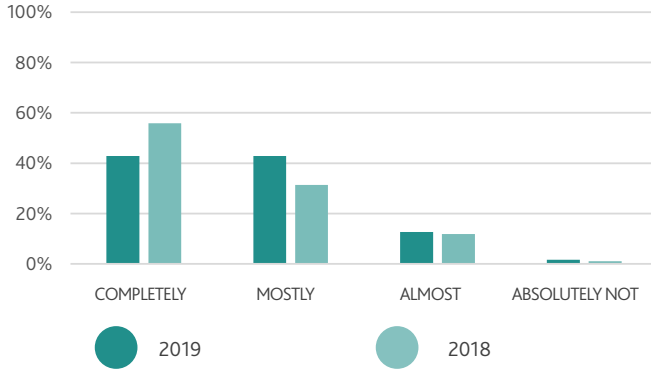
CAPABILITY TO MEET NDB OBLIGATIONS DROPS

Overall capability to meet the NDB scheme's obligations has dropped by an average of 26%. This means 26% fewer respondents are confident that they meet NDB capabilities than last year. Perhaps this is due to a larger pool of organisations only now understanding the extent of their compliance requirements, while also being completely unprepared to meet them.

HAS YOUR ORGANISATION MADE A BREACH NOTIFICATION UNDER THE NDB SCHEME



HOW CONFIDENT RESPONDENTS ARE IN MEETING NDB OBLIGATIONS - 2018 VS 2019



2019 - ADOPTION OF CAPABILITIES REQUIRED TO COMPLY WITH THE NDB SCHEME

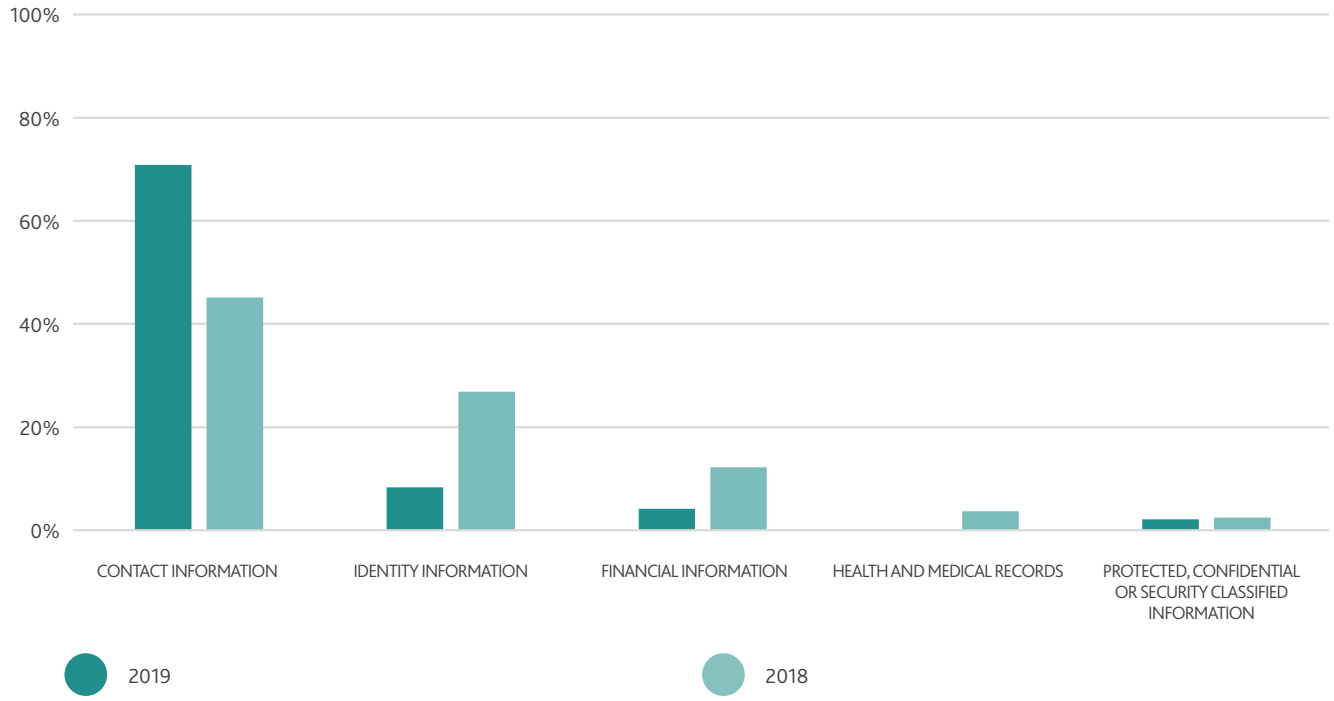
HACKERS TARGETING CONTACT INFORMATION

Adversaries target different types of information assets depending on their motivations, capability and intent. In 2019, respondents reported a 56% increase in the number of data breaches involving contact information compared to 2018. As hackers continue to harvest contact information, we can expect an increase in the volume of phishing/spear-phishing attacks over the next year.

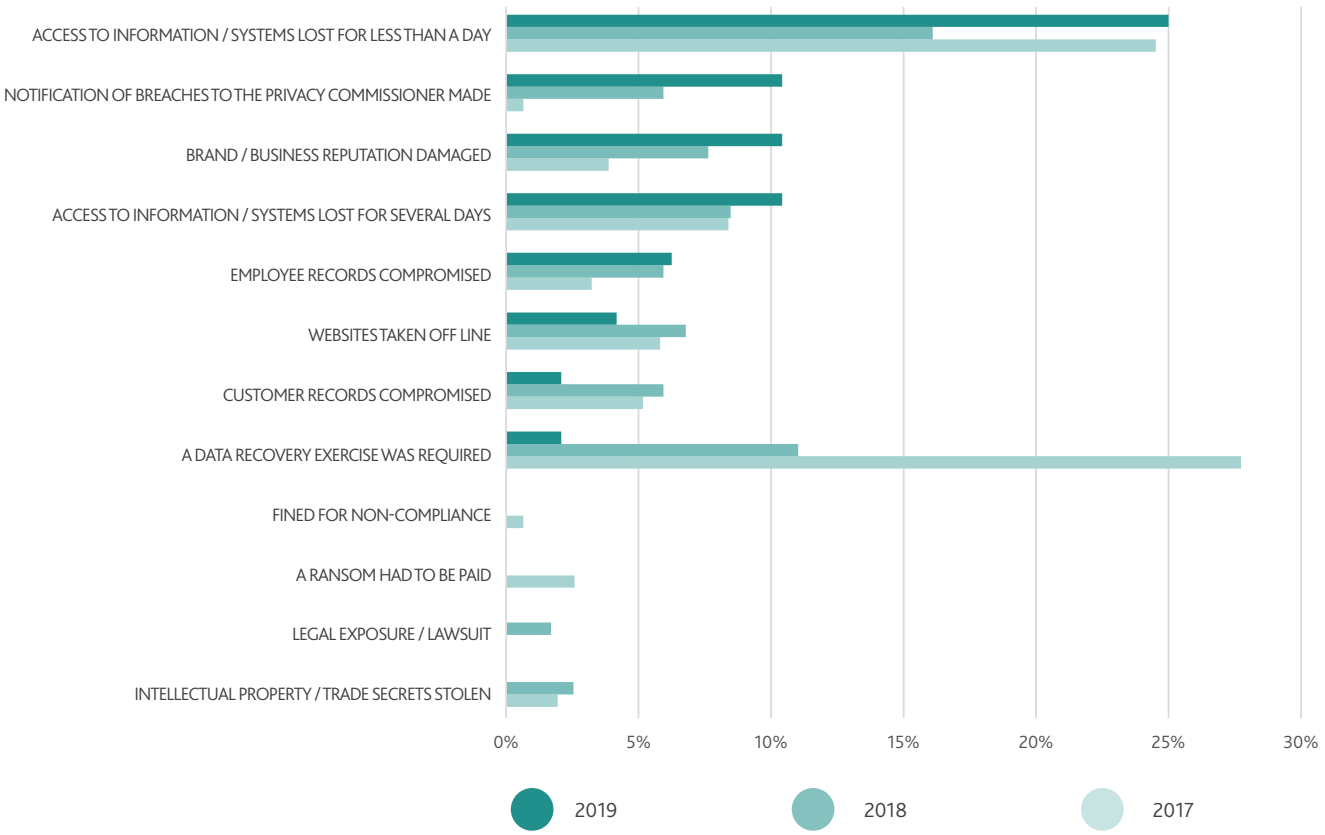
GREATER REPUTATIONAL HARM

As awareness of data breach regulations increase, so does public concern for the safety of private information. When consumers increase the importance of data security in their purchasing decisions, organisations are more heavily "punished" in the media for poorly managing the information they hold. Accordingly, it is not surprising that 2019 saw an increase in the extent of reputational damage caused by data breaches.

TYPES OF INFORMATION BREACHED - 2018 VS 2019



DATA BREACH IMPACTS



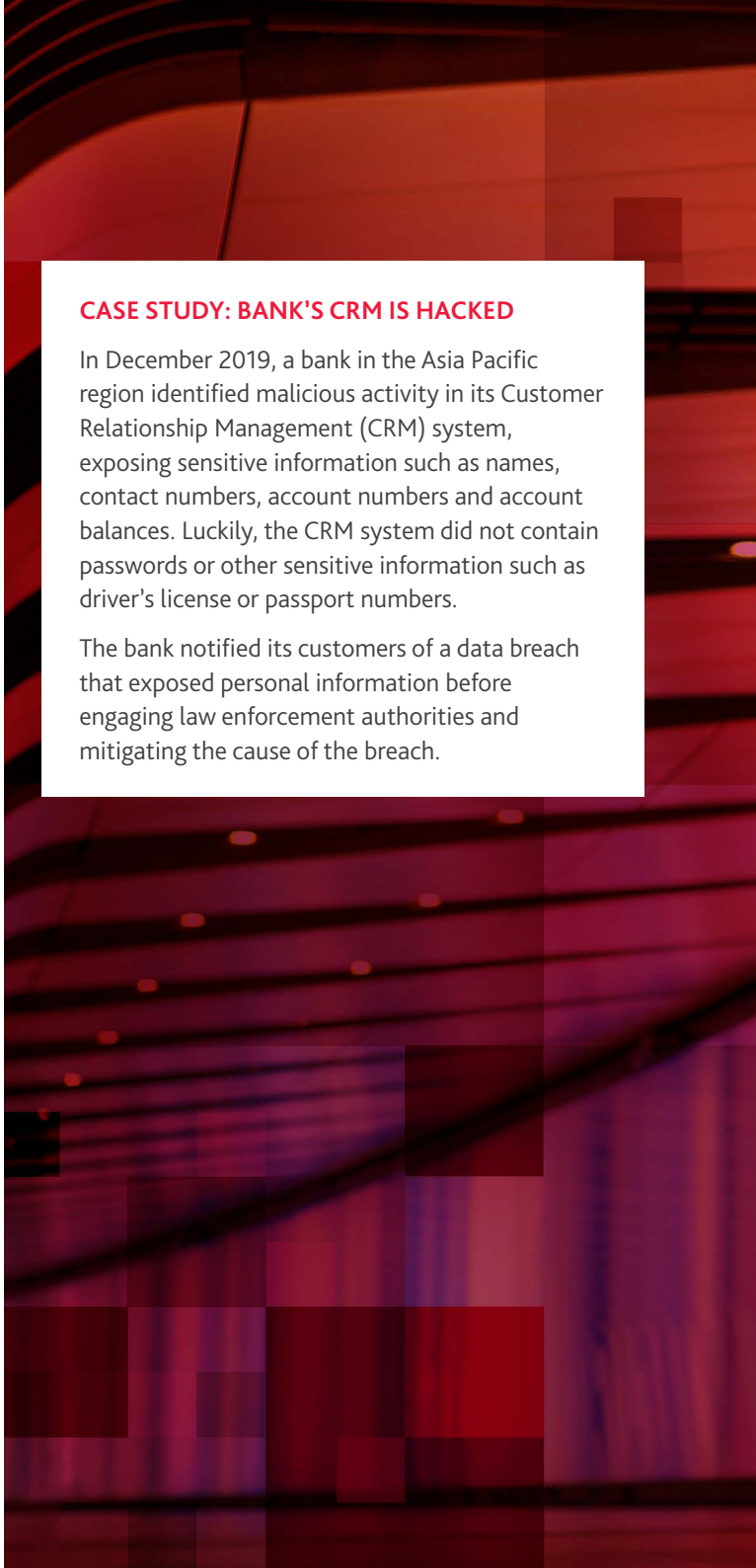
DATA BREACHES ACROSS THE NATION

The OAIC received a total of 964 eligible data breach notifications under the NDB scheme between April 2018 and March 2019. Of these, 60% were caused by malicious or criminal attacks. The OAIC reports that 153 eligible data breach incidents were caused by phishing/spear-phishing attacks specifically. Interestingly, our survey finds a probable correlation between the drop in ransomware and the drop in data recovery exercises as a result of data breaches.

DIFFERENT INDUSTRIES, DIFFERENT BREACHES

According to the OAIC, fewer than 1,000 individuals were affected by eligible data breaches between April 2018 and June 2019, with 86% of these breaches containing contact information at a minimum.

Human errors (such as employees emailing personal information to the wrong person) caused 53% of eligible data breaches in the health sector and 41% in the financial sector. These sectors were among the highest breached in Australia.



CASE STUDY: BANK'S CRM IS HACKED

In December 2019, a bank in the Asia Pacific region identified malicious activity in its Customer Relationship Management (CRM) system, exposing sensitive information such as names, contact numbers, account numbers and account balances. Luckily, the CRM system did not contain passwords or other sensitive information such as driver's license or passport numbers.

The bank notified its customers of a data breach that exposed personal information before engaging law enforcement authorities and mitigating the cause of the breach.

DEFENDING BEYOND 2020

Businesses face a range of cyber security threats and risks that originate both internally and externally. These threats and risks change over time, along with technologies and adversary motivations. As cyber attacks continue to change in complexity and sophistication, their impact will spread across more organisations and people. For this reason, it is imperative that organisations take a threat based approach and work to truly understand the types of threats they face and the most effective ways to defend against them.

We identified a set of key trends in this year's survey. In doing so, we've found that respondents continue to underestimated the threat landscape – particularly phishing insider threats. These trends showed that:

- In 2019, data breaches via insider threats were more than twice as common as expected
- Respondents have consistently underestimated the prevalence of data breaches caused by insider threats
- Phishing, malware and Business Email Compromise (BEC)/Payment Redirection Fraud attacks were the most common in 2019.

We can see from this data that the threat-based approach to cyber security is a forward-looking, predictive approach that focuses investments to maximise return, by defending against the most likely threats in a tailored way. Rather than (or in addition to) focussing solely on protecting critical data assets or applying baseline cyber security programs, threat-based cyber security leverages the organisation's unique threat profile to focus investments towards the areas of greatest return.

As respondents have come to understand that cyber attacks are a certainty, they've moved away from 'silver-bullet' vendor technologies and towards wider governance controls to help them best understand their most likely threats and risks, and to focus investments accordingly. The top five security control investments are governance-focussed rather than technically-focussed, with the exception of Security Operations Centres (SOCs) – which addresses both. We've seen this shift when looking at the most rapidly adopted controls since 2016, which shows that:

- CISOs have been the most rapidly adopted control, and are now more than twice as common than in 2016
- Respondents that implemented controls to enable risk visibility were 33% more accurate in predicting the most likely incidents
- Businesses who have focussed security investments on a set of key governance controls faced no cyber risk management challenges related to budget, strategy or management support.

BRINGING THREAT-BASED SECURITY TO LIFE

The first step in achieving organisational resilience through threat-based security is to understand and assign accountability for your organisational DNA: the data assets and IP that make an organisation unique, or a potential target. This process begins with governance – identifying, categorising, managing and protecting critical information assets through its lifecycle. The next step is to factor in the threat landscape and understand the most likely incidents your organisation will face. What this survey's data tells us is that businesses need to be keenly aware of the risk of phishing and insider threats – both malicious and accidental.

Finally, as a mechanism to embed ongoing resilience, your organisation must identify the most effective and pragmatic controls to defend against your most likely risk and attack vectors, based on the organisation's threat profile.

In this years' survey, we found that respondents are using governance processes to increase risk visibility and reporting to executives. Using this leadership oversight, respondents have adopted a more holistic approach to effectively identifying and managing cyber security risk. The survey results show that this is an effective approach with important benefits. Respondents who adopted key governance controls:

- Faced more than 30% fewer incidents
- Were 50% more confident in responding to incidents
- Were three times more likely to have completely aligned their cyber capabilities with business objectives.

WINNING THE BATTLE

Determined hackers are rewarded for their efforts. Our responsibility as cyber security practitioners, risk decision-makers, and business leaders, is to ensure the hacker's cost is greater than their reward. We can only do this by staying knowledgeable and abreast of the tactics, tools and procedures of our adversaries. We achieve this by knowing what they target, how they attack, and by sharing this information to the right people at the right times. Through embedding resilience into the fabric of our organisations, we help protect our industries and nations against the bulk of the macro-economic impacts incurred by cyber attacks. Along with ensuring the growth of our own organisations, this shared goal is one worth investing in.

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.

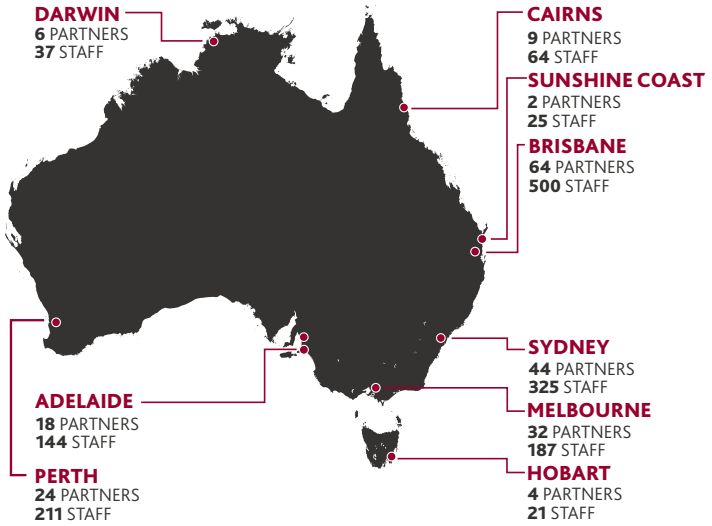
As a result of our client partnership approach, our cyber teams develop strong insight into their clients' business, enabling them to find innovative ways to help clients maximise their growth opportunities, improve processes and avoid pitfalls.

BDO has 1,900+ 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.

1,756 PEOPLE
10 OFFICES
203 PARTNERS
FIGURES TAKEN AS AT 01 JANUARY 2020



800+ PEOPLE
15 OFFICES
88 PARTNERS

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 is a Cyber Emergency Response Team (CERT) based in Australia.

It operates as a membership based organisation.

As a not-for-profit security group based at The University of Queensland, AusCERT delivers 24/7 service to members and helps them prevent, detect, respond and mitigate cyber-based attacks.

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

As an active member of the Forum for Incident Response and Security Teams (FIRST) and Asia Pacific Computer Emergency Response Team (APCERT), AusCERT has access to accurate, timely and reliable information about emerging computer network threats and vulnerabilities on a regional and global basis.

Additionally, AusCERT maintains a large network of trusted CERT contacts in North America, the United Kingdom, Europe and throughout Asia. AusCERT utilises these contacts to receive early warning of global threats and to assist in responding to incidents which span jurisdictions.

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

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