IDEAS | PEOPLE | TRUST

2020 CYBER SECURITY SURVEY

FOREWORD

The operating landscape for all Australian and New Zealand organisations has shifted significantly since we released our last BDO and AusCERT Cyber Security Survey Report. COVID-19 has shaken industries and governments across the spectrum and has brought focus back to cyber resilience. The need to engage executives and lay the foundations for oversight and improvement are the roots of strong cyber security, and the cornerstone for a cyber risk management approach driven from the top-down.

Our 2020 BDO and AusCERT Cyber Security Survey Report presents an interesting contrast between recurring themes and shifting investments. This year's results show a positive uptake in the engagement of leadership and risk visibility. It's these shifts that help our critical sectors enhance their capabilities to interpret and respond to the rapidly changing cyber threat landscape.

COVID-19 changed the way organisations operate, and our survey found it resulted in a cyber 'reality check', with many respondents realising they were overconfident and underprepared when it came to cyber risk. The threat landscape has changed, with data breaches rising significantly and organisations facing more sophisticated adversaries than ever before. While many respondents were prepared for the impacts presented by COVID-19,

KEY INSIGHTS

CONTINUED

almost all still directed extra investment into cyber security in response to the pandemic's impact. These initial investments focused on rapidly assembling secure remote working arrangements, allowing organisations the flexibility they needed to survive dramatic shifts in business operations. The initial rush to video conferencing and secure cloud technologies were, welcomingly, followed by efforts to 'catch up' to the risks their adoption introduced. Efforts must now be focused on establishing the essential oversight and visibility of risk required to secure these technologies into the future.

Never before has the modern world seen such a rapid, global rush to digitise business practices. Boards are now more cyber engaged than ever before, and more Chief Information Security Officers (CISOs) are being appointed – a necessity borne through our greater reliance on technology. We are hopeful this engagement will help mature our industries to address a consistent deficiency noted across five years of BDO and AusCERT Cyber Security Survey data - most organisations fail to interpret their threat landscape accurately. To effectively manage cyber security threats and risks, organisations must understand where the threat is coming from, which assets adversaries are seeking to compromise, and the methods they'll use to do so. Without appropriate cyber threat intelligence, organisations risk under-investing in areas that need it, and over-investing in areas that don't – exposing themselves to threats and risks without the resilience required to manage their impacts.

Our survey has shown encouraging themes of improvement. Through 2020, our industries and regions made years of digital progress within months.

This progress introduces opportunities, as well as risks – and we are at a crossroads. The past 12 months have demonstrated just how rapidly the cyber threat landscape can evolve. Now more than ever, organisations understand the importance of clear, ongoing visibility into their cyber threats and risks.

Organisations must now focus their efforts on building and improving this visibility if we are to continue safely enjoying the conveniences and opportunities that working remotely has introduced.

Thank you to all participants in this year's survey, and those who took part in previous surveys. Without your honest input and ongoing support, we cannot obtain and analyse data the represents the collective state of cyber security in our region. We greatly appreciate your efforts and look forward to furthering our understanding of the cyber threat risk landscape for Australian and New Zealand organisations with you.

Leon Fouche

National Cyber Security Leader,

BDO

Leon fouche

David Stockdale

Director,

AusCERT

COVID-19 IMPACT ON CYBER SECURITY

The environment that has emerged from the COVID-19 pandemic has driven a shift in attitude amongst organisational leaders in Australia and New Zealand. With changing priorities and highly publicised cyber security breaches occurring during the pandemic, many organisations have followed through on their planned implementation of cyber security controls from previous years.

THE REALITY CHECK INDUSTRY NEEDED

Respondents reported increases in cyber controls implemented during 2020, but COVID-19 appears to have been a reality check. Many organisations unfortunately learnt the hard way they were overconfident in their cyber risk posture. 2020 was a cyber 'trial by fire' for many, so it's unsurprising our survey found 20% of respondents are less confident or more uncertain in their ability to respond to cyber attacks now than pre-COVID-19. Respondents confident in tackling cyber threats during COVID-19 reported increased cyber budgets and clear cyber priorities. They also faced far less difficulty finding qualified staff compared to previous years. This confident cohort's increased budget and clear cyber priorities are likely tied to a notable increase in cyber risk reporting to the Board during initial shifts to remote working.

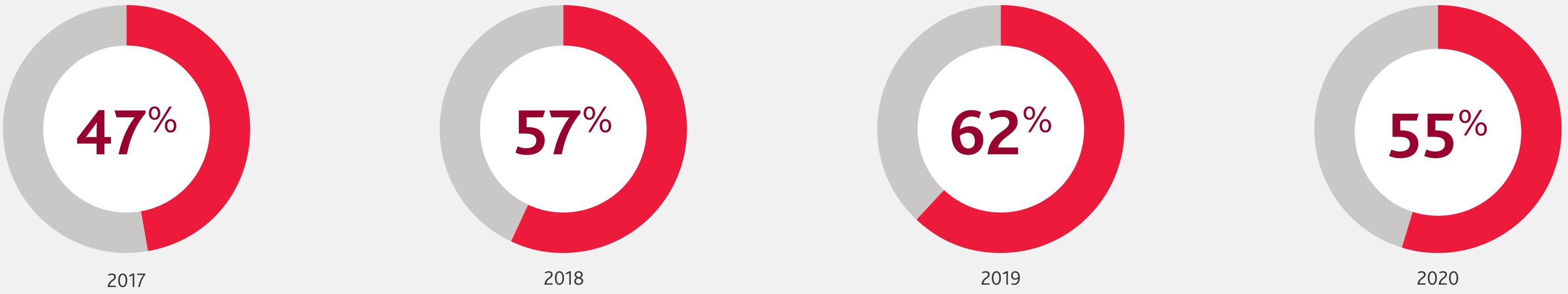
INCREASED ADOPTION OF CONTROLS

There is little doubt the pandemic led to increased adoption of cyber security controls. Prior to COVID-19, two-thirds of respondents reported having secure remote working capabilities, and those that did, experienced 40% less incidents overall. Respondents who were unprepared for the new remote working environment experienced four times as many data breaches via the supply chain, four times as many payment redirection fraud attacks, three times as many business email compromises and almost three times as many malware infections.

While many respondents had remote working measures prior to COVID-19, 85% of all organisations still made cyber investments in response to the changing situation.

As COVID-19 began to impact the globe, close to one in three respondents enhanced email security or implemented or upgraded VPN access. Another third saw an increase in IT resources, and more than 40% improved cyber security training and awareness efforts.

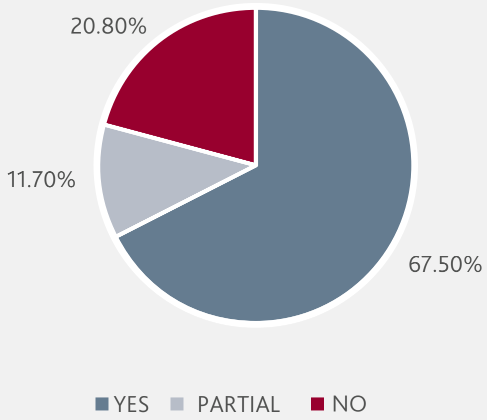
CONFIDENCE IN MANAGING CYBER INCIDENTS



GREATER INSIGHT FOR THE BOARD

The COVID-19 pandemic response led to significant changes in the way organisations structure their cyber security efforts. Boards have become increasingly concerned with cyber risk, as IT teams rapidly embedded new technology across their organisations. Shifts to digital service delivery, working-from-home arrangements, and an increasingly digitised business environment have changed fundamental business practices. These changes introduced new opportunities and new risks. Organisations must now focus on bridging the cyber risk gaps across these new processes and technologies.

ORGANISATIONS WITH SECURE REMOTE WORKING ARRANGEMENTS PRIOR TO COVID-19

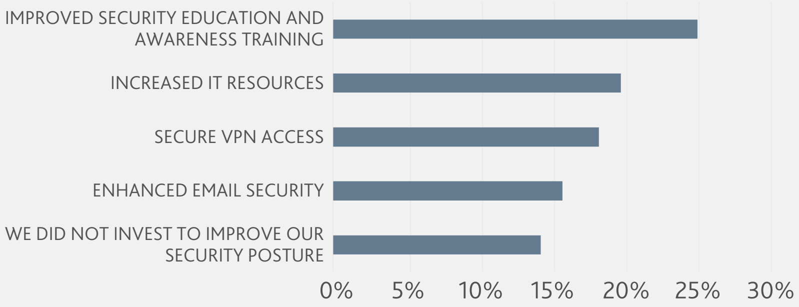


CYBER IS A BUSINESS ISSUE, NOT AN IT ONE

COVID-19 was also a reality check for many organisations across the world. It's emphasised that cyber security is a business priority and not an IT issue. Successful cyber responses to COVID-19 have demonstrated the importance of remaining responsive to, and informed about, the cyber threat landscape.

The pandemic forced organisations to confront the reality of their cyber resilience. Many who were overconfident and under-prepared have faced more significant cyber challenges, incidents and impacts since the emergence of COVID-19. Now, understanding the realities of their situation, many business leaders and owners recognise that cyber security is not a 'set-and-forget' issue. It requires constant oversight, investment and improvement to manage risks, many of which can emerge and worsen overnight.

WHAT CONTROLS DID YOUR ORGANISATION INVEST IN TO RESPOND TO COVID-19?



EVOLVING THREATS

DATA BREACHES RISING

Data breaches more than doubled in 2020 compared to the previous year, and accidental disclosures rose by almost 60%. In good news, one in four respondents increased their investment in information security education awareness training during the year, which would likely have avoided greater increases in the number of breaches.

Data breaches caused by malicious hacking increased by 91%. A staggering rise, likely caused by the lack of preparedness amongst respondents for increased cyber attacks during the COVID-19 pandemic. The professional and scientific industry experienced the most incidents, with almost 30% of all notifiable incidents being some form of data breach, whether accidental or deliberate.

SUPPLY CHAINS ARE AT RISK

Based on all respondent data, cyber attacks via supply chain are now more than 50% more likely than they were in 2016. This is a significant increase, but increasingly impacted those respondents who were not cyber-ready before COVID-19. Their reported supply chain data breaches more than tripled. Our prior surveys highlighted the importance of third-party risk assessments to build resilience through the supply chain. The rise in third-party data breaches is not surprising and has been on the radar of cyber risk decision-makers for a long time. That's why supply chain risk has been a driving factor in the Australian Government's push to secure our critical infrastructure sectors as part of the 2020 National Cyber Security Strategy.

RANSOMWARE ON THE DECLINE

The reported increase in data breaches correlates with the continuing and expected downward trend of ransomware (e.g. cryptolocker). Cybercriminals are changing tactics and turning away from ransomware. Instead, they are increasingly stealing sensitive data and threatening to disclose it unless a cyber ransom is paid. This technique is sometimes coupled with ransomware, also known as 'double ransom', and we expect to see an increase in these types of attacks during the next 12 months.

FOREIGN ACTORS STILL PREVALENT

Foreign governments have remained active, with attacks rising by 40% since last year, and doubling since 2016. From public sector respondents, 30% indicated that foreign governments were the most likely source of cyber security incidents during the past year. This is a sentiment that both our survey respondents and the Australian Government is expecting in the coming years. The release of the Australian 2020 Cyber Security Strategy highlighted the threat of foreign interference and espionage via cyber attacks.

Our 2019 survey found there were five top controls being adopted at a rapid pace:

- Chief Information Security Officers
- Security Operations Centres
- Cyber security awareness training
- Third-party/vendor risk assessments
- Cyber security incident response plans.

Respondents to that survey who implemented these top five controls experienced 31% less incidents than those without these implemented. It's unsurprising to see that this year, organisations who implemented the controls were 121% more likely to have complete alignment between cyber capability and business strategy. Contrastingly, not a single respondent without these controls reported 'complete' alignment between cyber and business.

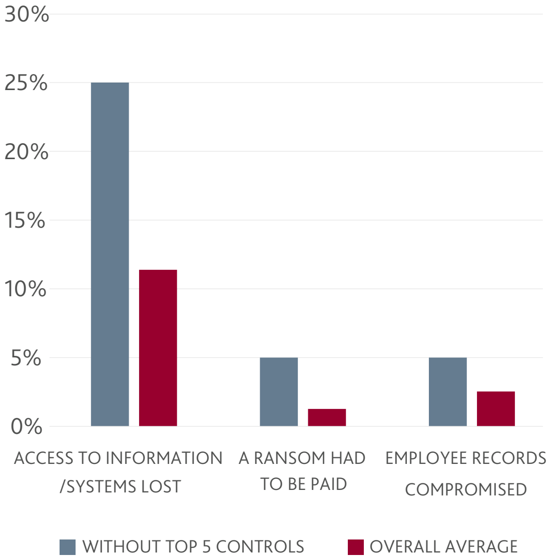
Attacks via supply chain are now more than 50% more likely than they were in 2016. This was far ***worse*** for those respondents who were ***not cyber-ready before COVID-19***. Their reported supply chain breaches more than ***tripled***.

EVOLVING THREATS
CONTINUED

This year, respondents with the top five controls experienced only two types of incidents - phishing and other miscellaneous attacks. Respondents without these controls may find themselves with a false sense of confidence, detecting fewer incidents than all other organisations on average. For example, respondents with the top five controls in place reported:

- 32% fewer data breaches caused by third parties/suppliers
- 45% less phishing attacks
- 32% less accidental disclosures.

INCIDENT IMPACTS WITH VS WITHOUT TOP FIVE CONTROLS



ORGANISATIONS MAY NOT HAVE A FULL VIEW OF THEIR EXPOSURE

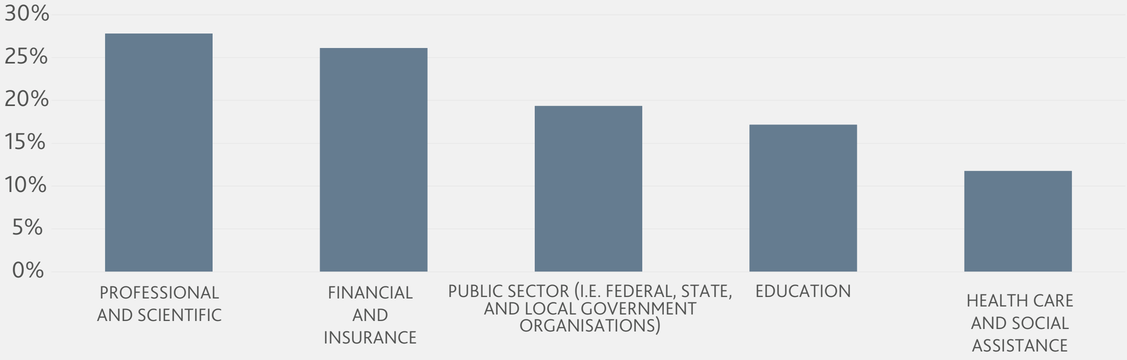
While it's possible that fewer cyber incidents have impacted these respondents, it's more likely they are not detecting them as well as those with the top five controls. This raises the concerning possibility that some organisations without the top five controls may be unaware they have experienced serious cyber security breaches at all.

Interesting, the incidents discovered by those respondents without the top five controls incurred more significant impacts. Organisations without the top five controls were:

- Almost four times as likely to need to pay a cyber ransom
- More than twice as likely to lose access to systems and data following a cyber incident
- Almost twice as likely to have employee records compromised in a data breach.

Respondents without the top five controls were almost twice as likely to expose personal records in a data breach, yet none of the respondents in this category reported those breaches to the Office of the Australian Information Commissioner. This suggests organisations without sufficient cyber resilience are not only failing to invest in the right areas and detect breaches, but are potentially failing to comply with data breach laws.

DATA BREACHES WITH SECURE REMOTE WORKING ARRANGEMENTS PRIOR TO COVID-19



CASE STUDY: PATIENT INFORMATION DATA BREACH

The sensitive details of every patient who received care from a public sector healthcare organisation between November 2020 and January 2021 were published online when unencrypted pager messages were intercepted.

WHAT HAPPENED?

In January 2021, a malicious website containing the information of a public sector healthcare organisation was discovered. The website contained more than 26,000 pages of sensitive information, including incident addresses, health condition, and HIV status. The third-party website continued to be updated with sensitive information contained within unencrypted pager messages sent every time paramedics were dispatched to patients.

WHAT WAS TARGETED?

The attack targeted unencrypted messages sent from radio-based pagers. The information contained within these messages was sensitive information that included information or insight into an individual's health or genetic information and sexual orientation or practices. Sensitive information requires a higher level of protection than personal information.

Patients were reasonably identifiable using the details contained in messages uploaded to the website. Patients dealing with family violence could be exposed to dangerous situations by having their addresses exposed.

WHAT WAS THE IMPACT?

The personal information contained within pager messages could be used to identify and locate individuals using leaked incident addresses. It's unknown how many people accessed the website, who accessed the website or whether the information uploaded to the website was saved elsewhere. A breach of patient information is harmful to healthcare providers because it impacts the organisation's reputation and its ability to protect patient information. It may also negatively impact current and future health initiatives like COVID-19 check-in practices because of lack of public confidence.

The case was referred to the Tasmania Police for further investigation and the Office of the Australian Information Commissioner for investigation under the Notifiable Data Breaches scheme.

ADAPTING TO THE THREAT LANDSCAPE

KNOWING WHO IS RESPONSIBLE FOR INCIDENTS IS CRUCIAL

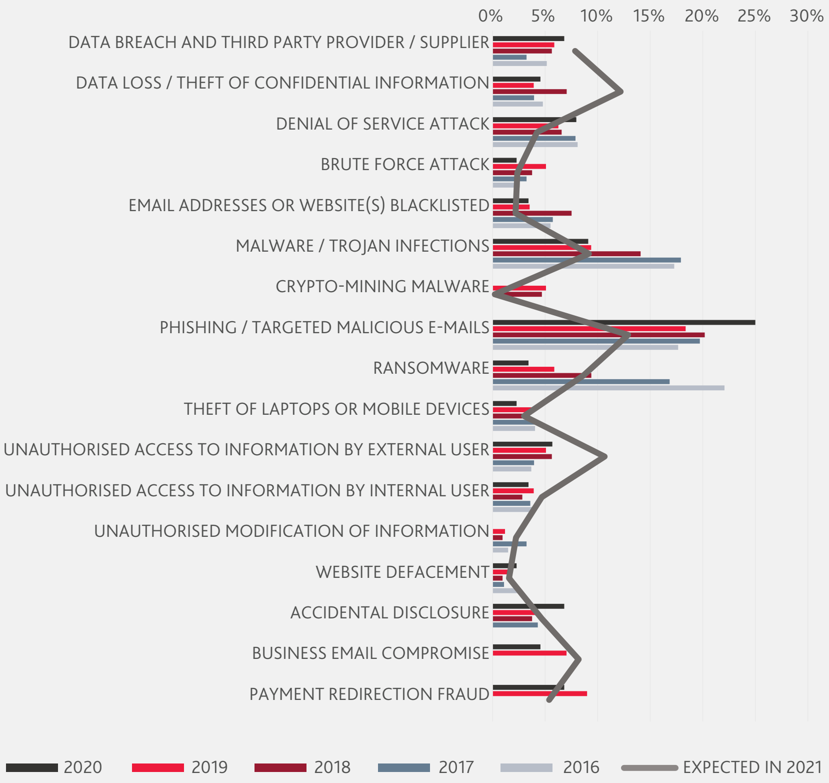
Analysing respondents' perceptions of who was responsible for cyber incidents and who will be causing them in 2021, highlights some insightful and concerning perspectives. In short, many organisations don't appear to understand which adversaries are targeting them, what assets they seek to compromise, and how they will do so.

Respondents expect data loss via supply chains to increase more than three and a half times in 2021. Similarly, they expect data breaches by external hackers to increase more than 150%. While we can expect an increase in supply chain loss and malicious data breaches, such dramatic increases may not be so likely.

Respondents suggested cyber criminals were responsible for 56.8% of all their incidents in 2020, yet they expect cyber criminals to cause just 19% in 2021. Interestingly, it's the opposite story with hacktivists. Respondents believed activists were responsible for 2% of all their incidents in 2020, but anticipate the incidents caused by this actor to be almost four times more common in 2021.

Surprisingly, many respondents were less concerned with accidental disclosure than its prevalence in 2019 would suggest. Similarly, against five-year downward trends, the average respondent expected ransomware to increase by a staggering 240% in 2021. Given their counterintuitive nature, many of these predictions may be less informed than they should be. This suggests many respondents don't understand their cyber threats and risks, which could mean they are potentially focusing cyber investment in areas that won't need them, and under-investing in areas that do.

INCIDENTS EXPERIENCED VS EXPECTED



GREATER INSIGHT TO THE THREAT LANDSCAPE IS NEEDED

As with prior years, the survey highlighted that respondents require greater clarity and a deeper understanding of the threat landscape. Cyber threat intelligence helps organisations understand who's targeting them, which assets they seek to compromise, and how they'll do so. This knowledge allows them to invest in the right cyber controls, and be prepared to defend against these attacks.

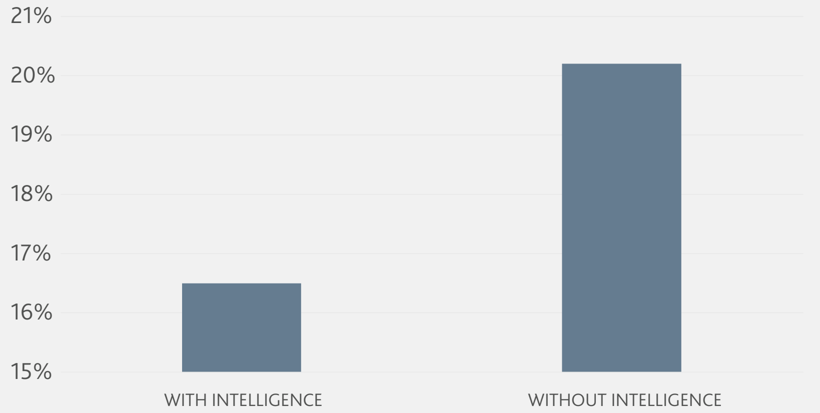
Therefore, it's unsurprising that respondents with Cyber Threat Intelligence (CTI) capabilities experienced an almost 20% reduction in incidents compared to those without intelligence during 2020.

Organisations with a better understanding of the threat landscape can adapt to it more effectively. Interestingly, but perhaps as expected, respondents with threat intelligence capabilities had different predictions for the year ahead than their peers without:

- Organisations with CTI capabilities expect accidental data breaches to increase in 2021, whereas those without expect them to decrease
- Those with CTI expect website defacements to increase, whereas those without expect them to decrease
- Respondents with CTI capabilities are half as concerned with malware infections in 2021 than those without CTI
- Organisations without CTI are six times more concerned with payment redirection fraud than those with CTI capabilities.

Each organisation is unique, with its own business imperatives, drivers, opportunities and risks. They exist in different sectors, regions, and sizes. Their cyber threats change and vary depending on the nature of their operations and the stakeholders they engage with. As such, some organisations may be rightfully concerned about cyber risks that many others may deem as insignificant - and vice-versa. For the past five years, the BDO and AusCERT Cyber Security Survey Report data has highlighted that most organisations fail to accurately predict which cyber threats they will face in the coming 12 months. This speaks volumes to the rapid-pace of evolving cyber threats and risks, but it's also connected to the stagnant adoption of cyber threat intelligence. In 2016, 53.90% of respondents had CTI capabilities. Compare that to 2020, where even less (52.30%) are reported to use CTI. To adequately manage cyber threats and risks, they must be understood. Evidence-based knowledge, such as CTI, is one of the most powerful tools in adapting to and navigating the cyber threat landscape.

INCIDENTS EXPERIENCED WITH VS. WITHOUT CTI



CASE STUDY: RANSOMWARE ATTACK ON MANUFACTURING FIRM

A large aluminium manufacturing firm needed to switch its factories to manual operations after a cyber ransomware attack shut down all of its computer systems.

WHAT HAPPENED?

In March 2019, an encryption process began running on numerous computers and servers within the organisation's network. The attacker used ransomware known as LockerGoga and logged out and locked employees' accounts to disrupt incident response efforts. LockerGoga did not have a known propagation mechanism and most likely spread throughout the organisation's systems after the attackers gained a foothold in the Active Directory.

WHAT WAS TARGETED?

The attack targeted the computers and servers on the manufacturer's network. While the exact number of devices infected with LokerGoga is unknown, LockerGoga was able to infect industrial control devices at manufacturing facilities. The organisation's email services are cloud-based and were not impacted by the attack, and staff were able to use email services on personal devices to maintain a basic workflow.

WHAT WAS THE IMPACT?

Manufacturing systems had to be disconnected from impacted computers and operated manually. Staff were unable to access the organisation's network for regular work and had to rely on cloud access to their email to conduct basic operations and client communication. The firm had no interest in paying the ransom demanded by the attacker and was forced to rely on backup solutions to retrieve computer systems. It's estimated the cost of restoring the organisation's IT systems amounted to more than $50 million.

PREPARING FOR THE 'NEW NORM'

PEOPLE AND PROCESSES ARE AT THE CORE

The BDO and AusCERT 2018/19 Cyber Security Survey shone a light on the alarming lack of preparedness across our respondent base. Organisations had traditionally focused heavy investment on security technology and systems. While important, technology is only one piece of the cyber risk puzzle. People and processes are both the front-line of defence and the glue that holds cyber defence technology and human skillsets together. Our 2018/19 survey called for greater focus on establishing oversight, governance, and tight procedures, to protect the business practices and technology organisations had invested heavily in establishing.

This focus was coupled with our expectation to see an increase in data breaches and phishing, targeting people and processes which are often the first line of defence. We also recognise that many organisations invest in expensive security technology, with neither the skill nor budget to sustain it. It's akin to giving a sports car to an inexperienced driver – and can end in expensive, and sometimes damaging outcomes. For 2020, many cyber practitioners were hoping for a reality check, encouraging industries to 'walk before they run', establishing solid foundations and getting the cyber-basics right before directing heavy investments into security technology.

CONTROL ADOPTION SPIKED

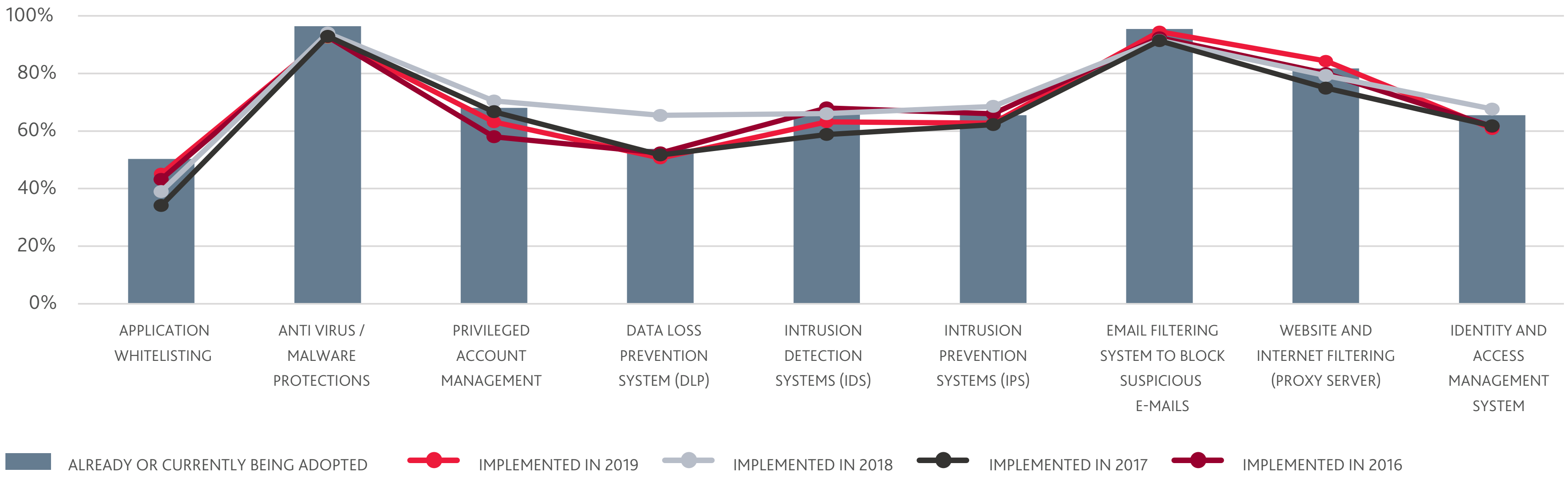
The COVID-19 pandemic impacted the expected trajectory for control adoption. Organisations focused on implementing the new technology needed to allow them to operate within devastating market changes and remote workforce requirements brought by COVID-19. C-Suites rapidly shifted budgets to accommodate necessary working-from-home systems, and IT teams, who are often under-resourced, were forced to put governance and oversight initiatives on the back-bench. Despite this initial rush, as the COVID-19 situation rolled through 2020, organisations began to proactively 'catch-up' to the cyber risk introduced by their rapid adoption of technology.

Throughout 2020, as COVID-19's impacts on the cyber landscape increased, organisations invested in bolstering their cyber postures. 2020 saw an 8% average increase in the adoption of cyber controls by respondents. Compare that to less than a 1% increase the prior year.

PREPARING FOR THE NEW NORM

CONTINUED

CONTROLS – IMPROVED PROTECTION OF ASSETS



RAPID CONTROL ADOPTION

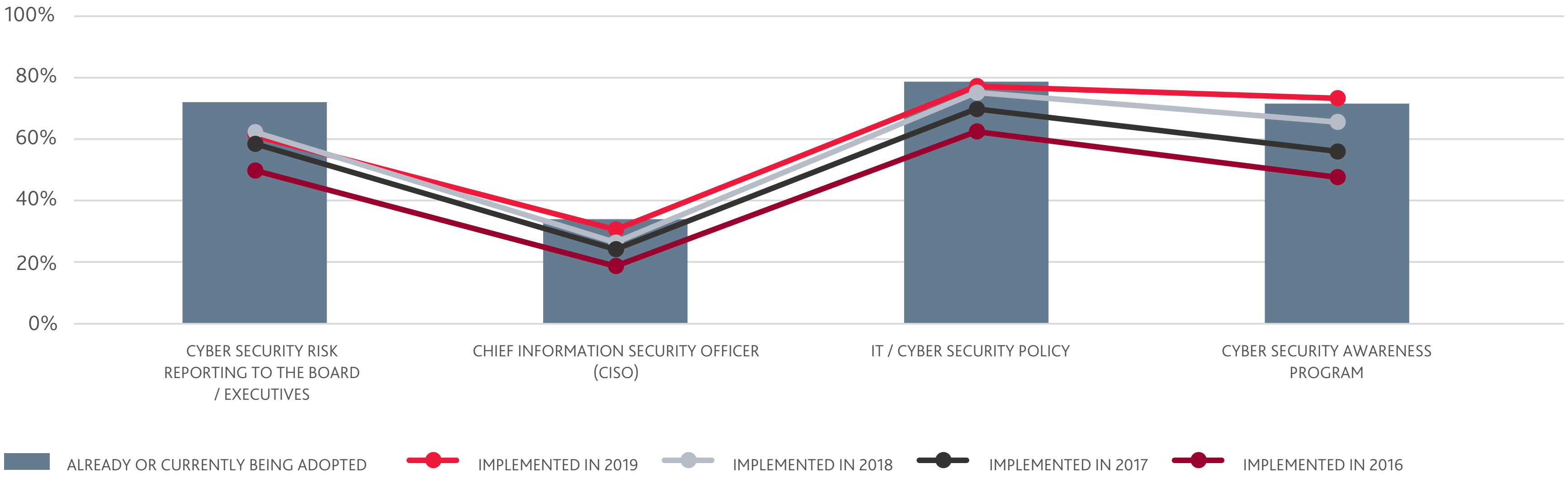
2020 saw a huge global effort with entire industries shifting towards remote working arrangements, increased networking capabilities, and significant cloud technology adoption. As social distancing requirements necessitated working-from-home, network traffic ramped up rapidly. This reliance on remote technologies, coupled with an increase in cyber threat activity globally, likely influenced organisations to seek out dedicated third-party security operations capabilities. Many respondents sought to formalise and firm-up roles and responsibilities with remote IT teams, which includes those in cyber security incident response. These factors have all played a role in the influencing the most rapidly adopted cyber controls in 2020.

- Mobile Device Management (MDM) systems saw a 26% increase – to improve security of user devices and connectivity for remote working arrangements
- Security operations centres increased by 18% - to improve operational security and support for remote user devices and workforce
- Cyber security risk reporting to the Board/Executives increased by 18% - to provide business leaders and decision makers regular updates on emerging cyber risks within their organisations
- Cloud security standards saw a 17% increase – to support secure integration of increased usage of cloud services (such as Zoom, Microsoft Teams, etc.)
- Cyber security incident response team/capabilities rose by 16% - to improve capability to respond to increased cyber attacks and provide remote incident response capability for remote workforce.

PREPARING FOR THE NEW NORM

CONTINUED

GOVERNANCE – ESTABLISHING STRONG LEADERSHIP



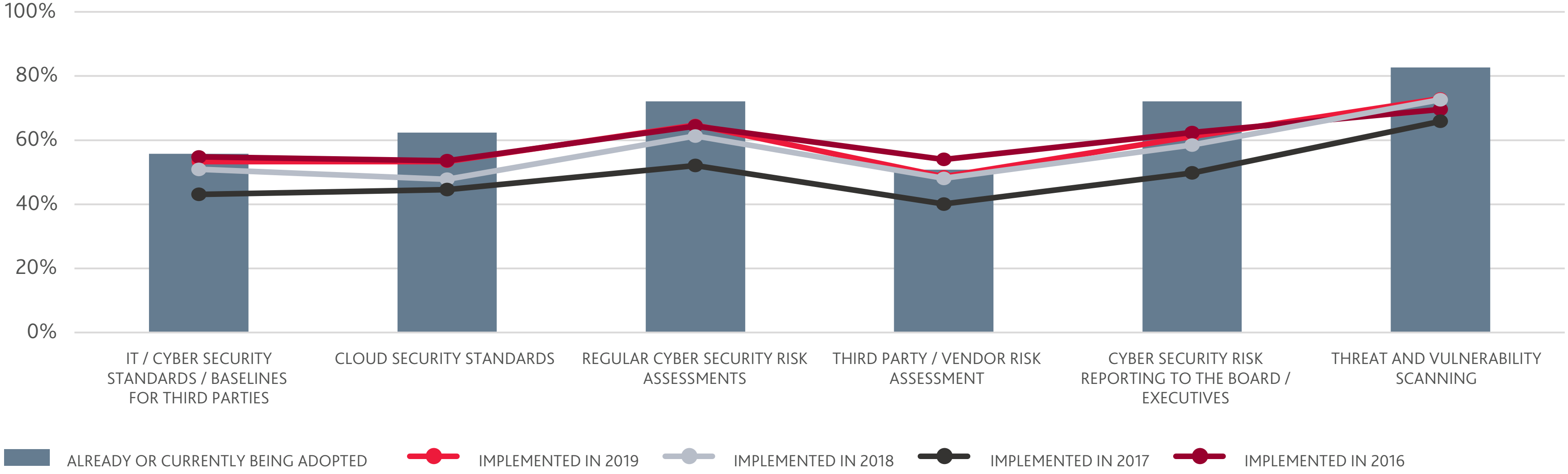
CISO APPOINTMENT AND BOARD REPORTING ON THE RISE

With growing concern at the Board level for the impacts of rapid technology changes, it's unsurprising that the 2020 survey results showed a significant increase in the appointment of CISOs (11% increase), and cyber risk reporting to the Board (18% increase). CISOs and Boards were understandably concerned with risk introduced by cloud technologies through 2020, which correlates with a 17% increase in cloud security risk assessments, and an 11% rise in regular cyber security risk assessments generally.

PREPARING FOR THE NEW NORM

CONTINUED

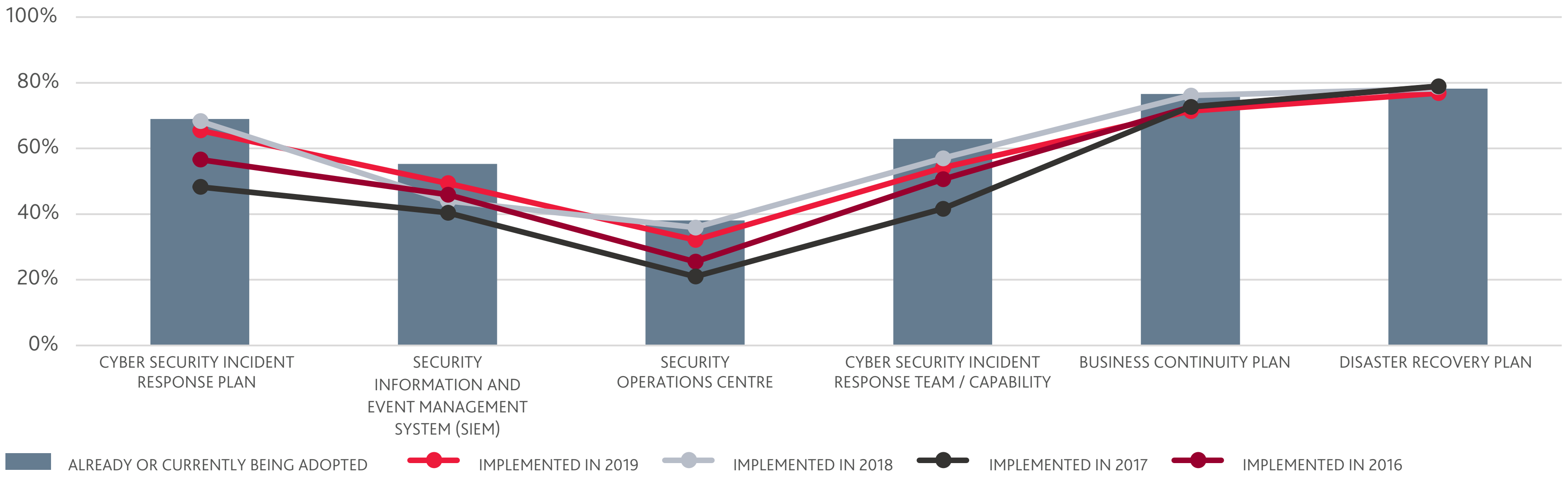
RISK VISIBILITY – UNDERSTANDING THE THREAT ENVIRONMENT



PREPARING FOR THE NEW NORM

CONTINUED

RISK IMPACT – INCIDENT DETECTION AND RESPONSE



SURVEY METHODOLOGY

BDO and AusCERT deliver the annual cyber security survey to identify industry trends across private and public small to medium-sized organisations across Australia and New Zealand.

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 findings presented in this survey report provides a more relevant benchmark for organisations in Australia and New Zealand, who are not necessarily subject to international legislation that has driven cyber security trends in North America and Europe.

In 2020, we conducted the fifth 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, 87% were based in Australia, 8% were based in New Zealand, and 5% were based internationally. BDO normalised 2019 and 2020 survey data.

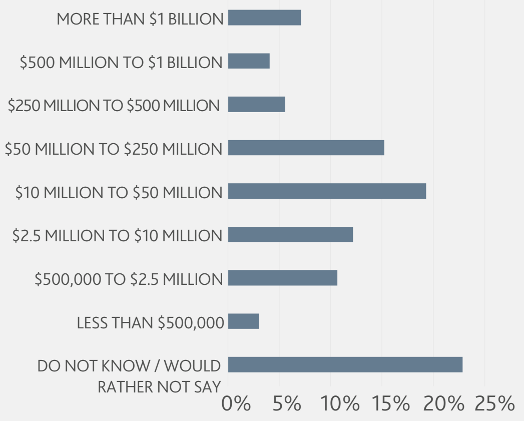
Our survey covered a wide variety of organisation types, across a range of industry categories. Most 2020 survey respondents were from five key industries:

- 17% were from the public sector
- 14% were from the professional, technical and scientific services industry
- 13% were from the education and training industry
- 12% were from the health care and social assistance industry
- 12% were from the financial and insurance services industry.

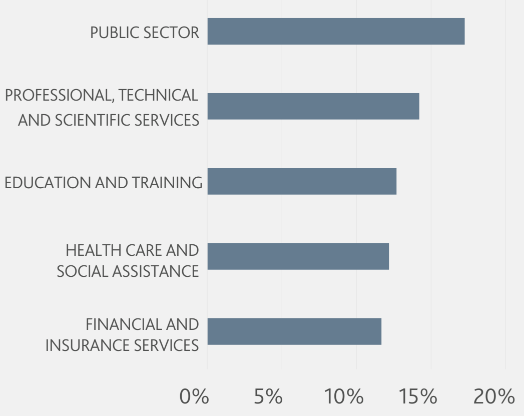
The individuals completing the survey were closely connected to cyber security and their organisation's risk management responsibilities:

- 45% were C-level executives
- 31% were IT/Security Managers
- 17% were Security Analysts/Engineers
- 1% were Internal Auditors
- 7% were in other roles.

RESPONDENT ORGANISATIONS ANNUAL REVENUE



TOP 5 RESPONDENTS



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.

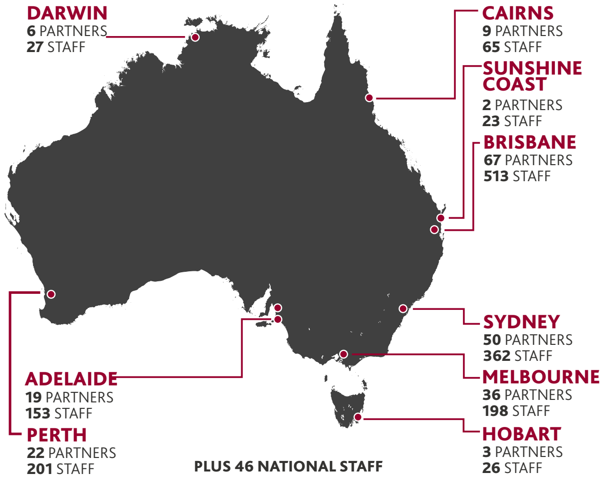
For more information about BDO services, visit www.bdo.com.au or www.bdo.co.nz.

1,828 PEOPLE

10 **OFFICES**

214 PARTNERS

FIGURES TAKEN AS AT 01 FEBRUARY 2021



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 cyber security 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

AUSCERT

AUSTRALIA'S PIONEER CYBER EMERGENCY RESPONSE TEAM

SERVICES

- Incident Management
- Phishing Take-Down
- Security Bulletins
- Security Incident Notifications
- Sensitive Information Alert
- Early Warning SMS
- Malicious URL Feed
- Education

1300 138 991
www.bdo.com.au

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

AUDIT • TAX • ADVISORY

This publication has been carefully prepared, but it has been written in general terms and should be seen as broad guidance only. The publication cannot be relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact the BDO member firms in Australia to discuss these matters in the context of your particular circumstances. BDO Australia Ltd and each BDO member firm in Australia, their partners and/or directors, employees and agents do not accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

BDO refers to one or more of the independent member firms of BDO International Ltd, a UK company limited by guarantee. Each BDO member firm in Australia is a separate legal entity and has no liability for another entity's acts and omissions. Liability limited by a scheme approved under Professional Standards Legislation.

BDO is the brand name for the BDO network and for each of the BDO member firms.