BDO

IDEAS | PEOPLE | TRUST

2021 CYBER SECURITY SURVEY

AUSCERT

FOREWORD

With a record number of respondents this year, it's evident many organisations and their employees continue to grapple with cyber security incidents, increasing regulatory requirements, inadequate budgets and the lingering impacts of COVID-19. As the focus of cyber attackers shifts to highly-targeted campaigns, the need for organisations to continually optimise their cyber security strategy is paramount. The key to cyber security is not only identifying the common risk and pain points but industries and cyber experts working together to identify the right solutions.

KEY INSIGHTS

Our 2021 report explores how cyber security leaders are faring and the progress made during the year when COVID-19 was predicted to end. This year's survey saw a record number of respondents across a range of industries, reinforcing the interest and focus on cyber security services. The continual growth of remote working, digitisation and disruption trends accelerated by the COVID-19 pandemic, have been reinforced by respondents and proven to be a major focus of organisations' holistic strategies.

High-profile cyber attacks impacting supply chains and critical infrastructure, and the Log4j vulnerability, caught many organisations off guard. This continuing digitisation highlighted a worrying trend of increasingly frequent, costly and damaging cyber security incidents involving data breach scenarios. However, more organisations are responding to this threat by taking the appropriate intelligence and defence measures. Encouragingly respondents reported an increase in training and awareness, highlighting the importance of the human factor when it comes to cyber security.

KEY INSIGHTS *CONTINUED*

Organisations without cyber insurance or cyber threat intelligence are now in the minority, and this year's respondents across the board are investing in greater incident response capabilities, including technical measures such as security operations centres, and dedicated incident response personnel.

The reliance on third-party service providers continued into 2021, but so too did data breaches of third-party suppliers, which increased by 50%. This highlights the risks placed on these organisations to not only secure and protect critical information but to remain operational in the face of continued cyber threats.

Ransomware remained a top threat throughout 2021, with large scale criminal groups showing no sign of slowing down. There has also been a paradigm shift in the broader business model with the emergence of 'ransomware-as-service'. This is a solution that allows cyber criminals to lease existing ransomware products to other organisations who may not ordinarily have the expertise or capacity to carry out an attack on their own.

There were also increasing changes and scrutiny in regulation during 2021, as regulatory bodies looked to shore up the cyber resilience of Australian and New Zealand organisations, government and critical infrastructure.

Looking at the year ahead, the most concerning threats indicated by respondents include data breaches, supply chain risks and ransomware. The source of cyber attacks being foreign governments and cyber criminals was also a key concern. Interestingly, there was a 64% increase in the number of respondents indicating they believe business competitors will be responsible for cyber incidents, signalling an interesting shift in the link between competitive and cyber risk landscapes.

The past 12 months demonstrate the ongoing complexities and wide-reaching impacts of cyber security. Our survey continues to show encouraging signs that organisations are seeking to understand the impacts of cyber attacks and forge the appropriate cyber resilience strategies.

2022 looks set to be another challenging year, with mainstay threats in the form of ransomware and increasing attacks on supply chains, and new challengers such as Artificial Intelligence (AI), as defenders and attackers look to leverage machine speed.

As always, we would like to thank the participants in this year's survey, and those who took part in previous surveys. It is through your participation, honest input and ongoing support, that we can obtain and analyse data that 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 IMPACTS AND DIGITISATION CONTINUE

With the impacts of the COVID-19 pandemic lingering and an increasing number of cyber security attacks focused on the supply chain and critical infrastructure, risk management and appropriate control selection and testing is still front of mind for many organisations.

INCREASE IN RISK MANAGEMENT

Building on the lessons encountered in 2020, many organisations have reacted quickly and responded to not only the change in working practices, but also the increased cyber risk profile the impacts of the pandemic created.

As we progress, we have seen an increasing focus on cyber risk management and control implementation overall, covering a broad focus, ranging from governance measures to technical controls. This includes the implementation of:

- Incident response capabilities
- Technical controls
- Governance
- Policies and standards
- Risk visibility rules and guidelines
- Risk impact procedures.

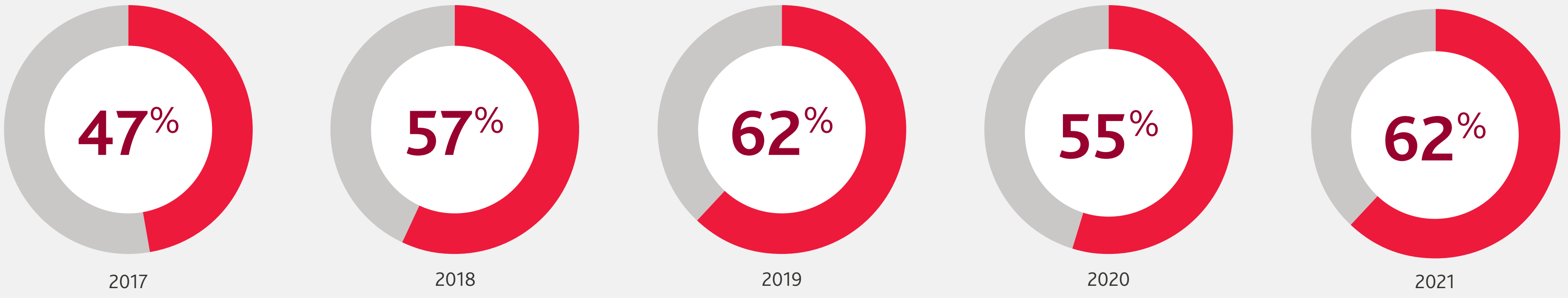
INCREASE IN DETECTIVE AND PROTECTIVE MEASURES

Nearly two thirds of respondents have implemented data loss prevention and intrusion detection mechanisms. With more than 90% implementing antimalware, virus and email filtering solutions. Insider threat protection continues to be an area of concern, with increases in both traditional identity and privileged access management.

Even with a clear understanding of potential threats and the adoption of more controls, organisations remain cautious when it comes to responding to cyber attacks, with "more confidence" increasing by 12% and "less confidence" increasing by 34%, since 2020.

This caution is likely to be appropriate given the challenge in hiring cyber security professionals and the continued adoption of third-party services. Respondents reported a 14% uplift in performing cyber security assessments over third-parties, and a 13% uplift in requiring third-parties to adhere to baseline cyber security policies and standards. These were the two largest increases in the category of managing cyber reliance.

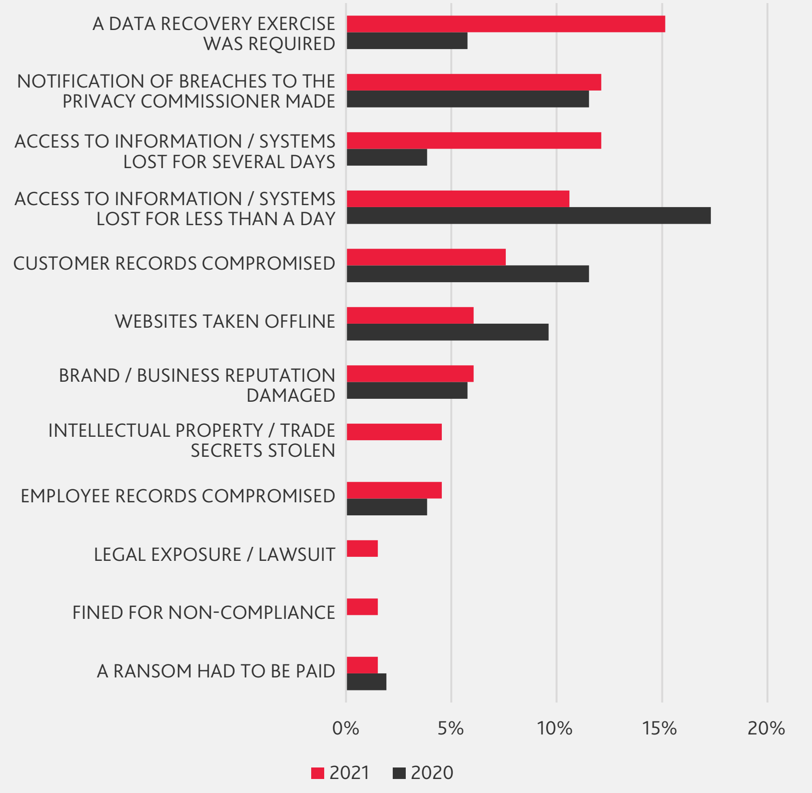
CONFIDENCE IN MANAGING CYBER INCIDENTS



RANSOMS ARE ADVANCING

There was a significant decrease in the number of ransom payments, yet the number of incidents requiring data recovery efforts increased by 2.5 times. There was a 5% increase in reportable data breaches and the number of incidents causing extended system outages rose by 3 times compared to 2020.

IMPACT OF CYBER SECURITY INCIDENTS



CYBER INCIDENTS, MORE THAN JUST RANSOMS

Each year, as the ways we work and the systems we use continue to evolve, cyber security threats become more advanced and spread at a higher rate. During the past 12 months, there was a noticeable decrease in the volume of ransom payments made by organisations since the previous year, however many other areas have seen alarming increases. For instance, the number of security incidents involving data recovery efforts saw a concerning rise of nearly 160%, with a 5% increase in reportable data breaches accompanying this.

Respondents are realising it's important to look at cyber security incidents as more than just ransoms paid. Industry professionals have noticed that although the number of ransoms being paid is decreasing, the targeting of larger organisations or 'big game hunting' of ransoms is maturing.

TARGETED ATTACKS CAUSING DISRUPTION

Hackers are becoming laser-focused and highly targeted in their ransomware campaigns. We see much less broad spectrum 'spray and pray' techniques, and a significant uptick in targeted double extortion attacks (where hackers encrypt systems and breach data, demanding a ransom for the safe restoration of both) and the overall success of ransomware when it is deployed.

Cyber attacks are becoming more disruptive, requiring significantly more time to recover from. Compared to the prior year, the number of cyber attacks during the past 12 months causing multiple days of system downtime increased by nearly 215%. Consequently, each year we are seeing a steady decrease in disruptions lasting less than one day, further cementing the conclusion that cyber threats are becoming more advanced.

CASE STUDY: RANSOMWARE PAYMENT BY A HEALTHCARE PROVIDER

While we are seeing a reduction in the number of ransomware payments made, these attacks appear to be more targeted and sophisticated, targeting larger organisations where impacts will be far reaching.

WHAT HAPPENED?

In April of 2021, an Australian health and community care provider fell victim to a ransomware attack, disrupting access to the healthcare provider's core systems, and forcing facilities to revert to pen-and-paper operations. The attack encrypted large amounts of the organisation's data, as well as attempting to delete backups before a ransom demand was made. Shortly after the initial attack, the notorious hacker group 'REvil' claimed responsibility for the breach, while providing an initial ransom demand and starting the response countdown.

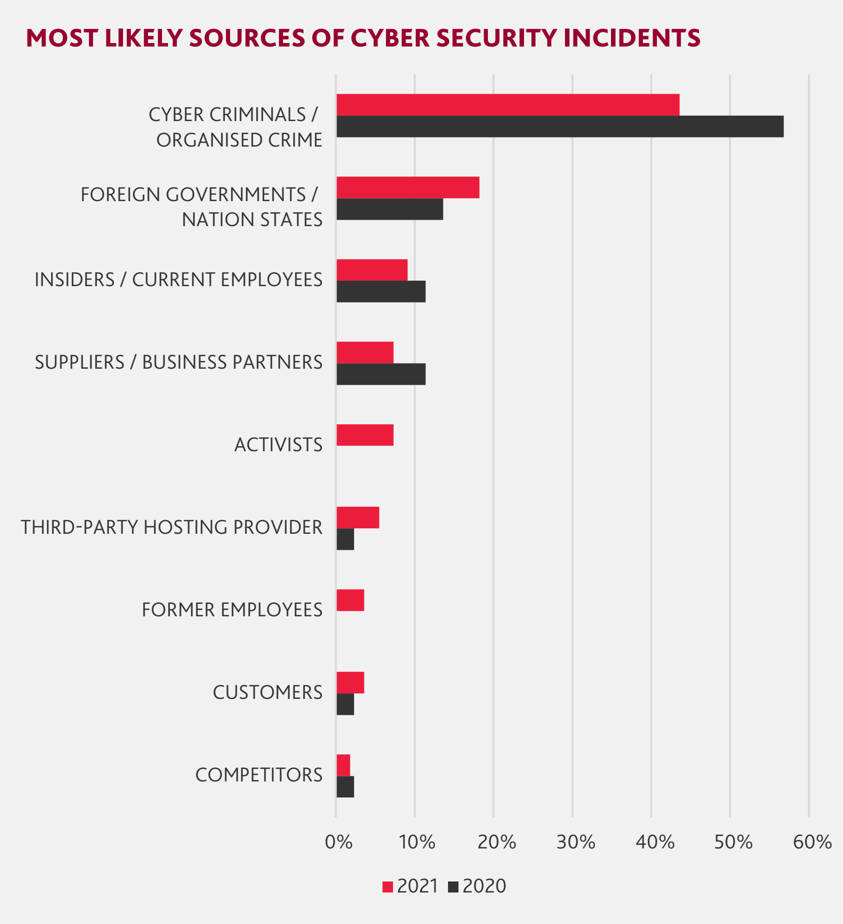
WHAT WAS TARGETED?

The ransomware attack followed traditional tactics - sending targeted phishing emails, installing ransomware, encrypting data, deleting backups, and as a consequence, barring access to wide range of key systems. In 2021, the OAIC reported that attacks on the healthcare sector accounted for 168 of 910 data breaches. As healthcare providers by nature hold large amounts of personally identifiable information and sensitive medical information, it is believed cyber criminals are specifically targeting this sector as priority target. Furthermore, due to the effects of the COVID-19 pandemic, healthcare provider resources were already severely stretched at this time, making them an 'easy target'.

WHAT WAS THE IMPACT?

Due to the severity of the attack, key systems of the healthcare provider were unusable and unstable for several months, with the organisation resorting to legacy operations, unable to process payments, and recording patient information through paper processes. Ultimately, the hacker group 'REvil' demanded $1,000,000 for the restoration of their data and systems. Through careful third-party negotiation with 'REvil', with many offers for payment were rejected and renegotiated. The hacker group eventually agreed to accept a payment of $300,000 in Bitcoin, with a 10% processing fee to be paid by the victim. Upon payment of the ransom, the healthcare provider's systems and data were restored. Although the healthcare provider managed to significantly reduce the ransom payment demand, the real financial and reputational costs will have been significantly higher than the Bitcoin payment.

THE CYBER SECURITY LANDSCAPE



FOREIGN INVOLVEMENT

In 2020, most respondents believed cyber criminals were responsible for their attacks. However, in 2021, respondents felt there were other forces at play. There was a 33% increase in the number of organisations that thought foreign governments were responsible for cyber attacks against them. With current socio-political landscapes and various regional tensions rising, it can be expected that this number will continue to increase in the coming years.

THE RISE OF HACKTIVISTS

In 2020, no respondents identified activists (or 'hacktivists') as a responsible party for organisational cyber attacks. Activists now comprise nearly one tenth of likely sources attributed to cyber security incidents identified in 2021 for the previous year, attributed to the growing understanding of climate change, the global pandemic and regional tensions.

THIRD-PARTY HOSTING PROVIDERS

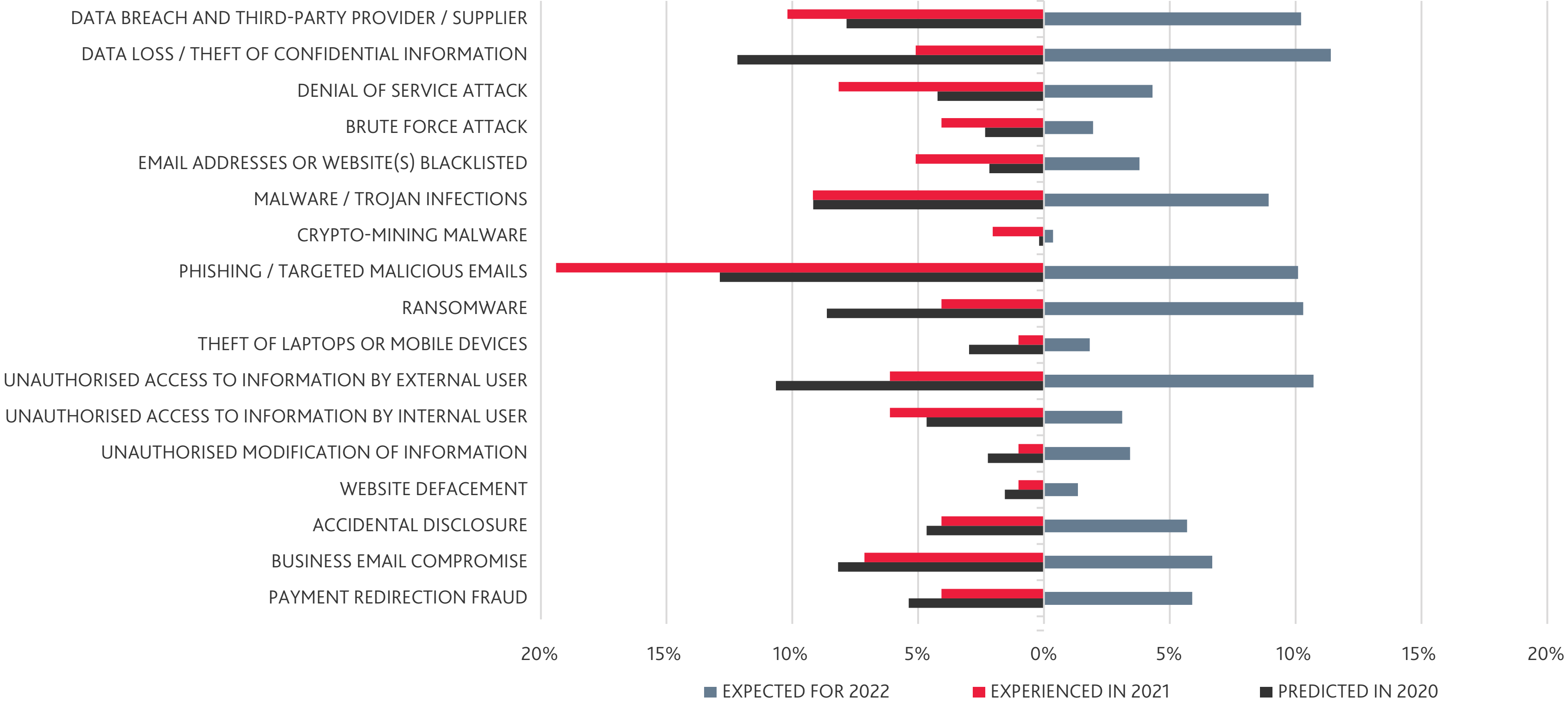
Third-party hosting providers were identified as a likely source of cyber security incidents that took place in 2021, constituting more than 5% of all sources identified. It is likely this increase is due to the added reliance placed on third-parties as a consequence of the COVID-19 pandemic and work from home situation.

EVOLVING THREATS

Concerns surrounding data breach and third-party providers increased by 30%, due to increased digitalisation and a greater dependency on third-parties, such as cloud providers, associated with remote working.

Incidents related to phishing and malicious emails were 50% higher than expected, and expected to remain high as email is becoming the choice of communication in an increased digital world.

INCIDENTS EXPERIENCED IN 2021 VS INCIDENTS EXPECTED IN 2022



EVOLVING THREATS
CONTINUED

THREATS LURKING AS WE WORK FROM HOME

With the effects of the COVID-19 pandemic still lingering in the workplace, and with working from home becoming a preferred solution for many around the world, the reliance on third-party vendors has never been higher. With cloud storage, data sharing and remote collaborative working being front of mind, the days of USBs and portable hard drives are numbered. These trends have not gone unnoticed by industry professionals, with concerns surrounding data breaches in third-party suppliers increasing by more than 30% in 2021. For many industries, their data and intellectual property is what keeps the lights on, so it is no surprise that concerns surrounding data breaches have dramatically increased.

The increase in remote working didn't come without its challenges, although cyber awareness training has been steadily implemented across all industries.

We are now receiving more emails than ever before. What is concerning is that incidents related to phishing and malicious emails are 50% higher than what was expected indicating that more work is required on awareness training.

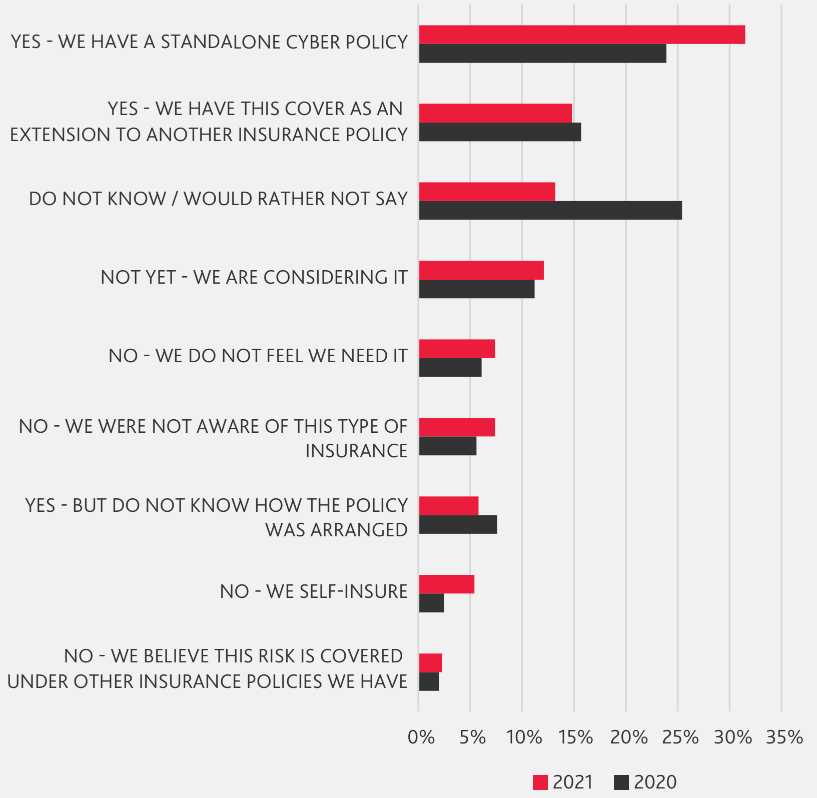
Other concerns, such as theft of confidential information and unauthorised access to information by an external user, have remained largely unchanged year-on-year. It is suspected these areas will always be of concern due to the inherent severity of the impacts resulting from these types of incidents.

THE GROWTH OF CYBER INSURANCE

More than half of respondent organisations now hold some form of cyber insurance policy.

Insurance brokers are now providing a greater range and choice of cyber insurance, indicating maturity in the space.

DOES YOUR ORGANISATION HAVE CYBER INSURANCE?



ADOPTING TO CYBER INSURANCE

With cyber security attacks making headlines more regularly, and organisations watching their peers suffer from the financial pressure as they recover from these attacks, many are beginning to realise the importance of cyber insurance. From the respondent data, it's been identified that more than half of organisations now hold some form of cyber insurance policy. Furthermore, the number of organisations with a standalone cyber insurance policy increased by 33%.

It's impossible to predict exactly when your organisation may be subject to a cyber security attack and unfortunately, this is out of your control. Preparedness, however, is in your control, and when it comes to the livelihood of your organisation, your staff and your clients, it pays to be safe rather than sorry.

Fortunately, insurance brokers are now providing a greater range of choice in cyber insurance, offering services such as negotiators and forensic analysts. This indicates growing investment and maturity in this space.

The adoption of cyber insurance is consistent with the 2022 World Economic Forum's Global Risks Report* findings that Australian business leaders see failure of cyber security measures as the number one risk to their organisation.

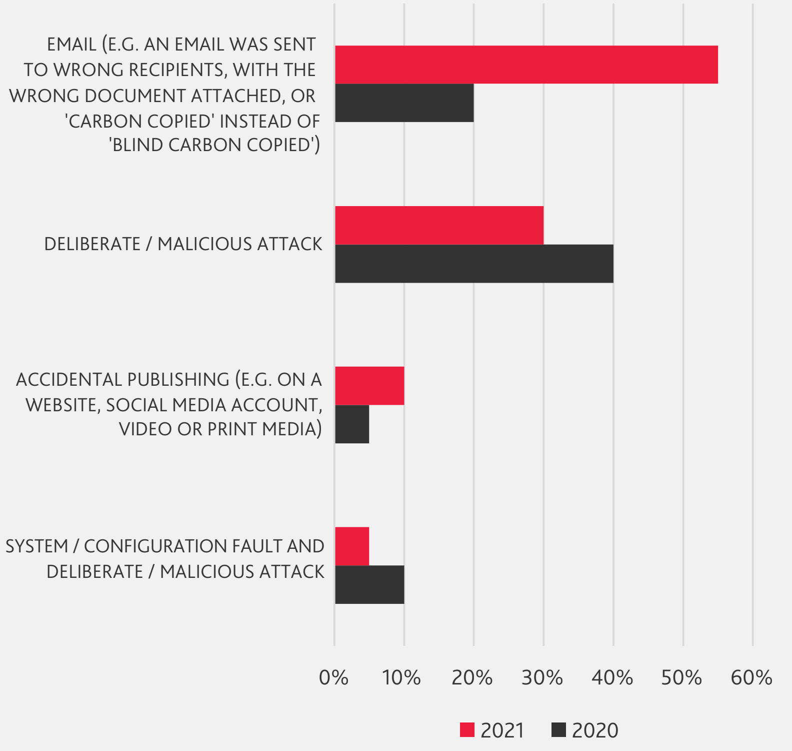
* https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf, page 96.

EMAIL DATA BREACHES RISING

There has been a staggering 175% increase year-on-year for emails being the source of data breach, accounting for more than half of respondent data breaches.

The move to working from home setups as a result of the COVID-19 pandemic saw sources like physical letters, theft of physical records, and insecure disposal drop drastically.

WHAT WAS THE SOURCE OF THE DATA BREACH?



EMAIL LEADING THE WAY FOR DATA BREACHES

As previously referenced, reportable data breaches have increased by 5%, with an astounding 160% rise in data recovery exercises being necessary. It is not surprising to see these statistics when data breaches as a source are put under the microscope. From respondent data, a staggering 175% year-on-year increase was found for emails being the source of respondent data breach. This could be attributed to users sending emails to the wrong recipients with the wrong documents attached, as well as the incorrect use of autocomplete.

This is another instance that can be linked to the persistent effects of the COVID-19 pandemic, and in turn working from home. Working remotely introduced a range of new systems and issues, including that of document sharing and distribution, especially during the early adoption of remote working. Where once employees could share sensitive information through secure physical drives, or established network drives, first instinct went to email as the solution for information distribution. Consequently, data breach sources regularly identified in prior years such as unauthorised written disclosures (letters sent to incorrect stakeholders), theft of physical records, and insecure disposal saw a dramatic drop off, with respondents not even identifying them as data breach sources in 2021.

While these statistics may remain buoyant as working from home continues to be the norm, they should not detract from the observation that changes in infrastructure can cause critical impacts to the safety and security of an organisations data and intellectual property.

CASE STUDY: ACCIDENTAL EMAIL DATA BREACH OF PERSONAL DATA AT SPORTING ORGANISATION

Email is becoming the main source of communication and collaboration in the modern workplace. Over 30% of all data breaches reported to the Office of the Australian Information Commissioner (OAIC) relates to human error.

WHAT HAPPENED?

Mid 2020, a member based sports organisation (club) experienced a data breach due to an email with a spreadsheet attachment containing personally identifiable information being sent to long-term club members. The spreadsheet contained the full names, dates of birth, home addresses and contact details of more than 500 club members. The data breach was identified the following morning, at which point the club attempted to recall the email before the information could spread further. Unfortunately, due to the delay, the email was not successfully recalled from all recipients.

WHAT WAS TARGETED?

This data breach appears to have been accidental by nature and not the result of a malicious organisation or a targeted cyber-attack. The breach was likely a result of insufficient cyber security awareness training, as well as genuine human error. Due to the demographic of the club members, the personal information leaked belonged to many high-profile individuals, including high-value business owners, barristers, and medical professionals. Though seemingly unintentional, the data breach has raised significant concerns for club members and their families.

WHAT WAS THE IMPACT?

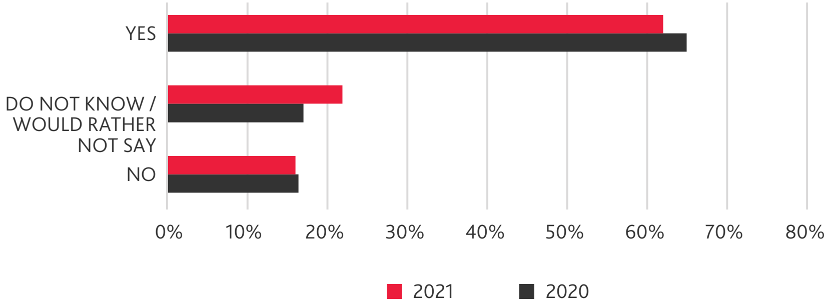
Shortly after the attempted email recall, the club's general manager publicly acknowledged the data breach, however made it clear in his statement that the incident was not required to be reported to OAIC. Despite this, the club's legal counsel had mentioned that this information could still potentially be uncovered by a 'determined searcher'. With members voicing concerns surrounding potential identity theft, as well as national media outlets quickly reporting the incident, the OAIC commented to a media platform that they would be contacting the club to further investigate the situation. This highlights that though it is important for organisations to take ownership of reporting data breaches, it needs to be done in close collaboration with the organisation's legal counsel, affected individuals and OAIC to avoid negative impacts to its reputation.

SEEKING CLARITY ON NOTIFIABLE DATA BREACHES

There was greater uncertainty in 2021 about whether organisations were required to report data breaches under the Notifiable Data Breaches (NDB) scheme.

However, for those organisations who knew they needed to comply, there was a continued increase in their confidence to meet NDB requirements.

UNDER THE NOTIFIABLE DATA BREACHES SCHEME, WOULD YOUR ORGANISATION BE REQUIRED TO MAKE A BREACH NOTIFICATION?

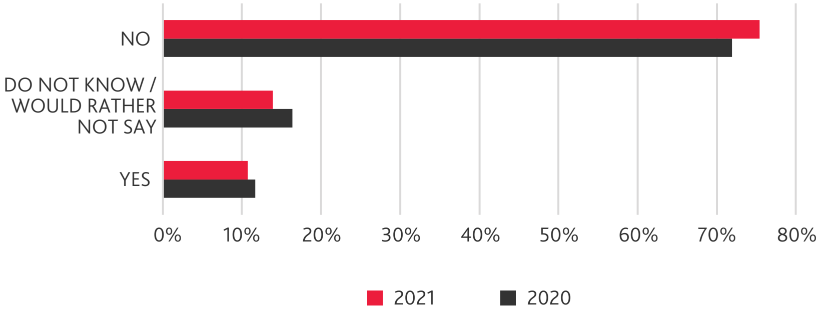


The breadth of information types impacted by data breaches appeared to reduce in 2021 compared to the previous year. 2021 saw decreased breaches of payment information, bank account information and tax file numbers.

However, protected and security classified information was highly targeted in 2021 and passport detail breaches increased. This could suggest data breaches are becoming more targeted, in alignment with trends indicating that ransomware attacks are becoming more laser focused.

While fewer organisations reported notifiable data breaches in 2021 compared to the prior year, there was a significant increase in organisations who were unsure whether they had to comply with the NDB scheme at all. This uncertainty could have contributed to less reporting.

HAS YOUR ORGANISATION MADE A BREACH NOTIFICATION UNDER THE NOTIFIABLE DATA BREACHES SCHEME?



CASE STUDY: RANSOMWARE ATTACK ON A FINANCIAL INSTITUTION PROVIDER

While many cyber attacks and data breaches were made public, many events happened in 2021 that did not make the press and they highlight how any organisation can be subjected to an attack.

WHAT HAPPENED?

In late 2020, an Australian based financial institution provider was hit by ransomware attackers. The attack compromised systems and infrastructure, taking the organisation completely offline. Luckily, the organisation could restore its systems with backups resulting in minimal data loss. Regardless, the time and cost taken to rebuild an entire infrastructure from scratch, and the operational downtime should not be overlooked.

WHAT WAS TARGETED?

It's not clear why the organisation was attacked, or whether it was part of a targeted operation or an opportunistic attacker. The attack utilised the DeepBlueMagic ransomware, which is known to disable an organisation's security tools. After the ransomware is deployed it encrypts all hard drives, except for the system drive. DeepBlueMagic uses tools to make the recovery of the drives impossible.

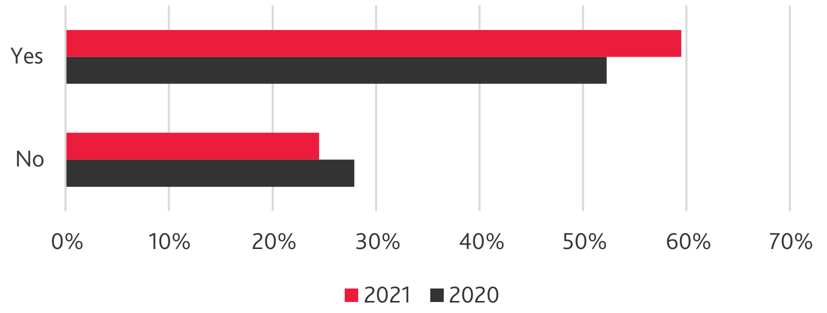
WHAT WAS THE IMPACT?

The organisation shut down and took its servers that contained personally identifiable information offline. However, the attackers managed to get their hands on employee records. The organisation did not want to pay the ransom and instead rebuilt its infrastructure from back-ups. This took more than five weeks with an estimated cost in the tens of millions of dollars. The organisation decided to take the prudent step of reporting the data breach of Personally Identifiable Information (PII) to the Office of the Australian Information Commissioner (OAIC).

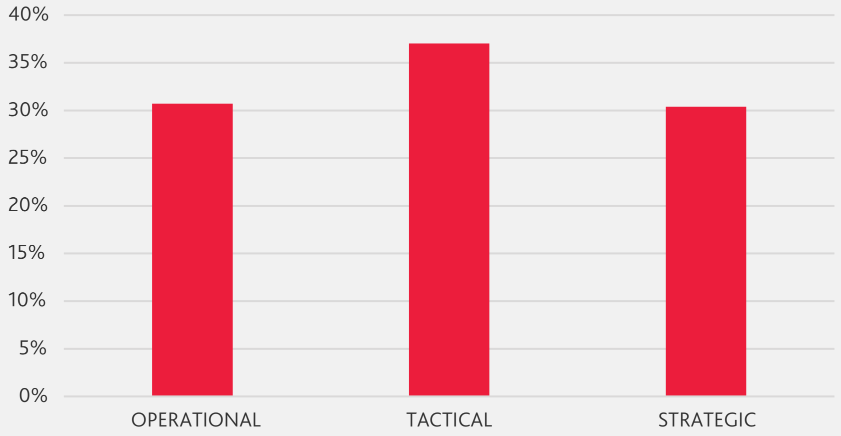
INCREASING CYBER THREAT INTELLIGENCE

With 60% of respondents receiving threat intelligence, those without are in the minority.

DOES YOUR ORGANISATION RECEIVE CYBER THREAT INTELLIGENCE?



TYPES OF INTELLIGENCE



UPTICK IN INTELLIGENCE

Threat intelligence is a crucial part in incident response and incident management. Fortunately, industry professionals understand this and for the fifth consecutive year, the number of organisations actively managing and receiving threat intelligence has increased. Through respondent data, we have identified an additional 15% of organisations actively managing their threat intelligence appetite, compared to 2020.

Focusing on the whole picture, we now see a total of 60% of organisations receiving some form of threat intelligence, placing organisations who don't manage cyber threat intelligence in the minority. The three key types of threat intelligence identified by respondents were operational intelligence, tactical intelligence, and strategic intelligence. The three types were quite evenly distributed in terms of respondent use, though tactical intelligence (human readable intelligence of a technical nature about specific adversaries, incidents and cyber attack campaigns) was marginally favoured as the strongest intel type, accounting for 37% of responses.

OPERATIONAL:

Includes atomic, granular intelligence data, such as Internet Protocol (IP) address and malicious website addresses.

TACTICAL:

Includes campaigns, threats or adversary specific reporting, such as on an emerging zero day, adversary activity and malware campaigns.

STRATEGIC:

Includes long-term insights and trends to inform strategic decision-making, such as human to human and Chief Information Security Officer (CISO) reports.

ESTABLISHING CYBER RESILIENCE

WHAT IS CYBER RESILIENCY?

Cyber resiliency involves accepting that cyber attacks happen and preparing for potential attacks to minimise the damage. Resiliency is about understanding what types of attacks may take place, what assets may be targeted, how quickly you can identify the attackers and how quickly you can remove them from your infrastructure. Resiliency brings together cyber security, business continuity and broader enterprise risk functions.

THE GROUNDWORK TO A CYBER RESILIENCE STRATEGY

2021 has again seen a focus on cyber resilience strategies with a steady increase year-on-year from respondents. To build cyber resiliency, it's important to lay a solid foundation with the correct tone from the top. Today, this requires cyber security leaders who do not operate in silos and think more broadly about organisational risks and alignment to business goals. This will also lead to greater buy-in and support from executives and board members, and less financial constraints.

Once the tone at the top has been established, organisations must start planning how to manage their cyber risk. This all starts with gaining a good understanding of:

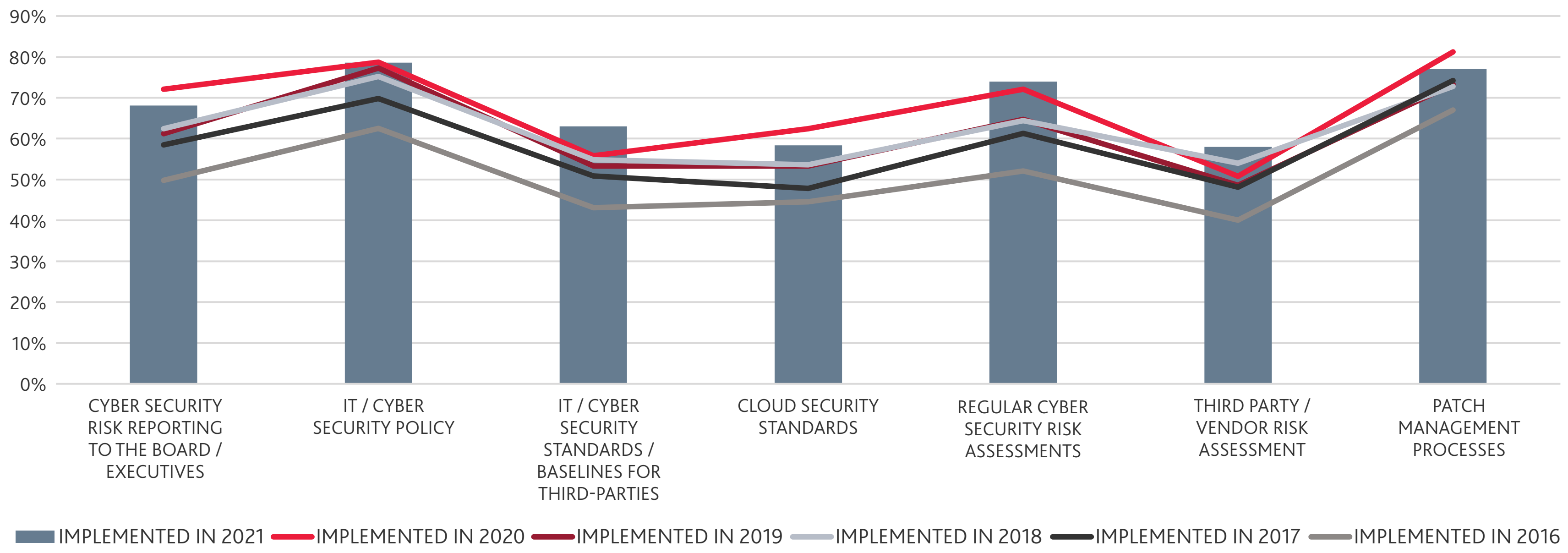
- The asset requiring protection
- Where the asset is located
- The threats to the asset
- The controls in place to protect the asset
- Whether the controls are tested.

Organisations can then start to build out the key requirements to support a cyber resiliency strategy.

Respondents are clearly invested in building this foundational understanding, highlighted by an increase in both governance and technical controls to build up their cyber resiliency.

With more and more organisations moving to cloud adoption, it's vital these strategies cover more than the traditional internal parameters. Organisations are reacting to the increasing risk of attacks on supply chains, by ensuring they have more oversight over third-parties.

RISK VISABILITY - ESTABLISHING A BASELINE



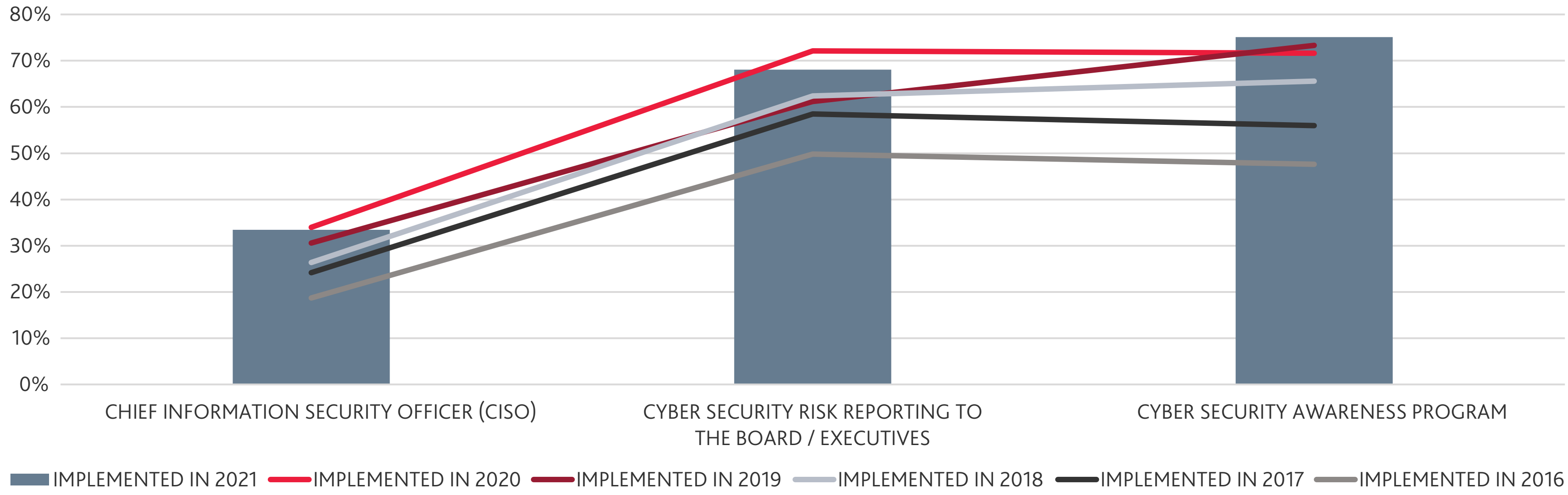
DEFINING AND IMPLEMENTING BASELINE STANDARDS

We have seen a steady increase in cyber security reporting to the board, which indicates top management is becoming more involved in cyber security. Setting minimum security standards fir third-party and cloud providers remains low. Although there is a higher reliance on third-party providers, regular risk assessments of third-parties is still remaining relatively low. It is important organisations define baseline security requirements and ensure that these are implemented throughout their supply chain.

ESTABLISHING CYBER RESILIENCE

CONTINUED

IMPLEMENTATION - A HOLISTIC VIEW TO CYBER AWARENESS



IMPROVED AWARENESS OF CYBER SECURITY

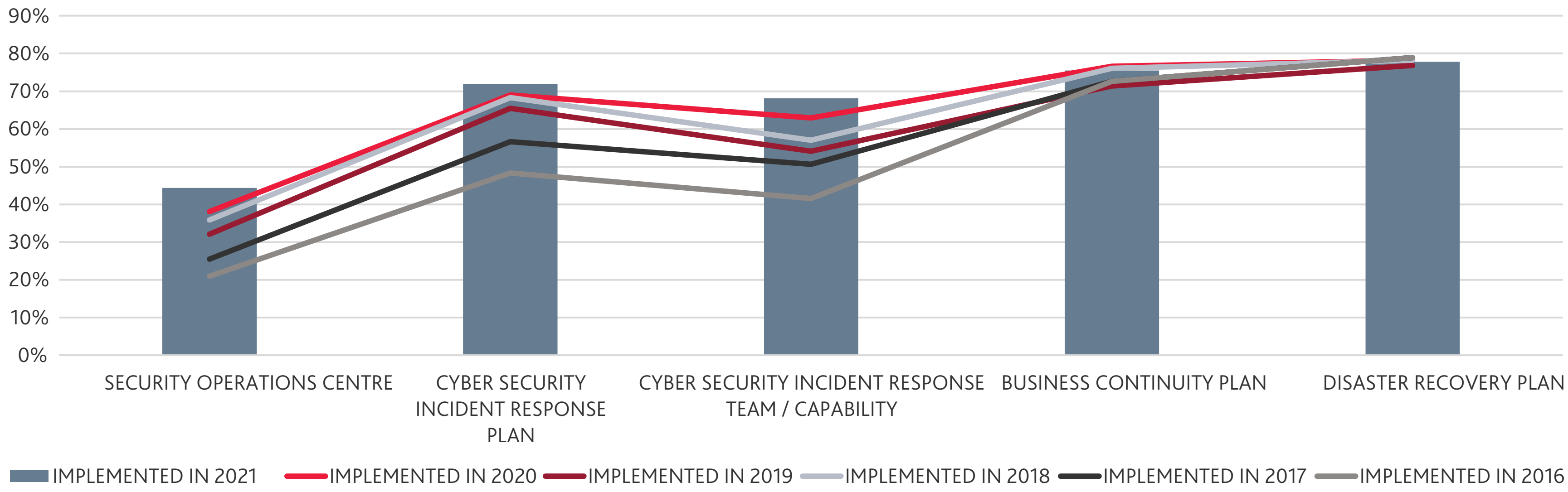
Cyber awareness training for employees was another strong area of focus for many respondents, with more than 75% of organisations reporting to have a cyber security training and awareness program in place.

This shows the importance of educating your workforce about the vastly changing and more convincing cyber attacks they may face. A cyber attack is an organisational risk (potentially a 'stop trade'), so staff must know what to look for.

ESTABLISHING CYBER RESILIENCE

CONTINUED

CAPABILITIES – IMPROVING RESPONSIVENESS



IMPLEMENTATION OF INCIDENT RESPONSE CAPABILITIES

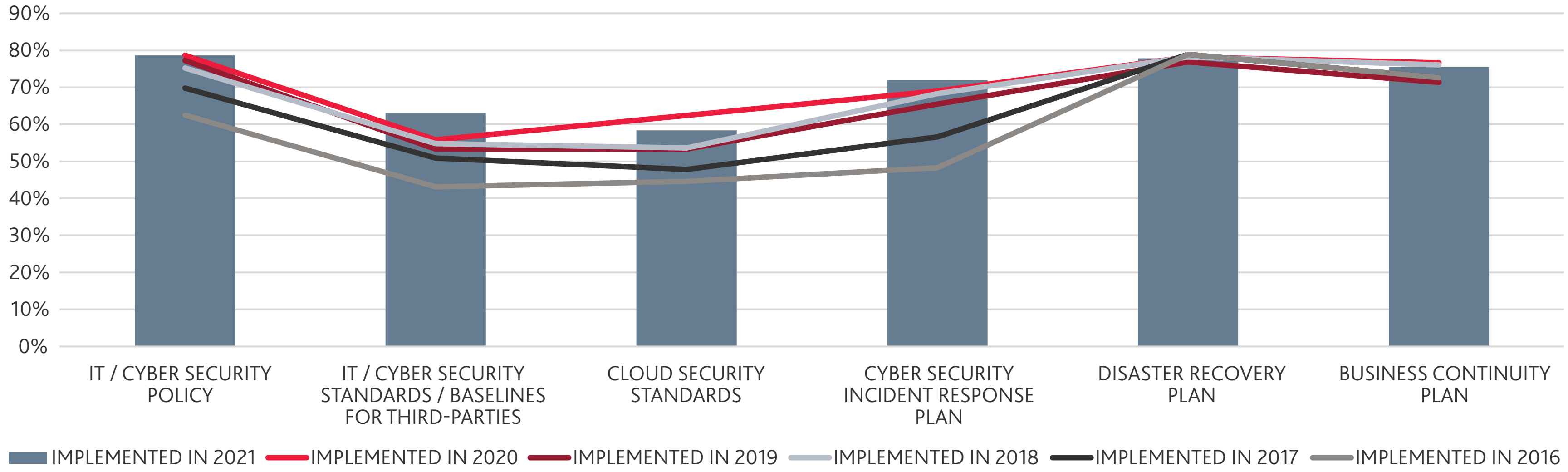
Another pillar of cyber resiliency, incident response, was in sharp focus during 2021. One area of particular interest was the increase in respondents who said they had implemented a Security Operations Centre, which was up 16% compared to 2020.

This rise compliments increases in cyber response capability (up 8%), cyber security incident response plans (up 4%) and investment in technology solutions, (up 11%), such as DLP and IDS.

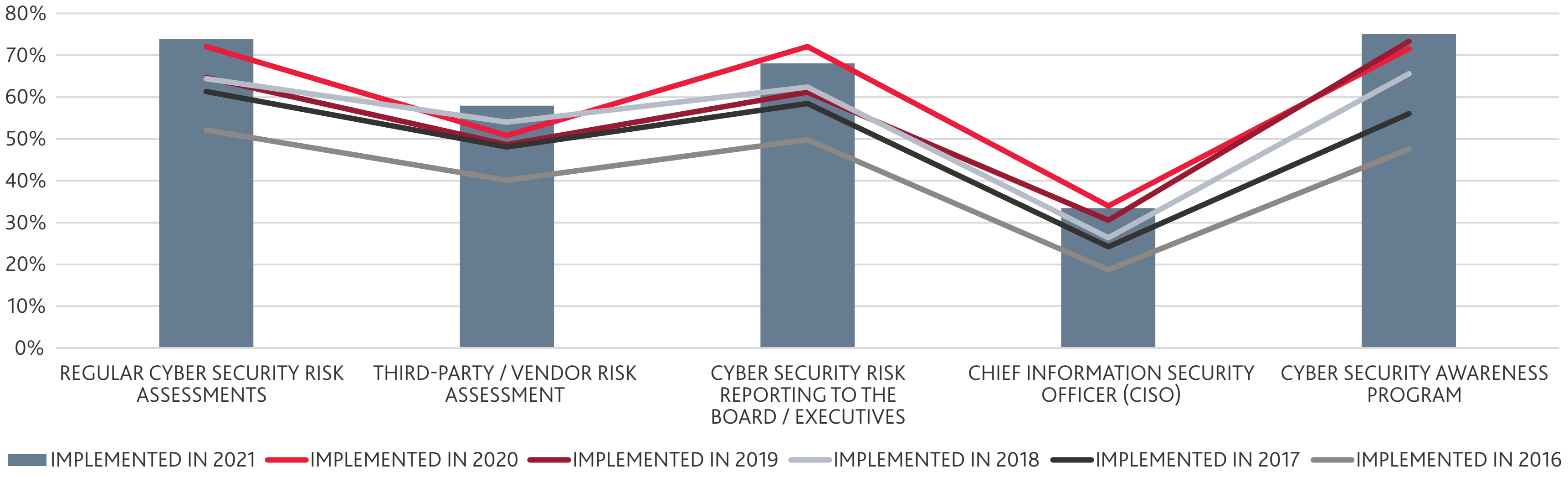
ESTABLISHING CYBER RESILIENCE

CONTINUED

GOVERNANCE - OPTIMISING PLANS AND PROCEDURES



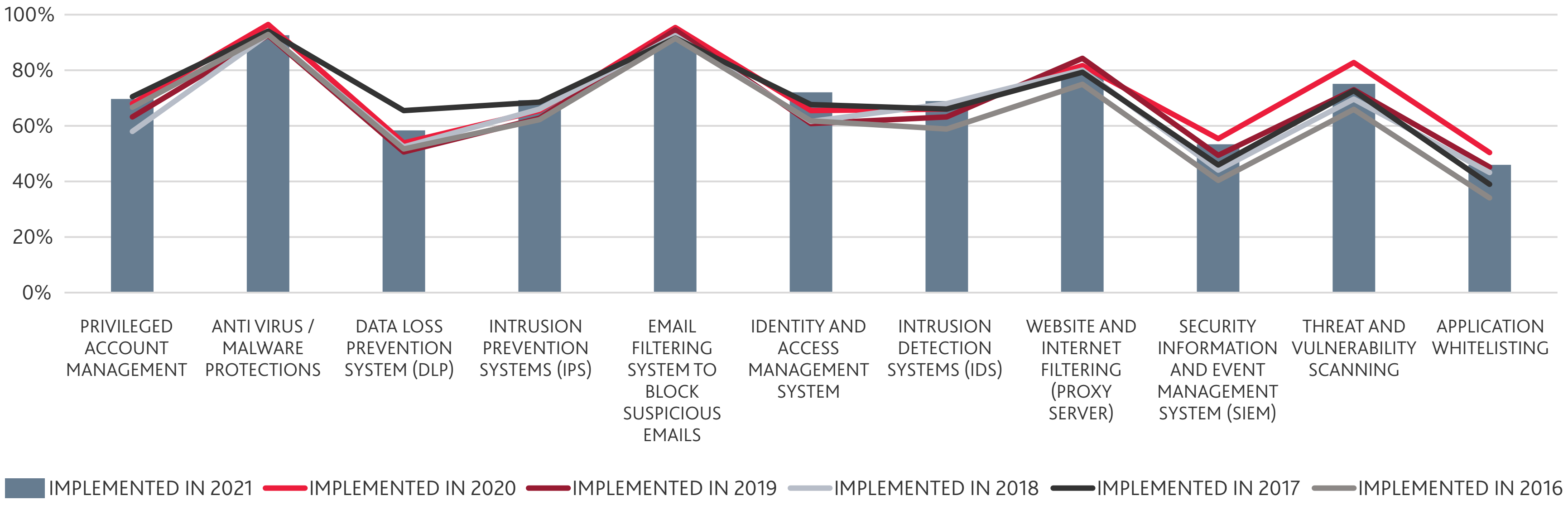
RISK VISABILITY - UNDERSTANDING THE THREAT ENVIRONMENT



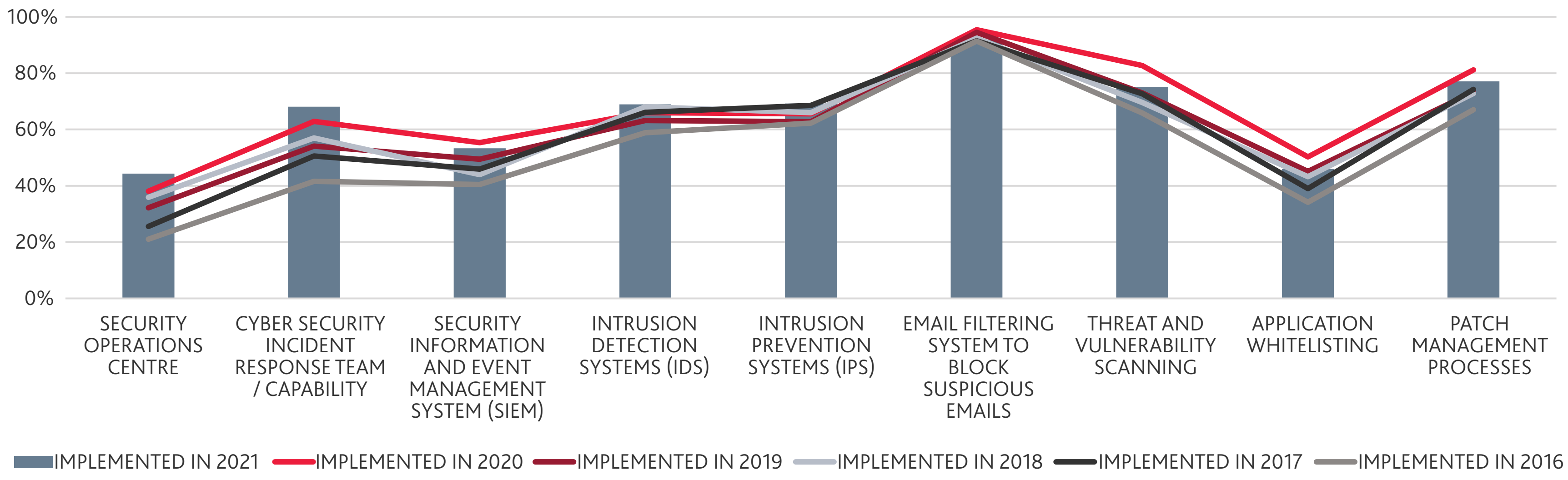
ESTABLISHING CYBER RESILIENCE

CONTINUED

CONTROLS - IMPLEMENTATION OF TECHNICAL CONTROLS



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 provide 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 2021, we conducted the sixth annual BDO and AusCERT Cyber Security Survey. We achieved strong participation in the survey, with almost 500 respondents across a variety of industry sectors. Of these respondents, 72% were based in Australia, 20% were based in New Zealand, and 8% were based internationally.

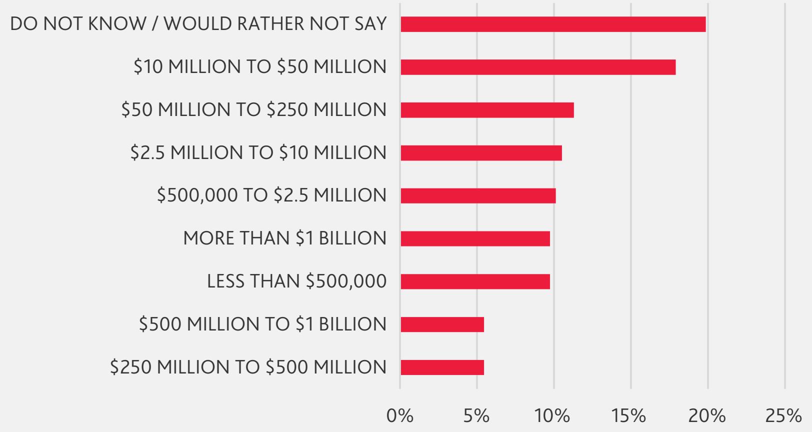
Our survey covered a wide variety of organisation types, across a range of industry categories. Most 2021 survey respondents were from three key industries:

- 48% were from the public sector
- 14% were from the private sector
- 17% were from the not-for-profit sector.

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

- 50% were C-level executives or Board Members
- 26% were Information Technology/Security Managers
- 8% were Security Analysts/Engineers
- 1% were Internal Auditors.

RESPONDENT ORGANISATIONS ANNUAL REVENUE



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 900 partners and staff in 15 offices across the North and South Islands, and BDO is the fastest-growing business services firm in the country.

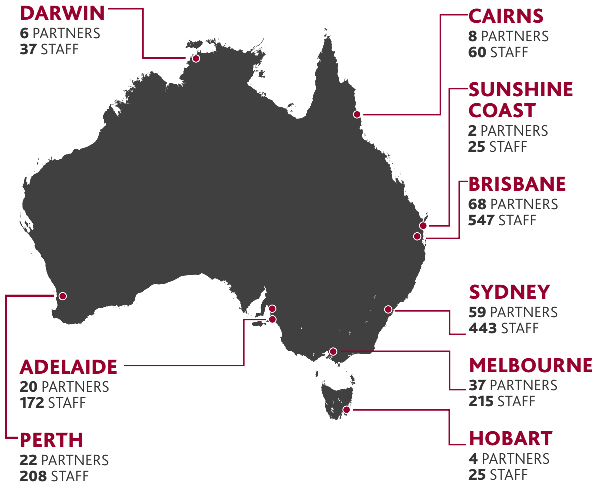
For more information about BDO services, visit www.bdo.com.au or www.bdo.co.nz.

1,958 PEOPLE

10 **OFFICES**

226 PARTNERS

FIGURES TAKEN AS AT 01 JANUARY 2022



900+ PEOPLE

15 **OFFICES**

100 PARTNERS

Growth

The fastest growing business services firm in New Zealand.

Backing smart NZ business

We support over 16,000 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
- Sensitive Information Alert
- Phishing Take-Down
- Early Warning SMS
- Security Bulletins
- Malicious URL Feed
- Security Incident Notifications
- 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.