

2019 ANNUAL REPORT

STATE OF CYBER SECURITY



PREPARED BY **MICHAEL CONNORY, CEO**



SECURITY IN DEPTH

1300 041 042

www.securityindepth.com.au

Level 2, 1 Southbank Blvd, Southbank, Melbourne 3006

Level 9, 50 Clarence St, Sydney 2000

Level 2, 37 Barrack St, Perth 6000

Level 9, 204 Alice St, Brisbane 4000

276 5th Av, New York, NY 10001

20-22 Wenlock Rd, London, N1 7GU

STATE OF CYBER SECURITY

TABLE OF CONTENTS

Executive Summary	4
Report Highlights	5
Cyber Security In 2019	7
Industry Results	8
Industries Reviewed	9
2019 Largest Australian Data Breaches	11
Which Industry Is Your Organisation In?	12
How Many People Does Your It Department Employ?	13
Does Your Organisation Have A Cyber Security Specialist On Staff?	14
CARR Australian Standards	15
CARR Identify	16
CARR Protect	17
CARR Detect	18
CARR Respond	19
CARR Recover	20
Cyber Costs	21
Loss Of Cyber Crime In Australia	22
Cost of a Data Breach in Australia	23
How Difficult Is It To Convince Management To Invest In Security?	24
What Part Of Your It Budget Was Spent On Cyber Security?	25
Can You Describe Year-To-Year Cyber-Security Spending?	26
Cyber Governance	27
Strategic Vs Tactical Cyber Security	28
Does Your Organisation Adhere To It Security Frameworks?	29
Which Procedures Has Your Organisation Approved?	30
Who Do Your Cyber-Security Executives Report To?	31
Cyber Risk	32
How Secure Do You Believe Your Network Is?	33
How Would You Describe Your Cyber-Security Maturity?	34
What Do You Think Will Help Improve Your Security Levels?	35
What Do You Consider To Be Your Greatest Security Risk?	36
Which Security Measures Have Been Implemented?	37
Has Penetration Testing Been Performed In Your Organisation?	38
Cyber Awareness	39
Does Your Organisation Provide Cyber-Security Awareness Training?	40
Trusting Third Parties With Your Data	41
How Confident Are You In The Cyber-Security Of Your Third Parties?	42
How Do You Ensure Cyber-Security With Third Parties?	43
Our Methodology	44



STATE OF CYBER SECURITY

EXECUTIVE SUMMARY

We are not surprised by the statistical information produced in the inaugural "State of Cyber Security" in Australia report. Reported data breaches have increased by more than 700%, while the cost of a data breach in Australia is estimated to be \$2.5 million, new legislation has been introduced and adopted such as the Notifiable Data Breaches act 2017 and CPS 234, but sadly, very little has changed.

Security in Depth has completed Australia's largest and most extensive cyber report in the belief that by understanding the current threats and challenges organisations face, it will enable them to manage cyber risk more effectively. By providing an overview of cyber in Australia, and an in depth understanding of where current cyber risks lie and the gaps most organisations either fail to recognise or view with minimal importance, organisations will have the ability to self-review and create strategies that will help reduce the possibility of a significant cyber incident impacting them.

During the past year, Security in Depth reviewed 903 data breaches, where 1894 Australian companies responded to our survey, State of Cyber Security in Australia, with over 922 qualitative discussions occurring with C-Level executives providing what we believe to be the most accurate and in depth understanding of Australian organisational cyber maturity.

What we have discovered is a slight shift in cybersecurity maturity across Australia.

Without doubt the biggest challenge Australian organisations face is directly linked to staff. Over the past year we have seen 70.1% of Australian data breaches caused directly through human error. This isn't any surprise when we observe that over 55% of Australian organisations do not have any Cyber Governance platform in place, 63% of Australian organisations have no dedicated department for Cyber Security and 38% of companies have not conducted any formal Cyber awareness training.

What comes through strongly is that Australian organisations still are highly likely to be impacted by a motivated threat actor, although we believe this could easily be reduced by a number of simple steps. Improved training, better co-ordination and communication between the IT department and the rest of the organisations and finally further input from the board to improve Cyber governance.

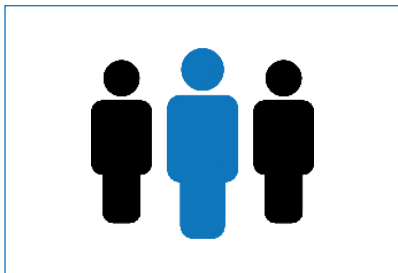


MICHAEL CONNORY, CEO
SECURITY IN DEPTH

STATE OF CYBER SECURITY

REPORT HIGHLIGHTS

Still the biggest issue facing Australian companies in 2019 is the disconnect between the board, the IT department and the organisation staff. More often than not, Cyber security is the sole responsibility of a few key individuals within the organisation, where it should be an organisational wide responsibility. This disconnect is the prime reason data breaches eventuate and that Cyber Security costs are high in Australia.



70%

of data breaches are caused by human error



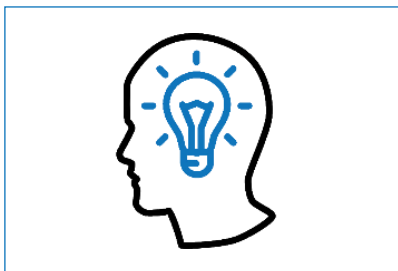
55%

of organisations in Australia have no cyber security governance



84%

of organisations in Australia blindly trust third parties with their data with no review of Cyber maturity or security practices



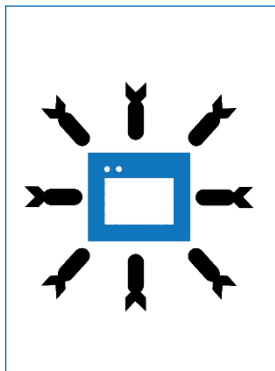
38%

of organisations in Australia have never provided cyber security training to their staff

AUSTRALIAN STATISTICS

CYBER SECURITY IN 2019

We say that 67% of Australian organisations will be impacted by a Cyber Incident. We believe the number is significantly greater – in fact almost 92%, but we have reviewed how a Cyber Incident impacts an organisation and unless both financial loss and or significant downtime eventuated the numbers have not contributed to the statistic.



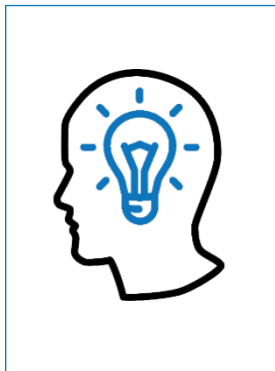
67%

of all Australian organisations will be impacted by a cyber incident in 2019



90%

of all data breaches in Australia begin with an email



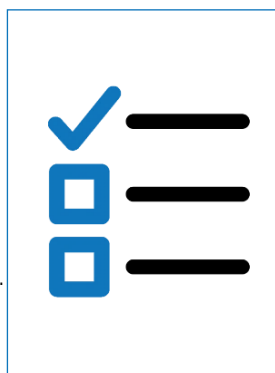
38%

of Australian businesses do not provide any cyber awareness training to staff



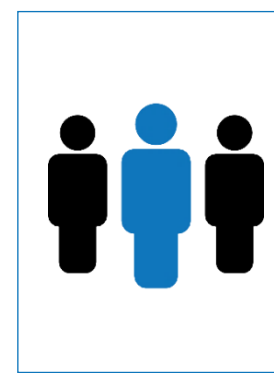
55%

of Australian organisations have no Cyber Governance framework in place



17%

of organisations have a tested incident response plan



71%

of all data breaches are a direct result of human error

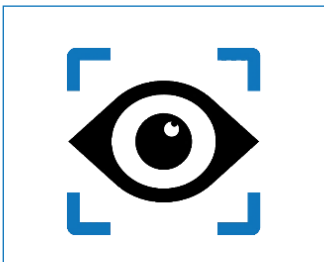
AUSTRALIAN STATISTICS

CYBER SECURITY IN 2019

It has been reported by CrowdStrike that once an attacker once has compromised the credentials of a company, it can take as little as 20 minutes to begin to accessing the network and moving laterally through the network. This is known as 'breakout time'. This information is crucial for organisations to understand, as it is an indicator of how quickly a data breach leads to a compromise of an entire network. In Australia today, we see 'breakout time' and 9.55 days significantly greater than the 20 minutes suggested. The greatest concern Australian organisations have is not the 'breakout time', but the time it takes for an organisation to actually detect a data breach and begin to act.



A Cyber Criminal takes **< 10 days** to use stolen credentials



A breach is detected **~ 90 days** after the initial hack



It then takes an extra **28.25 days** to notify the individual

**A HACKER HAS YOUR INFORMATION FOR
188 DAYS BEFORE YOU EVEN KNOW.**

INDUSTRY RESULTS

Security in Depth's focus this year was to conduct the largest, most comprehensive cyber research project undertaken in Australia. To do that we reached out and discussed current cyber maturity with 1,894 organisations. These organisations range from 20 staff through to organisations that have over 50,000 people employed. The focus being to truly understand how mature Australian organisations are when it comes to one of the greatest challenges and risks in today's business environment – cyber.

OVERVIEW

INDUSTRIES REVIEWED

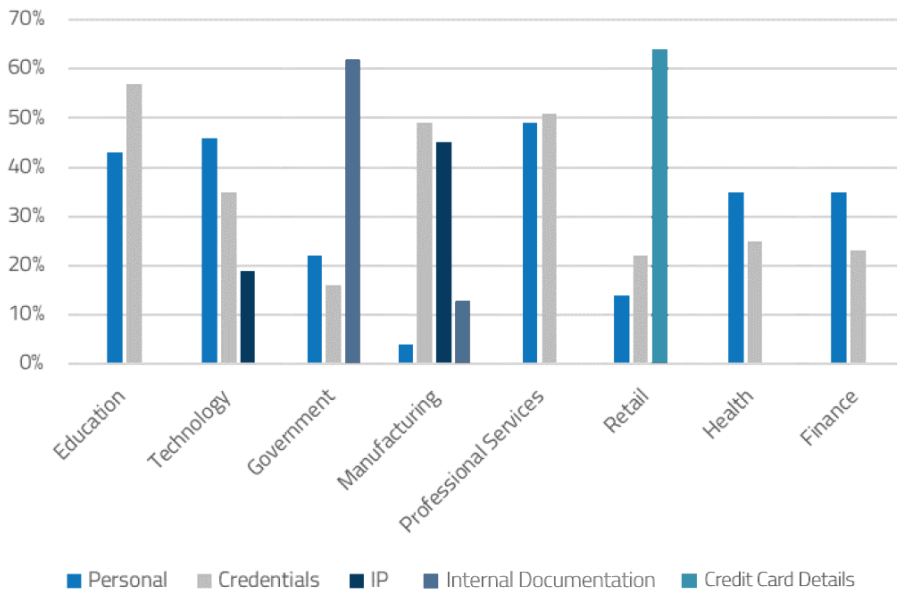
Security In Depth had 1,894 responses from 14 major industries. With all Australian Finance organisations (this incorporates all organisations that fall under APRA as well as accounting firms) contributing to 27% of all respondents, Technology organisations 17%, Health organisations 16%.

What has been fascinating is the breakdown of data breaches within Australia across these organisations with almost 24% of all Australian data breaches attributed to health

organisations, and 20% of data breaches attributed to finance organisations across Australia.

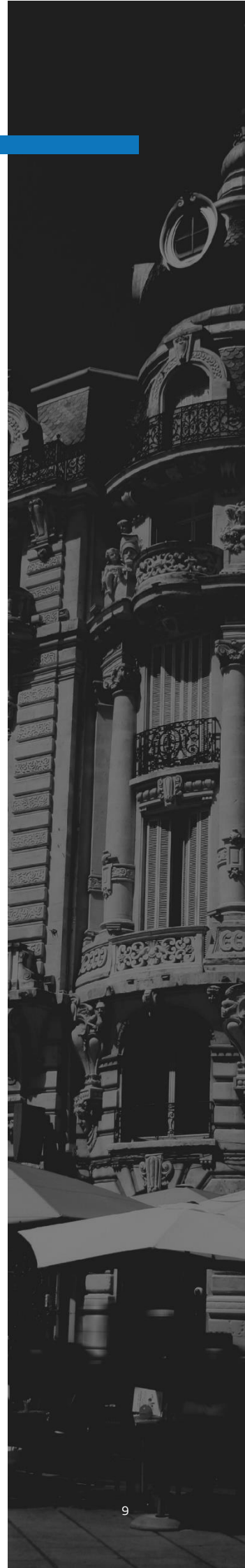
During the past 12 months, Security in Depth has reviewed 4,067 cyber Incidents in Australia* not all cyber incidents fall under mandatory notifiable data breach legislation. These incidents came from various sector: Finance (899), Health (445), Education (331), Technology (878), Government (330), Manufacturing (342), Professional (644), and Retail (188).

We can reveal the following about the types of information stolen between industry sectors:



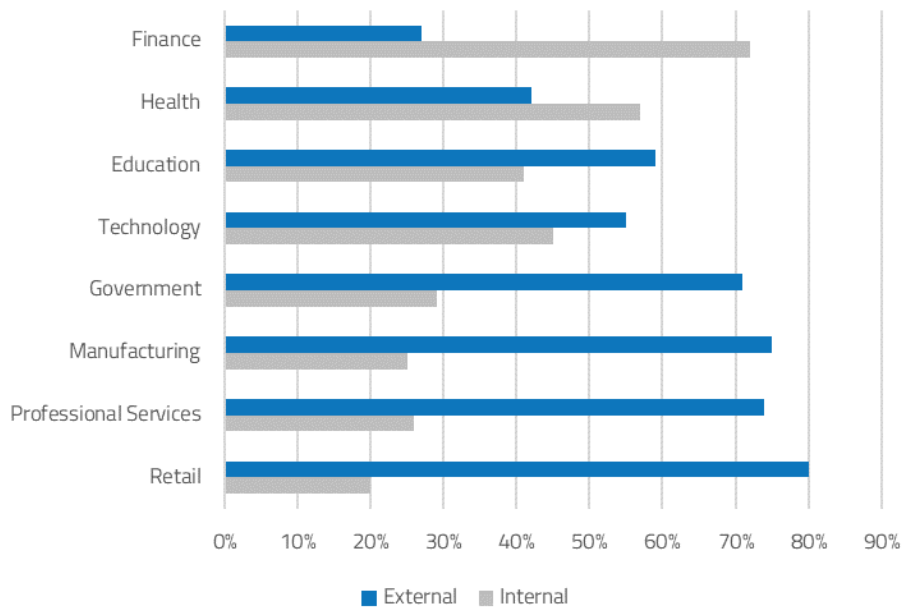
Personal information includes bank account details, Tax File Numbers, and identification documentation. Credentials are the username and passwords individuals use.

** This information has been compiled accessing information from the following sources. Notifiable Data Breaches quarterly statistics reports, June 2018, Sept 2018, Jan 2019, April 2019, Verizon Enterprise Data Breach Report 2019, Webinsurance List of Data Breaches in Australia 2018 and 2019, Ponemon Institute Cost of Data Breaches 2018/2019, Accenture Cost of Data Breach 2019, and Security in Depth State of Cyber Security Research 2019*

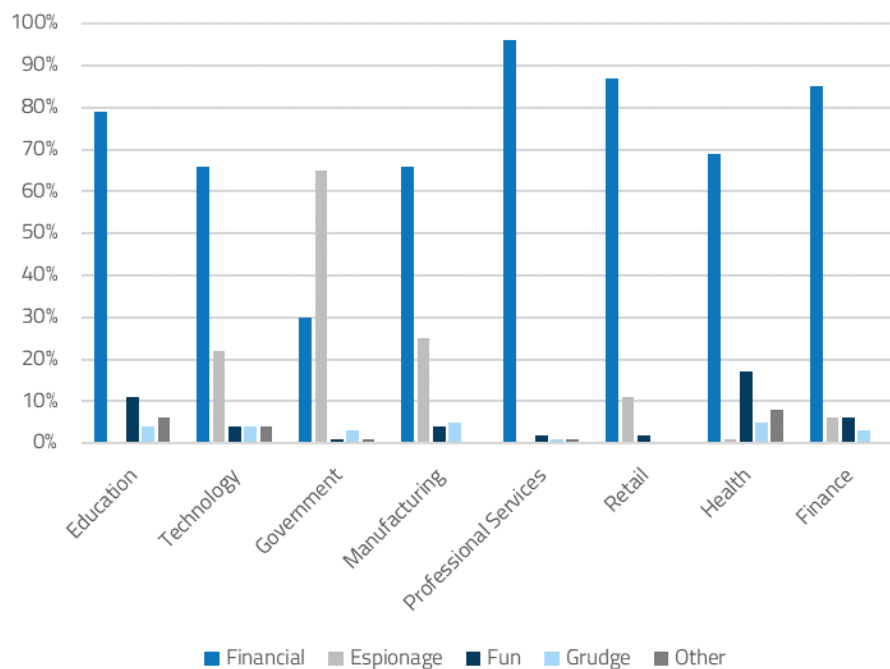


CONTINUED INDUSTRIES REVIEWED











We can reveal the following about the source of the cyber attacks between industry sectors:



We can reveal the following about the motive of the cyber attacks between industry sectors:



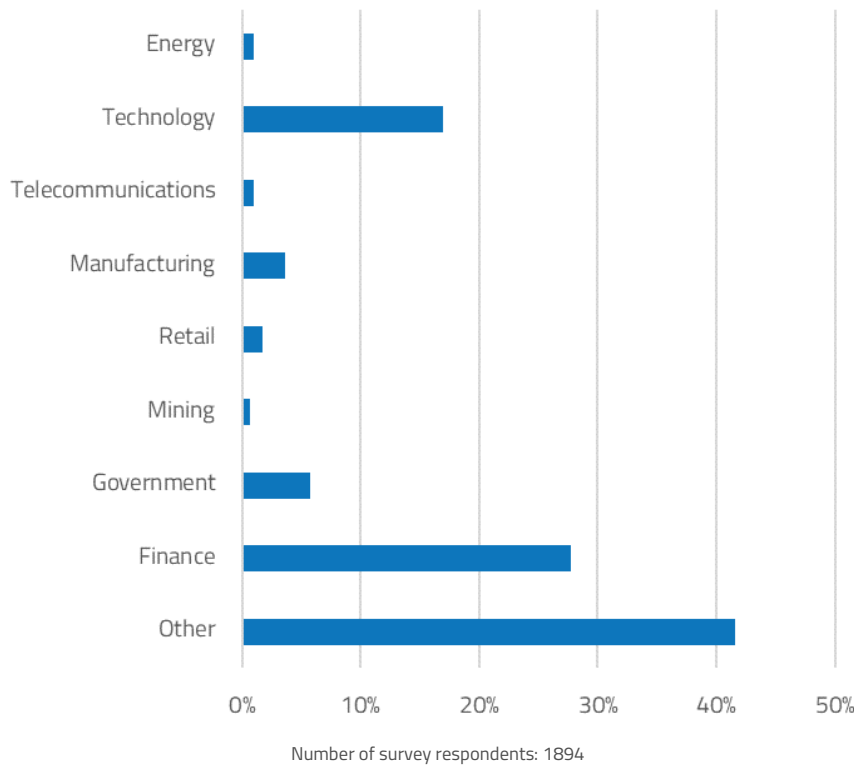
2019 LARGEST AUSTRALIAN DATA BREACHES

26/07/19		11/03/19	
17/06/19		21/02/19	
14/06/19		15/02/19	
07/06/19		21/02/19	
01/06/19	PRINCESS POLLY	12/02/19	
27/05/19		13/02/19	
28/05/19		06/02/19	
10/05/19		31/01/19	facebook
14/05/19		29/01/19	
14/05/19		28/01/19	
11/04/19		11/01/19	
16/04/19		08/01/19	
27/03/19		07/01/19	
26/03/19		02/01/19	
11/03/19		05/01/19	
13/03/19		07/01/19	
15/02/19		01/01/19	



INDUSTRY RESULTS

WHICH INDUSTRY IS YOUR ORGANISATION IN?



Security In Depth had 1894 different organisations respond to its 2019 survey. The vast majority identifying as ‘other’ when categorising into business type. Many of these organisations identified across different industry segments and represented classic organisations like health, legal, property and consulting organisations as well as organisations that had different business requirements. Some examples include:

- Health organisations that provided only technological services
- Human relations organisations that provided both technological and legal support

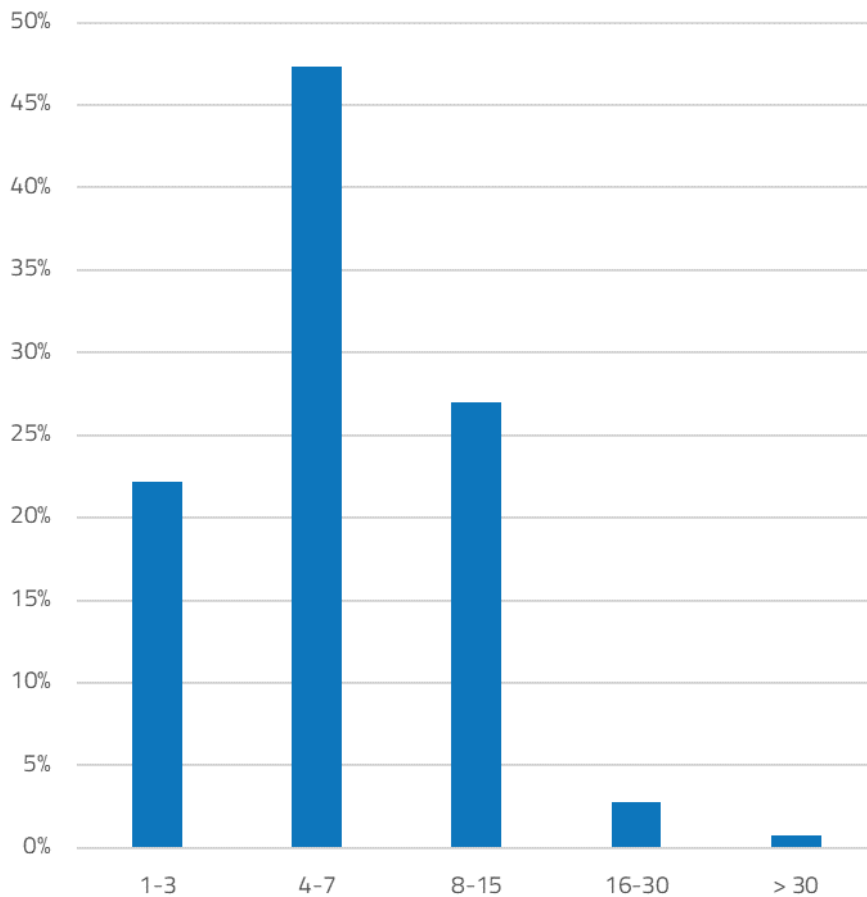
This year Security In Depth had a significant increase in organisations that identified as providing financial services both as a B2B and B2C function. These included organisations providing the following services: Accounting, insurance, financial advice and management, superannuation, and banking services.

It is Security In Depth’ belief this group provides us with the most detailed study of Australian organisations and cybersecurity undertaken so far.



INDUSTRY RESULTS

HOW MANY PEOPLE DOES YOUR IT DEPARTMENT EMPLOY?



Number of survey respondents: 1894

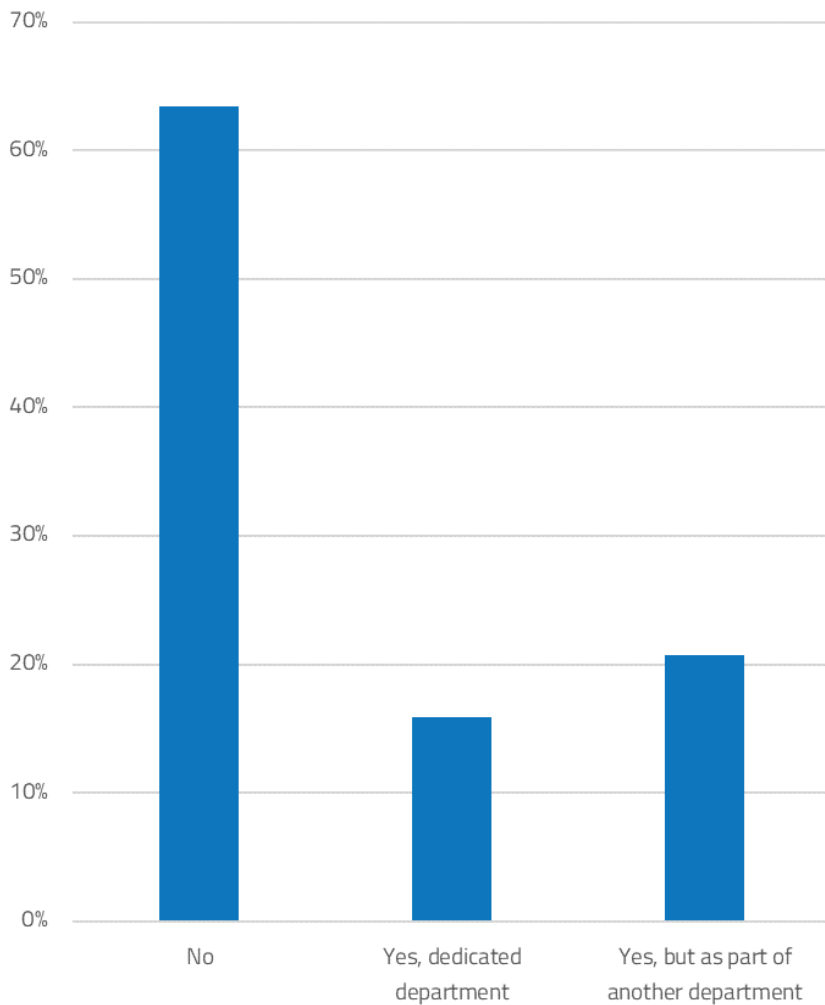
The substantial difference with the 2019 figures compared to the 2018 figures, is due to the substantial increase in organisations interviewed. Over the past year, our focus has been to increase our understanding of organisations from as little at 25 staff members all the way through to organisations that have over 100,000 employees.

After interviewing 1,894 organisations across Australia, Security In Depth believes the information relating to IT staff numbers within organisations is a strong representation of IT within Australian business today. With almost 70% of companies who have between 1-6 IT staff employed - correlating directly to the number of organisations that do not have any cybersecurity staff employed.



CYBER GOVERNANCE

DOES YOUR ORGANISATION HAVE A CYBER SECURITY SPECIALIST ON STAFF?



Number of survey respondents: 1894

It has become evident that over the past twelve months, many organisations have elected to have a dedicated department focusing on cybersecurity. The increase in organisations now having dedicated IT Security staff within existing departments has

increased almost 47%, whilst the increase for organisations starting a separate department focusing solely on cyber security has grown exponentially over the past twelve months alone – a staggering of 1400% increase.



CYBER ASSURANCE RISK RATING CARR AUSTRALIAN STANDARDS

The Cyber Assurance Risk Rating (CARR) is the defacto Australian standard in assessing business risk, when reviewing business relationships with third party suppliers.

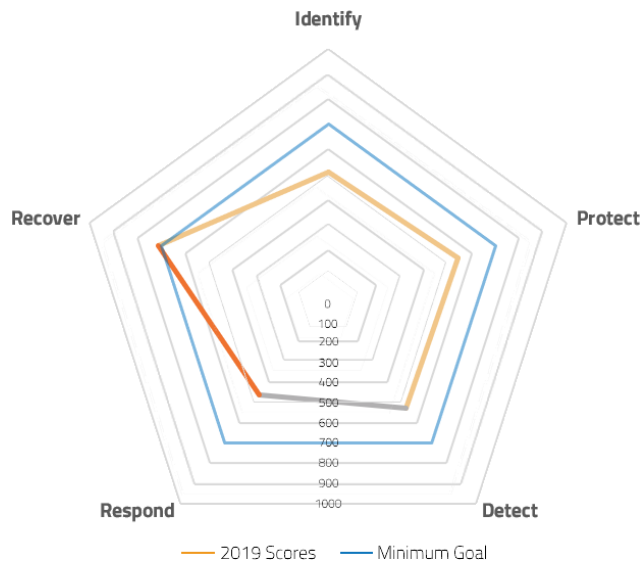
CARR provides a global, regional and local view of an organisation's cybersecurity risk profile and the likelihood of a data breach via third party suppliers.

WHAT IS RATED?



- IDENTIFY** The data, personnel, devices, systems, and facilities for the organisation's business purposes are identified and managed.
- PROTECT** Policies, procedures, and processes to manage and monitor the regulatory, risk, legal, and environmental requirements.
- DETECT** Detection processes and procedures are maintained and tested to ensure timely and adequate awareness.
- RESPOND** Response processes are validated and maintained to ensure timely response to detected cybersecurity events.
- RECOVER** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems affected.

WHAT DOES IT LOOK LIKE?



KEY

EXCEPTIONAL 800 – 1000	VERY GOOD 700 – 799	GOOD 600 – 699	FAIR 500 – 599	POOR < 500
Highly unlikely to experience a cyber incident in 12 months	Unlikely to experience a cyber incident in 12 months	Medium risk of experiencing a cyber incident in 12 months	Potential risk of experiencing a cyber incident in 12 months	High level risk of experiencing a cyber incident in 12 months

CYBER ASSURANCE RISK RATING **CARR**

IDENTIFY



Organizations must develop an understanding of their environment to manage cybersecurity risk to systems, assets, data, and their capabilities. To comply, it is essential to have full visibility of your digital and physical assets and their interconnections, defined roles and responsibilities, as well as understanding your current risks and exposure and put policies and procedures in place to manage those risks. This covers cyber governance and how it is managed.

The scores provided identify industry averages for cyber maturity, primarily across cyber governance. We can see that certain business types have greater capabilities than others

energy and telecommunications having the best scores and areas such as health, retail and manufacturing having low maturity levels. The primary reason for these scores is the inability of boards within these industries to classify cyber risk as a major concern. We would like to highlight the finance sector, whilst the major banks, superannuation companies and insurance organisations have significant governance platforms in place, this is not reflected by smaller financial organisations which struggle to both understand and implement any form of cyber governance across the organisation. We will be interested in how new Australian legislation CPS-234 impacts this number in 2020.



KEY

EXCEPTIONAL 800 – 1000	VERY GOOD 700 – 799	GOOD 600 – 699	FAIR 500 – 599	POOR < 500
Highly unlikely to experience cyber incident in 12 months	Unlikely to experience a cyber incident in 12 months	Medium risk of experiencing a cyber incident in 12 months	Potential risk of experiencing a cyber incident in 12 months	High level risk of experiencing a cyber incident in 12 months

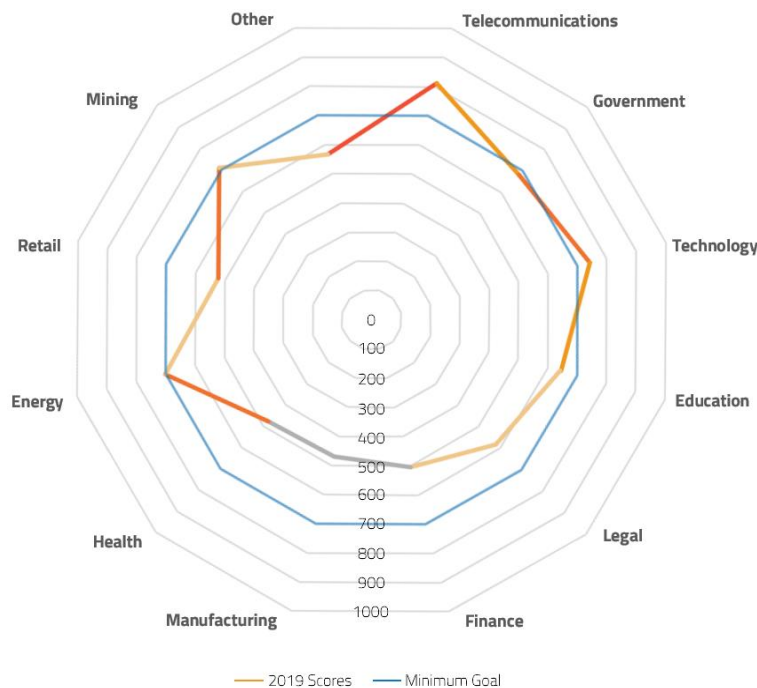
CYBER ASSURANCE RISK RATING [CARR](#)

PROTECT



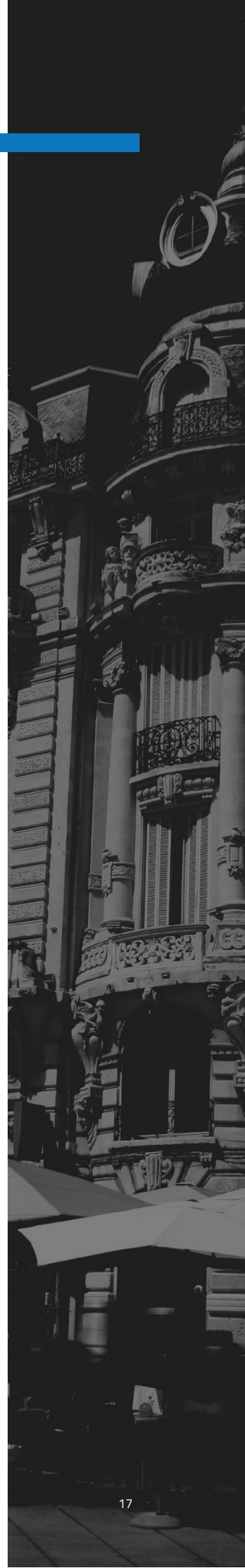
Organisations must develop and implement appropriate safeguards to limit or contain the impact of a potential cybersecurity event. To obtain a high score, organisations must demonstrate a focus on cybersecurity that reduces the likelihood of a cyber incident, this incorporates: control access to digital and physical assets, provide awareness education and training, put processes into place to secure data, maintain baselines of network configuration and operations to repair system components in a timely manner and deploy protective technology to ensure cyber resilience.

Being able to protect an organisation in the event of a cyber incident should be standard for all organisations across Australia today. Unfortunately, the Cyber Assurance Risk numbers are far from convincing. We have seen outliers within industry results – again these come from organisations that could be classified as critical infrastructure within Australia as well as highly developed technology and mature government organisations. The vast majority however, especially across health, manufacturing, retail and small business do not have the capabilities of either protecting an organisation from a cyber event or containing such an event.



KEY

EXCEPTIONAL 800 – 1000	VERY GOOD 700 – 799	GOOD 600 – 699	FAIR 500 – 599	POOR < 500
Highly unlikely to experience cyber incident in 12 months	Unlikely to experience a cyber incident in 12 months	Medium risk of experiencing a cyber incident in 12 months	Potential risk of experiencing a cyber incident in 12 months	High level risk of experiencing a cyber incident in 12 months



CYBER ASSURANCE RISK RATING [CARR](#)

DETECT

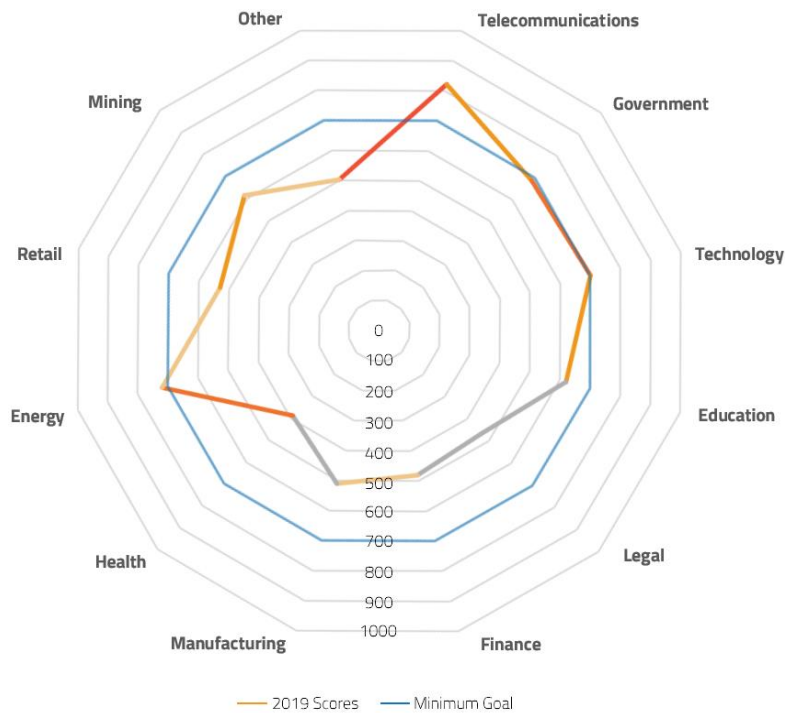


Organisations must implement the appropriate measures to quickly identify cybersecurity events. The adoption of continuous monitoring solutions that detect anomalous activity and other threats to operational continuity is required to improve an organisation's score within this function. To achieve this, we review your organizational visibility into its networks to anticipate a cyber incident as well as having information at hand to respond to one.

Organisations across Australia have a significant challenge when detecting cybersecurity events. From simple cyber

events such as phishing activities not being reported through to individuals consistently having user credentials compromised through continuous cyber events (both internal and third party) more often than not, organisation simply have no idea that an event has taken place until well after initial incident occurred. The issue we see here eventuates from both poor governance programs being in place as well as staff not capable of understanding what to look for if an event was to occur and effective technology in place to help identify events in real time.

Australian organisations across the board have major issues with detection.



KEY

EXCEPTIONAL 800 – 1000	VERY GOOD 700 – 799	GOOD 600 – 699	FAIR 500 – 599	POOR < 500
Highly unlikely to experience a cyber incident in 12 months	Unlikely to experience a cyber incident in 12 months	Medium risk of experiencing a cyber incident in 12 months	Potential risk of experiencing a cyber incident in 12 months	High level risk of experiencing a cyber incident in 12 months



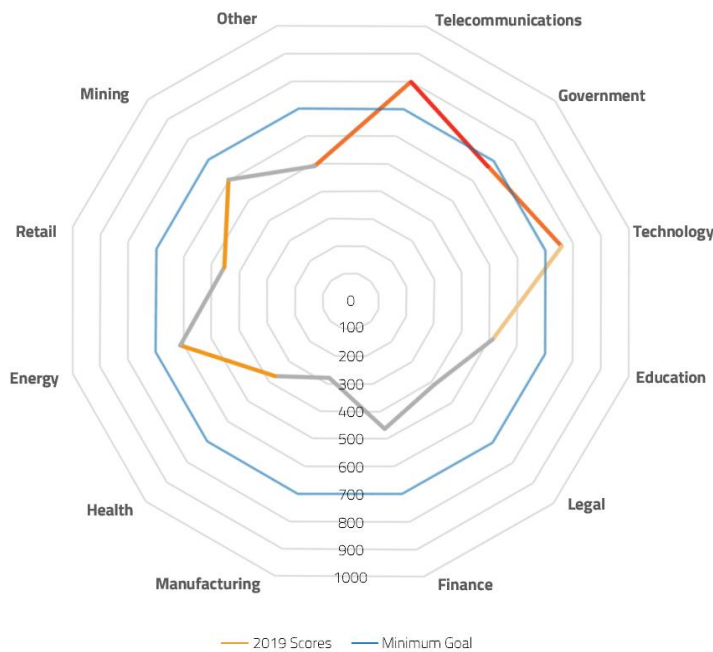
CYBER ASSURANCE RISK RATING CARR RESPOND



Should a cyber incident occur, organisations must have the ability to contain the impact. Security In Depth’s review is to understand how organizations have crafted a response plan, as well as defined communication lines among the appropriate parties, collect and analyse information about the event, perform all required activities to eradicate the incident and incorporate lessons learned into revised response strategies.

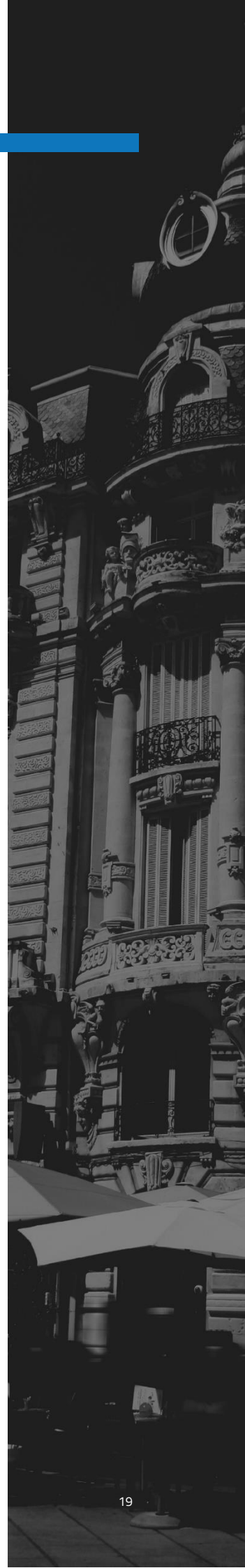
During the past 18 months, Security in Depth, has witnessed the ability of organisations to respond to a cyber event as critical. Most people today see having a cyber event as when it might happen rather than if one ever will.

With that in mind, an organisation’s ability to respond effectively is critical. Responding effectively can protect and limit the impact a cyber incident may have on organisations, with Cisco (2018) reporting up to 62% of small and medium sized businesses will close within six months of a major cyber event occurring. With that in mind, the Australian Government has implemented two significant pieces of legislation around mandatory data breach notifications as well as CPS-234. The Office of the Australian Information Commissioner (OAIC), has established a dedicated website to assist organisations develop an incident response plan to deal with major data breaches. And yet, most organisations across Australia, continue to remain vastly underprepared.



KEY

EXCEPTIONAL 800 – 1000	VERY GOOD 700 – 799	GOOD 600 – 699	FAIR 500 – 599	POOR < 500
Highly unlikely to experience a cyber incident in 12 months	Unlikely to experience a cyber incident in 12 months	Medium risk of experiencing a cyber incident in 12 months	Potential risk of experiencing a cyber incident in 12 months	High level risk of experiencing a cyber incident in 12 months



CYBER ASSURANCE RISK RATING [CARR](#)

RECOVER



Organisations must develop and implement effective activities to restore any capabilities or services that were impaired due to a cybersecurity event. Our review assesses an organizations ability to have a recovery plan in place, be able to coordinate restoration activities with external parties and incorporate lessons learned into an updated recovery strategy. Our focus also reviews how well an organisation has defined a prioritised list of action used to undertake recovery activity critical to a timely recovery.

It has been of no surprise the scores across the recover section for Australian business is higher than everything else. There has been almost two decades of communication on the importance of backing up data and disaster recovery capabilities. This is now easier than ever for organisations, as many move to cloud based solutions with the investment moving from managing on premises data to cloud based – with a significant investment made by software vendors to keep and protect and restore critical business functions in case of disaster.



KEY

EXCEPTIONAL 800 – 1000	VERY GOOD 700 – 799	GOOD 600 – 699	FAIR 500 – 599	POOR < 500
Highly unlikely to experience a cyber incident in 12 months	Unlikely to experience a cyber incident in 12 months	Medium risk of experiencing a cyber incident in 12 months	Potential risk of experiencing a cyber incident in 12 months	High level risk of experiencing a cyber incident in 12 months



2019 ANNUAL REPORT

CYBER COSTS

Australia is an attractive target for serious and organised crime syndicates due to our nation's relative wealth and high use of technology such as social media, online banking and government services. Due to the possible lucrative financial gains for serious and organised crime syndicates, the cybercrime threat is persistent.

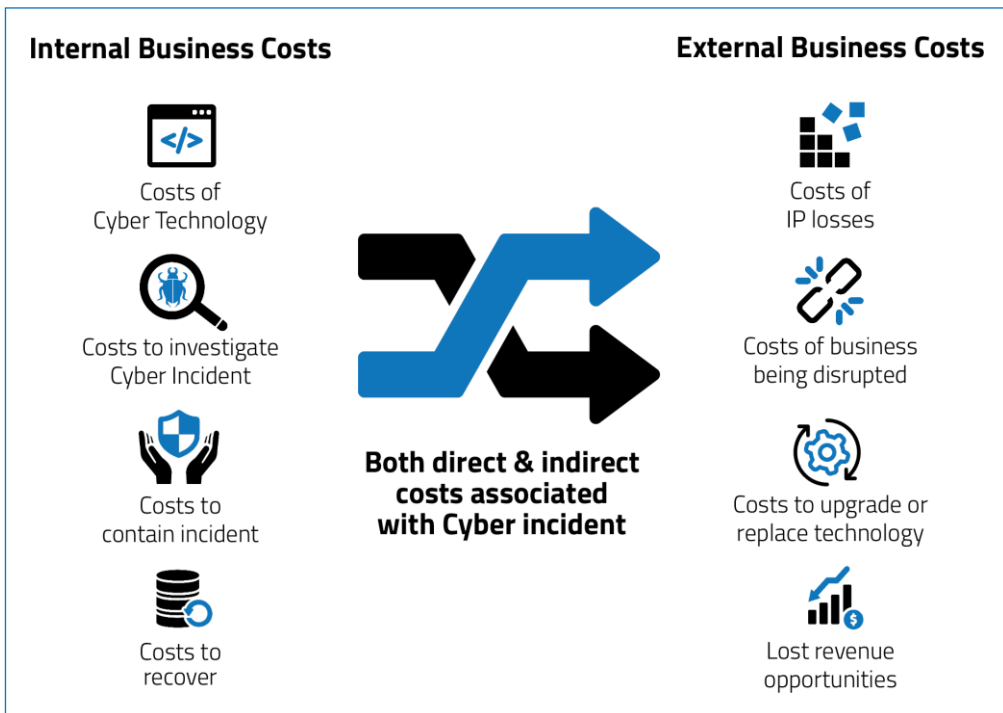


SECURITY IN DEPTH

CYBER COSTS

LOSS OF CYBER CRIME IN AUSTRALIA

The cost of cybercrime in Australia has increased dramatically with costs in 2017 estimated to be from \$276,000 in 2016¹ and has year on year increased by an estimated \$397,000 in 2019².



The increasing costs cybercrime can be accounted for by the shortfalls in almost all major areas of cyber resilience. Security In Depth, simply refers back to the industry

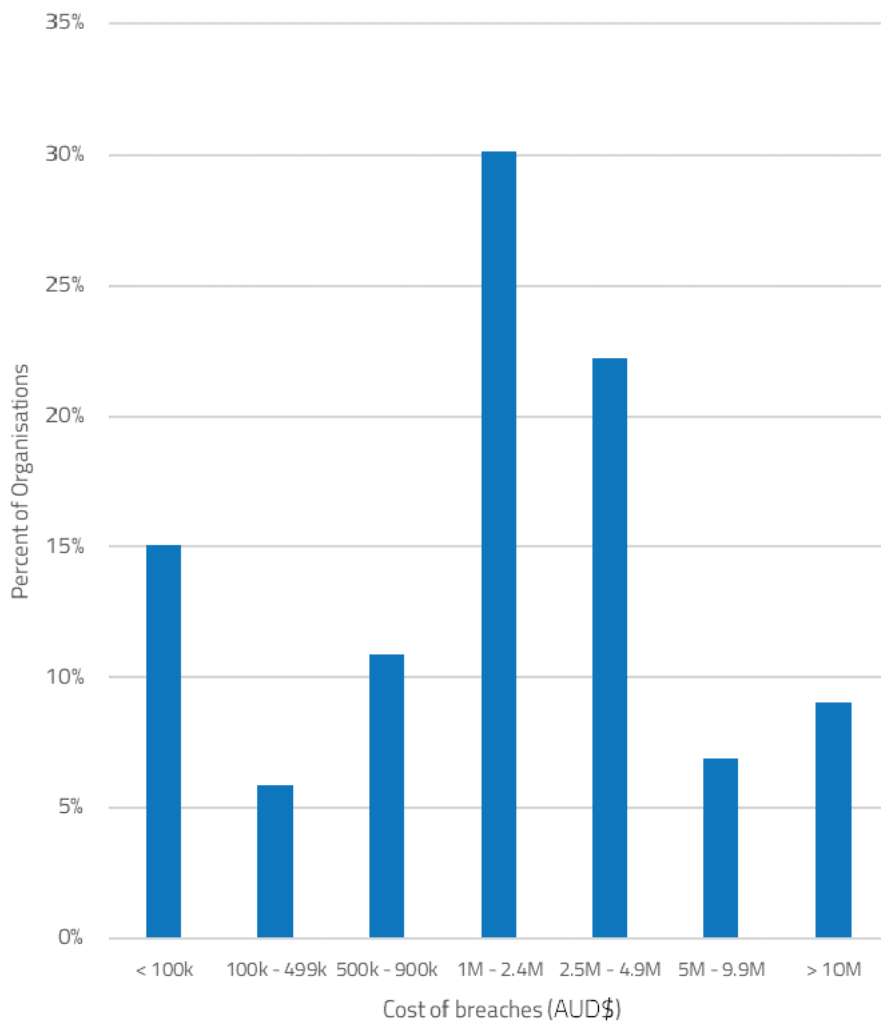
standards for how organisations identify, protect, detect, respond and recover from cyber incidents to account for a continuing escalation of costs.

¹ These figures are based on PWC Global Economic Crime Survey 2014; ABS Count of Australian Businesses 2014; ABS Business use of Information Technology 2014; Ponemon Institute Cyber Security Report 2014; Symantec Internet Security Threat Report

² Numbers based on growth rates of cybercrime listed in Accenture's 9th Annual Cost Of Cybercrime Study.

CYBER COSTS

COST OF A DATA BREACH IN AUSTRALIA

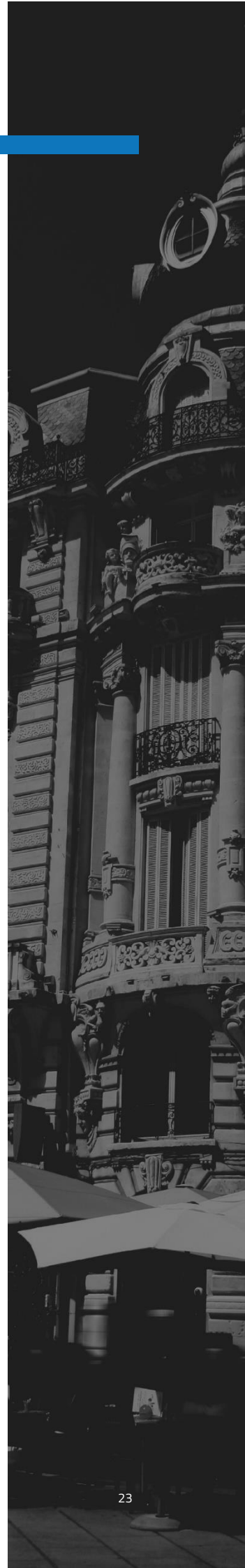


9% of organisations in Australia reported that a data breach cost the business more than \$10million.

The cost of a data breach is significant. It has been stated that upto 60% of small businesses who experience a major cyber incident never recover and close their business within six months.

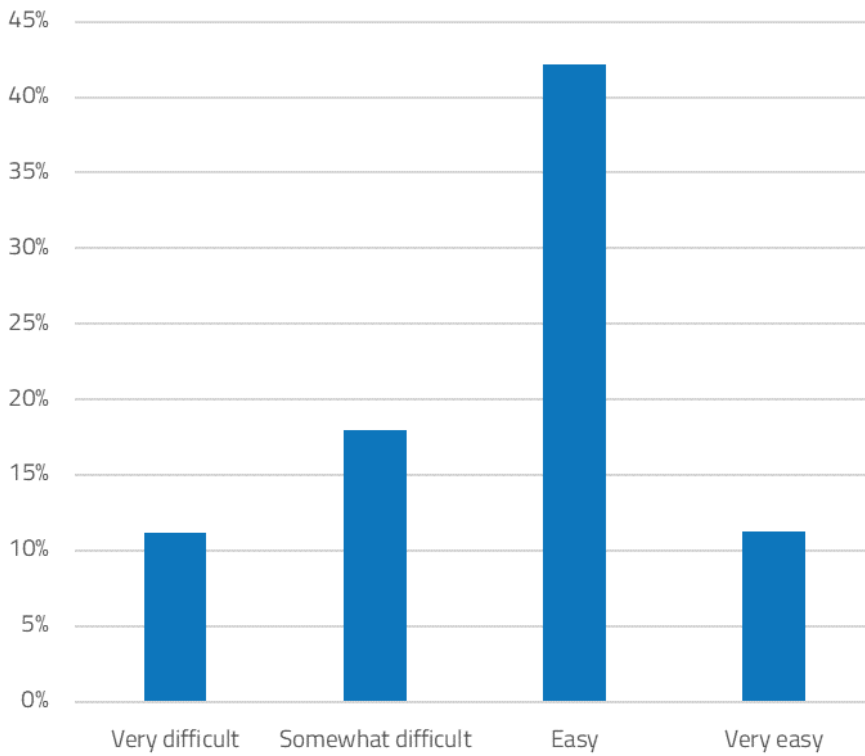
The cost when a large organisation has a cyber incident is also significant, with total costs exceeding \$10 million per organisation and an average cost of \$7.8 million.*

** Asia Pacific security capabilities 2018 – Cisco*



CYBER COSTS

HOW DIFFICULT IS IT TO CONVINCe MANAGEMENT TO INVEST IN SECURITY?



Number of survey respondents: 1894

Security In Depth has seen during the past 12-months, organisation executives starting to understand and allocate finances to increase both security resources and technology advancements into organisations across Australia. A substantial shift in attitudes has seen many organisations take significant steps forward with trying to combat cyber risk.

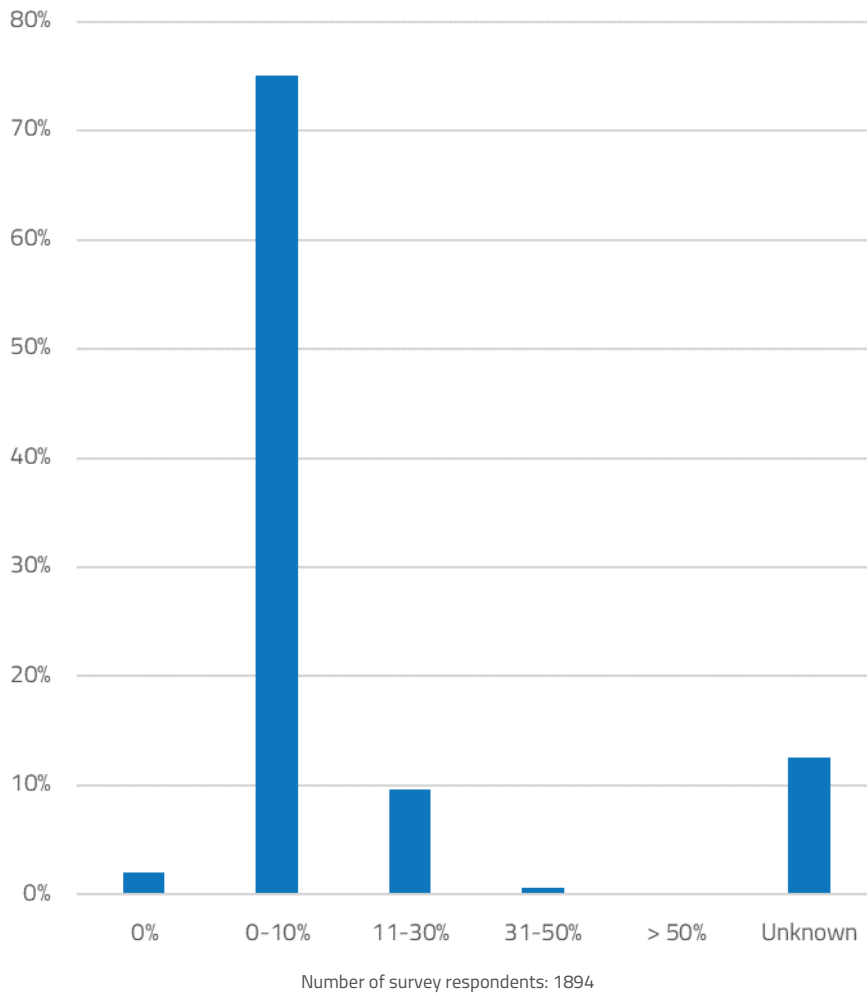
The challenge we see across the spectrum is how organisations are allocating funds – Security In Depth is finding more often than

not, the decision has become more tactical to try and cover specific challenges requiring immediate attention, an example being requests for security information and maturity from the supply chain, and organisations implementing activities like training, penetration testing or improved technology such as malware solutions. Security In Depth would like to see organisations initially improve the strategic component of cybersecurity and start with a solid governance framework.



CYBER COSTS

WHAT PART OF YOUR IT BUDGET WAS SPENT ON CYBER SECURITY?



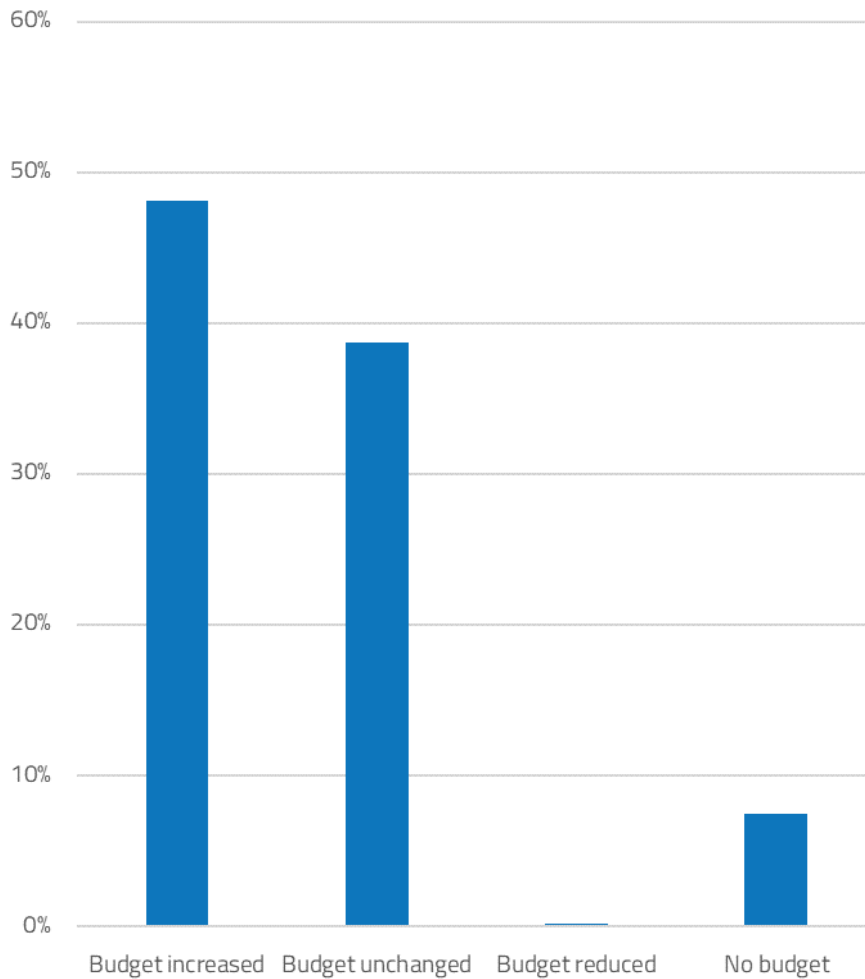
In 2019 we can see a significant increase from organisations across Australia making further investments in Cyber security. The most pleasing statistic is the 9% of organisations who had no real investment in Cyber reduce to

just over 1.5% - a significant improvement. This is also reflected in a significant spike in organisations investing up to 10% of their annual IT budget in cyber from 53% to almost 75%.



CYBER COSTS

CAN YOU DESCRIBE YEAR-TO-YEAR CYBER-SECURITY SPENDING?



Number of survey respondents: 1894

In our research, we wanted to truly understand if organisations had in fact increased spending and we have seen over the past 12 months an increase in budget and spend by almost 100%

over the 2018 numbers, indicating that organisations are assessing and seeing cyber as a significant part of their day to day business activities.



2019 ANNUAL REPORT

CYBER GOVERNANCE

Cyber Governance is essential to mitigating emerging cyber risks and managing the growing complexity of cyberspace. The potential implications of an attack are so severe, with potential disruptions to supply chains and significant business interruption, safety and reputation risks, that cybersecurity needs to be on the agenda at a board and C-suite level and applied globally.

The challenge for today's Boards, is to design and develop a cybersecurity governance framework that is flexible enough to evolve with a changing threat landscape, but also fixed to such an extent that identified and previously solved security breaches and incidents do not reoccur under known circumstances.

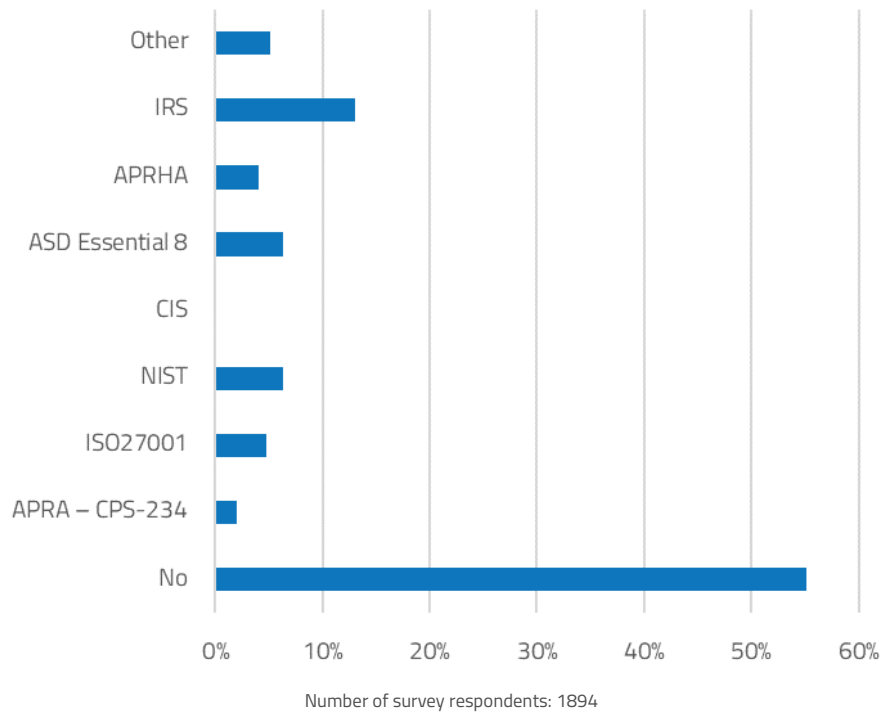
With just over 56% of today's businesses having no cyber governance framework in place, we suggest it's almost impossible to slow down the occurrence of cyber incidents within Australia, businesses, and the impact to Australian business and Australian citizens is significant with direct and indirect costs set to exceed \$7 billion AUD in 2019.



SECURITY IN DEPTH

CYBER GOVERNANCE

DOES YOUR ORGANISATION ADHERE TO IT SECURITY FRAMEWORKS?



With a substantially increased number of organisations responding and working with Security in Depth over the last twelve months, believes the numbers are indicative of larger organisations. Organisations with greater than 5,000 staff being more focused on implementing security frameworks like NIST and ISO27001. This is reflected in the increase in sample size as well as the overall increase in organisations with these frameworks in place.

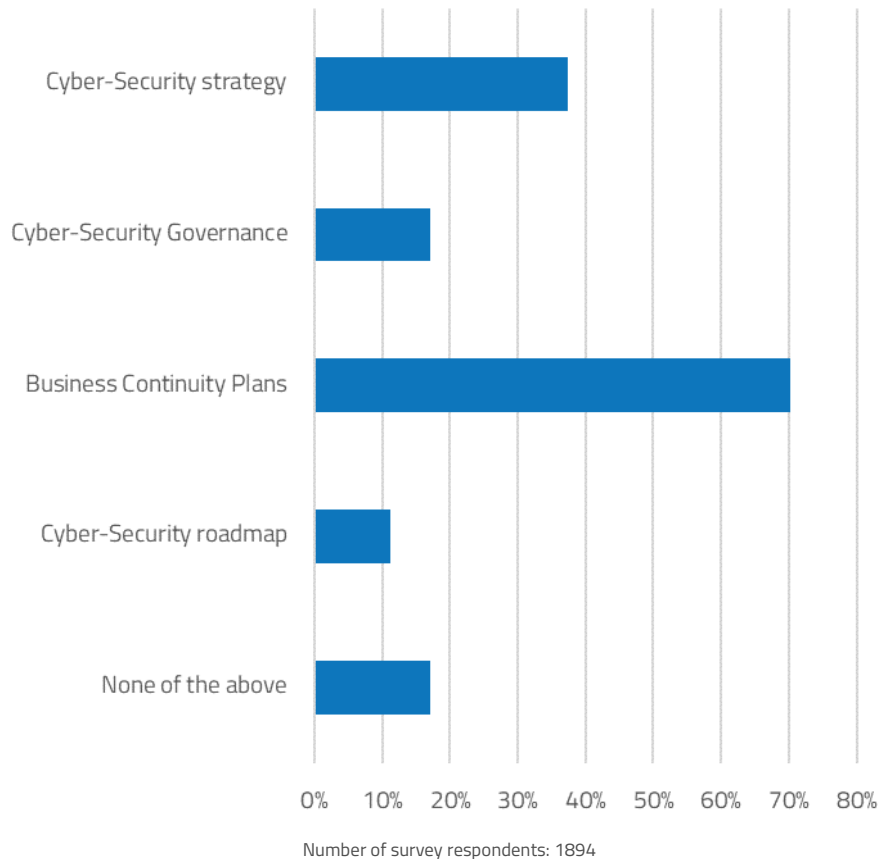
What is concerning is the number of organisations between 25 and 2,500 staff who currently have no formal security framework in place.

Many of these organisations' policies and procedures, are driven by larger organisations demanding they have certain policies and practices in place to conduct business. This adhoc approach, is considerably dangerous, as it creates a belief that appropriate security controls are in place in case of a cyber incident when in reality, there are no security controls in place. It is a false level of comfort created through naivety.



CYBER GOVERNANCE

WHICH PROCEDURES HAS YOUR ORGANISATION APPROVED?



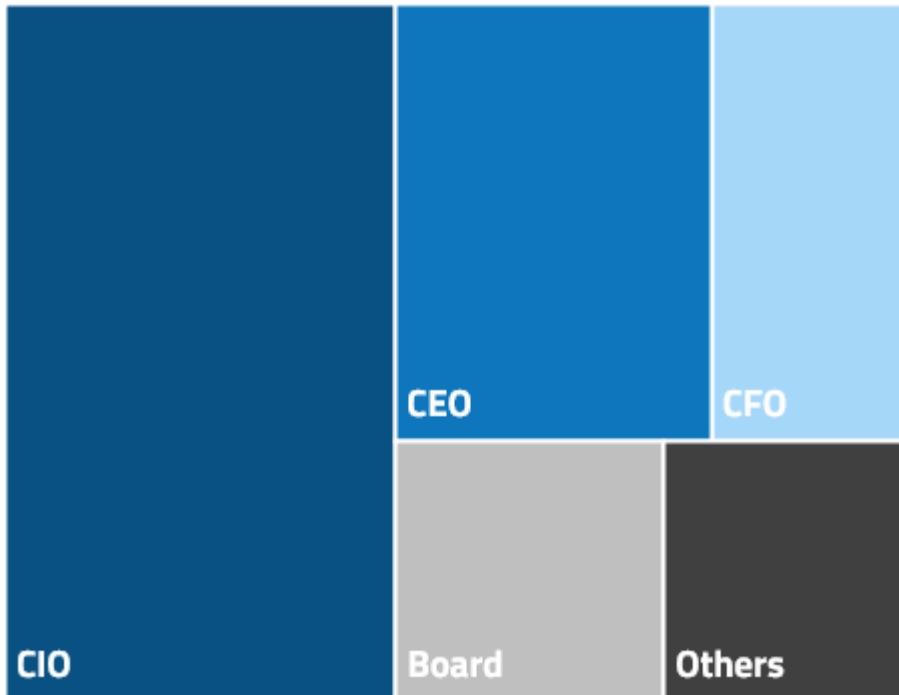
The numbers presented here correlate to numerous statistics across the report. It is obvious that IT teams have begun implementing cyber strategies and roadmaps in 2019. They have great business continuity plans and are certainly looking ahead. The challenge is the numbers tend to reflect the

cyber assurance risk scores, in that few are taking great steps forward, whilst most organisations across Australia, have a long way to go. It maybe a long bow to draw, but the numbers almost reflect the likelihood of an organisation experiencing and being compromised in a data breach in 2019.



CYBER GOVERNANCE

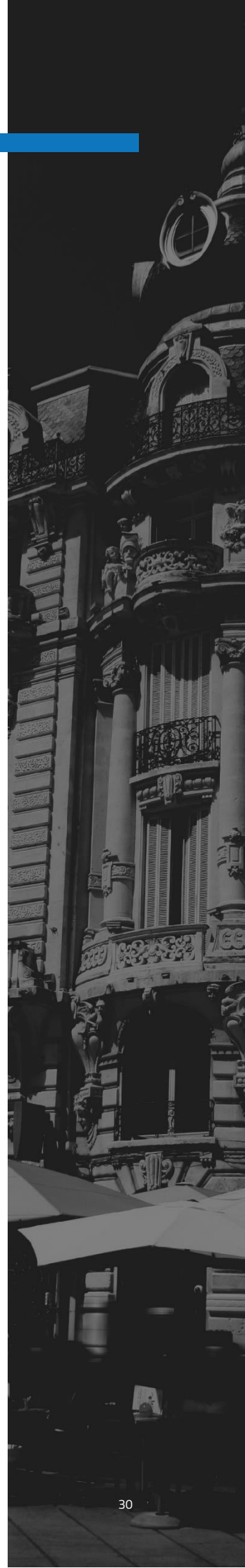
WHO DO YOUR CYBER-SECURITY EXECUTIVES REPORT TO?



Number of survey respondents: 213

Security In Depth, understands cyber risk is viewed differently by many organisations and as such, the reporting lines will be different from company to company. Our observation is that approximately 40% of organisations still have cybersecurity falling under the banner of IT. With the next 40% reporting to either the CEO, CFO or directly to the Board in certain circumstances. We infer, many of the challenges with data breaches and in particular human error, relate to a reporting line to IT.

The challenge here is, IT has no real control or impact on people across the organisation and as such, the ability to change individual behavior, is almost non-existent. Those organisations who have removed cyber risk from their IT operations, have seen significant changes in user behaviour resulting in a more mature, resilient and risk averse organisation.



OVERVIEW

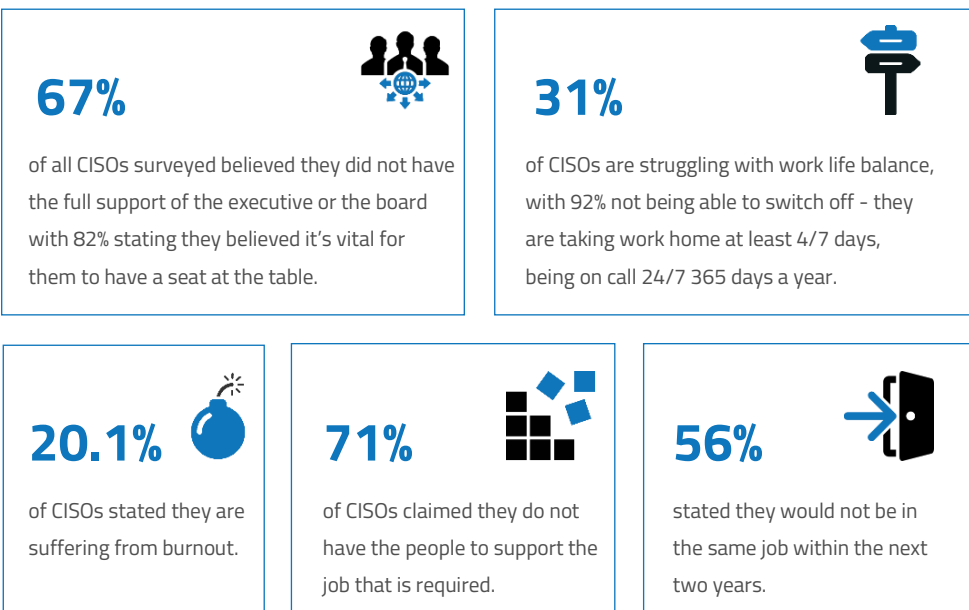
STRATEGIC VS TACTICAL CYBER SECURITY

One of the most challenging aspects of cybersecurity for organisations today, is how the CIO and CISO manages its day-to-day activities. From our reviews, one of the greatest challenges is the ability to implement a strategic framework that can be executed effectively.

From our day-to-day discussions, Security In Depth found that 88% of CISOs focus on day-to-day tactical requirements of the business rather than being able to implement a strategic vision across the organisation. Security In Depth believes the statistics back up the numbers. For example:



These challenges have led to these results:



Securing an organisation's infrastructure, has become one of the more stressful jobs in today's ICT environment, and with a lack of support across the organisation to implement a string and effective cyber strategy, is leading to high stress and burnout amongst Australian CISOs.



2019 ANNUAL REPORT

CYBER RISK

The risks and opportunities which digital technologies, devices and media bring us are manifest. Cyber risk is never a matter purely for the IT team, although they clearly play a vital role. Cyber risk, means any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems.

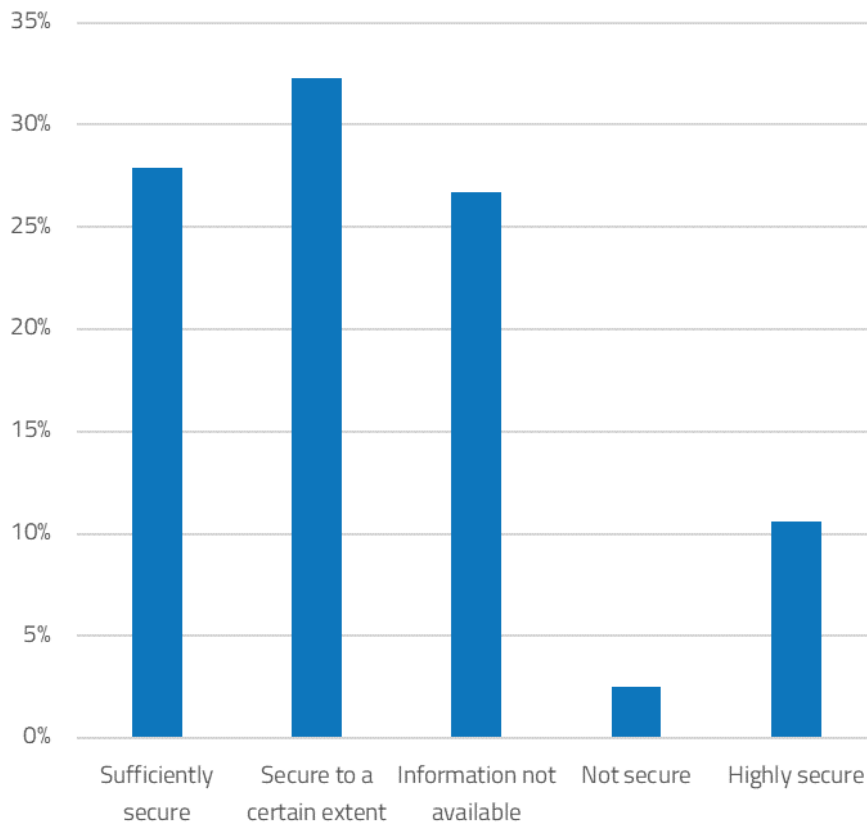
In today's business environment, cyber risk continues to be seen as a negative – another cost, complicated procedures and incoming legislative demands. Most organisations today, don't see the use of good cyber risk management as a differentiator, a selling point, and as a measure of organisational maturity.



SECURITY IN DEPTH

CYBER RISK

HOW SECURE DO YOU BELIEVE YOUR NETWORK IS?



Number of survey respondents: 1894

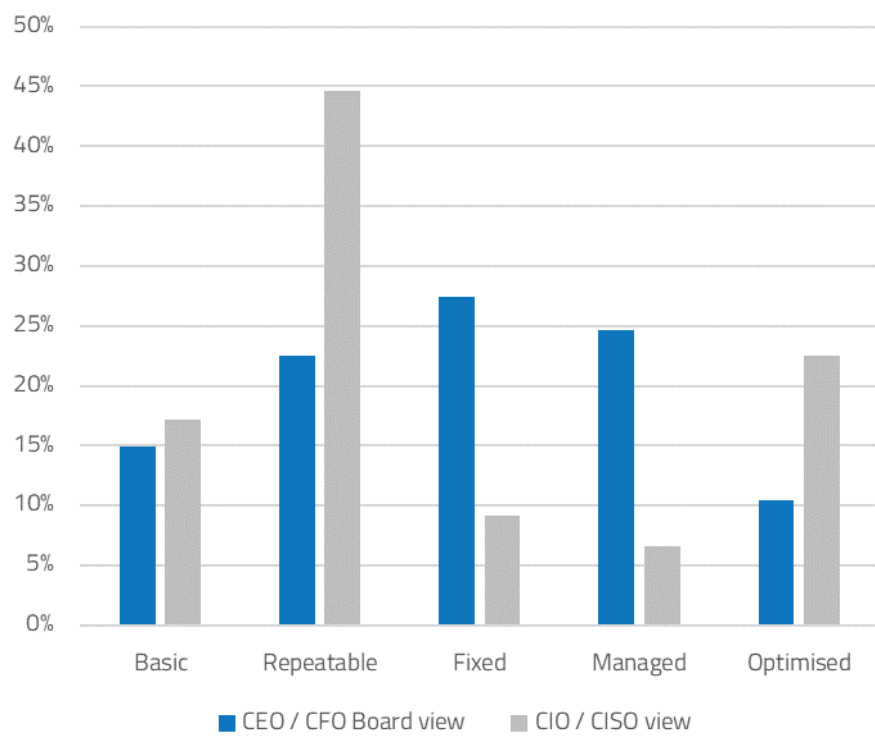
During the past twelve months, it has become evident that most organisations have taken steps to ensure they are safer and less likely to be impacted by a cyber incident. This is reflected not only here with an increase in organisations believing they are 'sufficiently

secure' as well as 'highly secure,' but also in the number of organisations who either choose not to communicate this information with a substantial increase in 'information not available' numbers.



CYBER RISK

HOW WOULD YOU DESCRIBE YOUR CYBER-SECURITY MATURITY?



Number of survey respondents:
 CEO / CFO Board view – 241 CIO / CISO view – 93

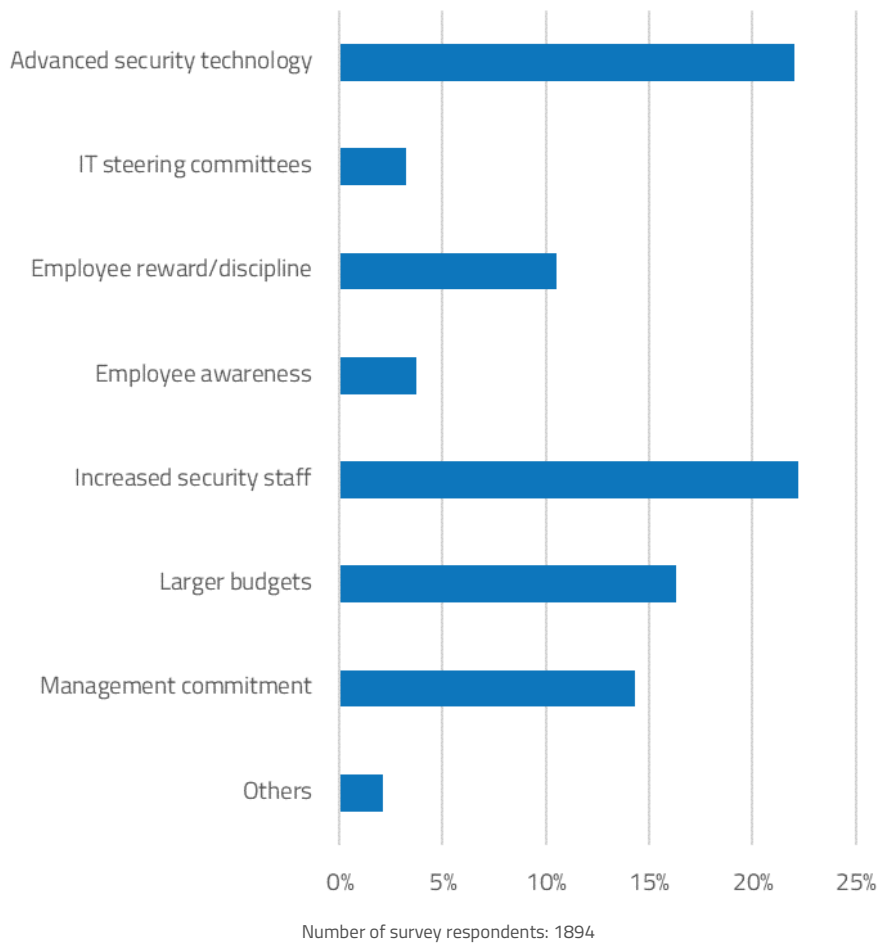
A cybersecurity maturity model provides an organisation with the ability to understand where they currently are. It provides a path forward, enabling the organisation to periodically assess where it is along that path. This is a valuable tool for improving cybersecurity efforts, as well as for communicating with management and Boards on the best way to move forward.

The numbers we see here demonstrate a significant difference in understanding cyber maturity. It is Security In Depth’s assertion, the numbers reflected by the CIO / CISO responses to be far more accurate and reflective of the different environments, whereas the CEO and CFO numbers are chosen on a belief of where the environment is.



CYBER RISK

WHAT DO YOU THINK WILL HELP IMPROVE YOUR SECURITY LEVELS?



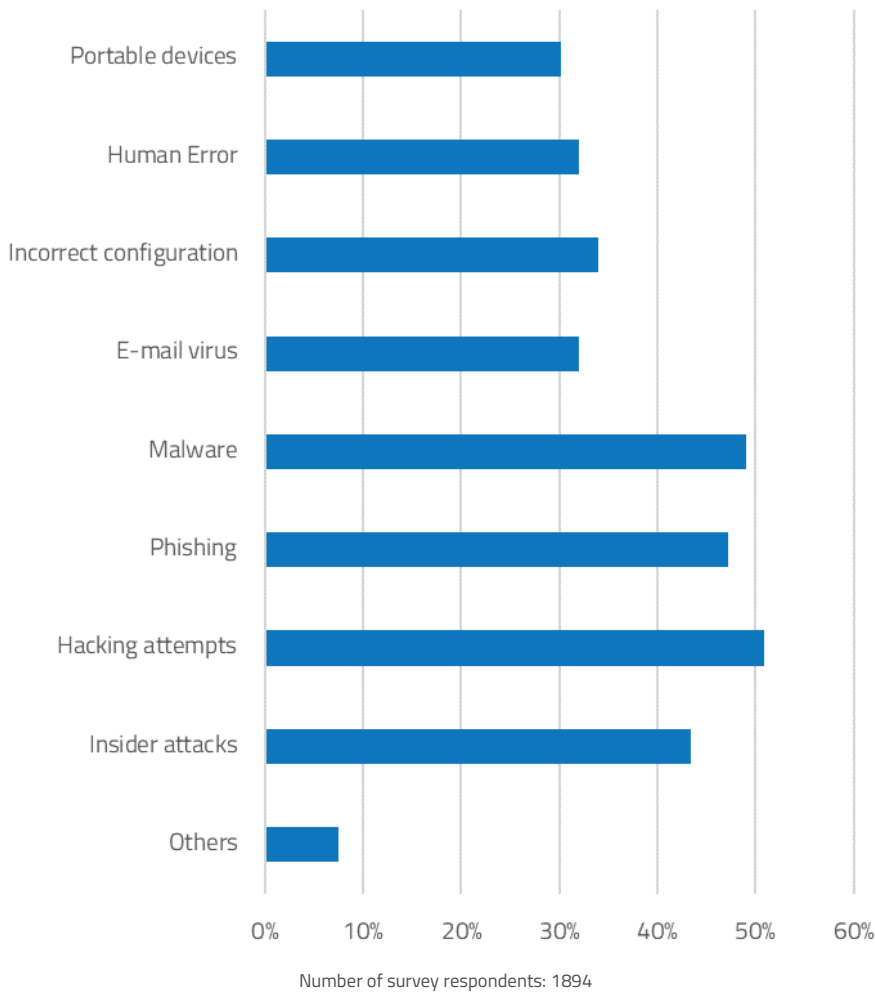
The information emanating from this question, we believe, is one of the more significant of the entire research project. The numbers continue to reflect a belief that organisations see a lack of IT resources and more advanced technology as the most appropriate way forward. Security

In Depth, offers a different viewpoint - people and processes have been highlighted in this year's research project as the main contributors to cyber incidents and the numbers indicate a belief this message is not being heard throughout Australian business.



CYBER RISK

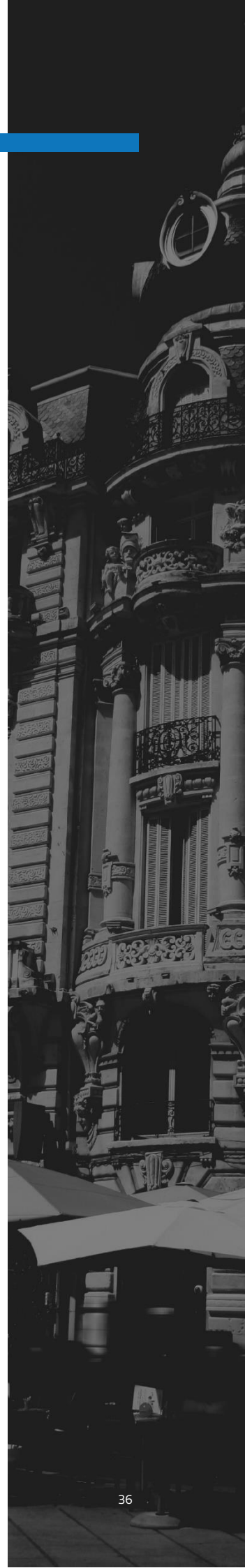
WHAT DO YOU CONSIDER TO BE YOUR GREATEST SECURITY RISK?



Many individuals believe a threat actor (hacker) is the most serious cyber risk organisations face. While a hacker remains a significant threat and is seen as the individual breaking into an organisation via their firewall, or through phishing attempts, using emails to install malware within an organisations systems, the real threat continues to remain human error.

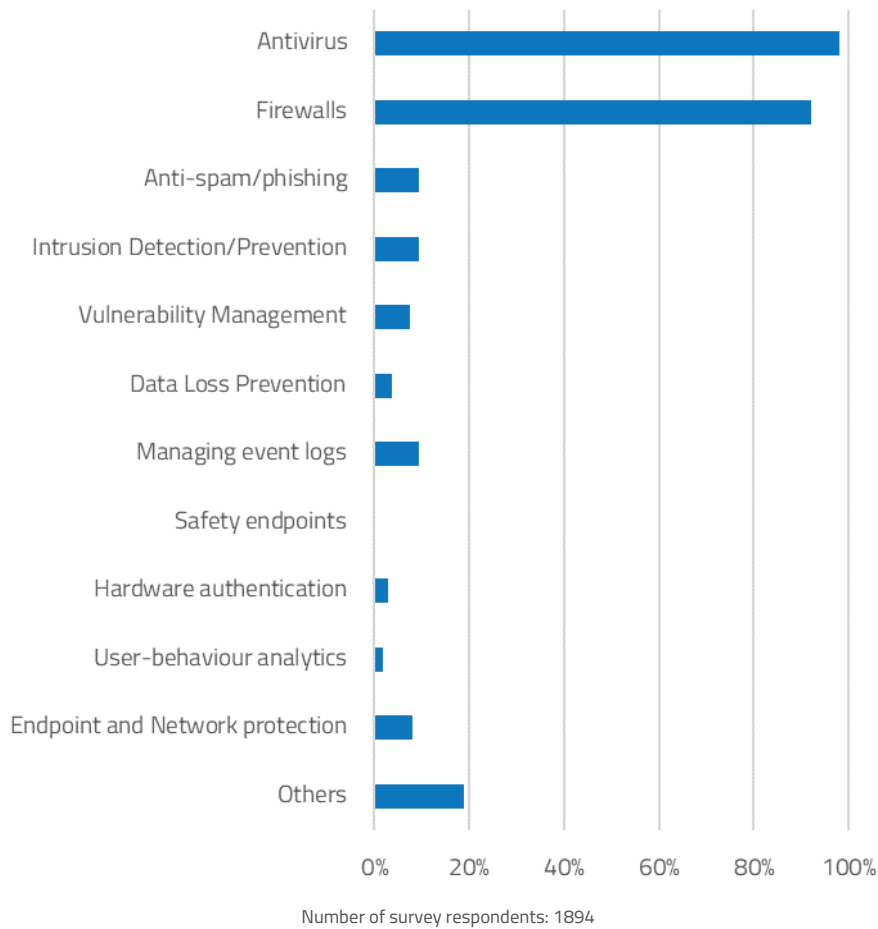
In Australia, almost 71% of data breaches are caused through human error.

This misalignment in understanding, where cyber risk lies, is one of the key challenges organisations face, and one of the greatest challenges IT and Security teams have when implementing cyber security best practices.



CYBER RISK

WHICH SECURITY MEASURES HAVE BEEN IMPLEMENTED?



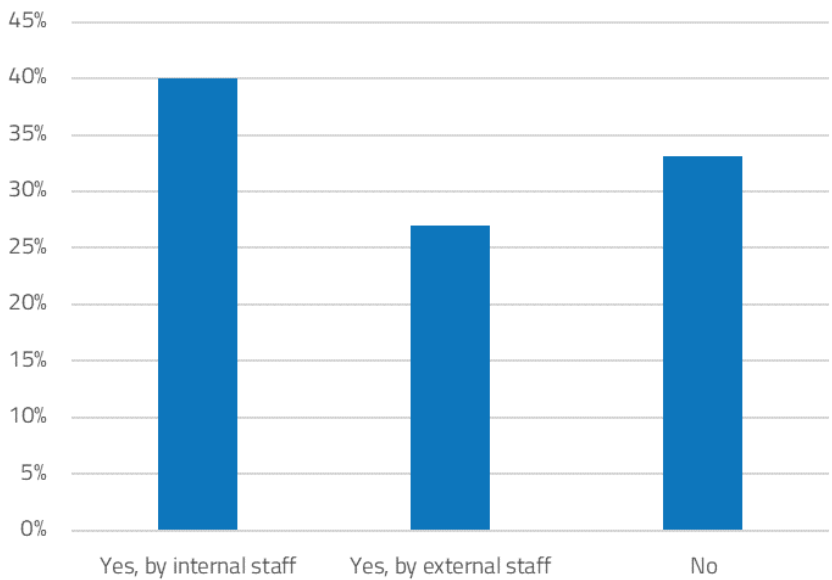
While organisations have accepted the requirement for strong anti-virus software as well as updated firewalls, the gap between utilising the two most established technologies against additional technologies is significant. What remains obvious, is the larger and more complex the organisation is, the greater the use of technology to prevent cyber incidents.

Smaller organisations cannot afford the costs associated with managing additional technologies including the cost of procuring, managing, staffing, training and additional ongoing costs. For many, the investment is too much. The outcome being, smaller organisations are significantly unprepared for a cyber incident in Australia.



CYBER RISK

HAS PENETRATION TESTING BEEN PERFORMED IN YOUR ORGANISATION?



Number of survey respondents: 1894

The numbers presented here are disturbingly confounding. What has become apparent is that we are finding it difficult to accept that only 67% of organisation do some form of penetration testing within their infrastructure. Our experience and what we are witnessing daily, overtly contradicts this figure.

Whether it be a web application test or a simple external penetration test, Security In Depth is concerned the numbers do not accurately reflect organisations that are actually conducting these tests. What is more palatably acceptable is that 26% of organisations are conducting annual penetration testing, while almost 40% of organisations are in fact conducting a form of vulnerability testing and scanning rather than true pen testing.

The difference being, penetration testing is focused on identifying insecure business processes, lax security settings or other vulnerabilities a threat actor could exploit, while vulnerability scans test for known vulnerabilities – a significant difference.

If we make this assumption, which Security in Depth will confidently make, then what becomes evident is a dramatic shift in the figures where only 27% of companies or 1 in 4, actually conduct penetration testing. This once again represents a challenge to Australian organisations to improve their testing regime and understand where and how they may be vulnerable.



2019 ANNUAL REPORT

CYBER AWARENESS

If you speak to any cybersecurity professional in the world and you ask what's the weakest part of any organisation, they will categorically say to a person – humans. That can easily be seen by observing that almost 70% of data breaches reported in Australia over the last twelve months can be directly attributed to human error.

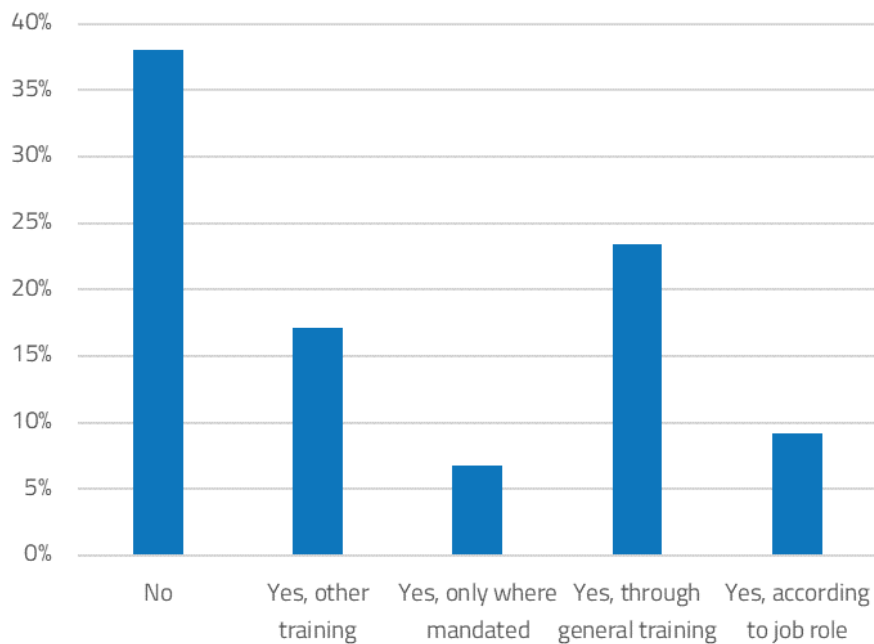
For an organisation to institute cyber awareness training they are taking important steps to reduce cyber risk, to mitigate the chance of a data breach. This is how organisations are effectively building the bridges between technology, the technology department, the processes within an organisation and their people. It is at the moment, the most critical step an organisation can take in the path to cyber maturity.



SECURITY IN DEPTH

CYBER AWARENESS

DOES YOUR ORGANISATION PROVIDE CYBER-SECURITY AWARENESS TRAINING?



Number of survey respondents: 1894

The realisation across organisations that cyber awareness training is now a significant part of their cyber strategy and cyber maturity, is seen from the figures we see above. More organisations are conducting cyber awareness training this year than last year. We have seen a significant improvement in the number of organisations who have adopted with an overall jump by approximately 10% - which translates to an estimated extra 3,500 organisations recognising the need for training and implementing a training program. The challenge that remains, is the 62% of organisations who fail to provide any cyber awareness training to staff members.

Security In Depth would like to suggest during the last 12 months, the number of data breaches caused by human error correlates closely with the percentage of organisations who do not conduct cyber awareness training.

We recognise there will always be outliers – The Australian Banks for instance are the highest reporting groups for data breaches under the Notifiable Data breach legislation, however they have significant and consistent cyber awareness training.



2019 ANNUAL REPORT 2019 ANNUAL REPORT

THIRD PARTIES & YOUR DATA

While key operations and processes can be outsourced to a third party, your business risks can't. Why do so many organisations still fail to adequately assess their third party supplier IT security risks and ensure the on-going security and availability of their business critical information?

Third party suppliers can be an attractive way for cyber criminals to gain access to data and networks that would otherwise be beyond their reach. A huge range of external suppliers, from marketing to accountants to legal firms, can all be potential vulnerabilities. These suppliers may hold customer data, employee data or intellectual property that is hugely valuable to competitors.

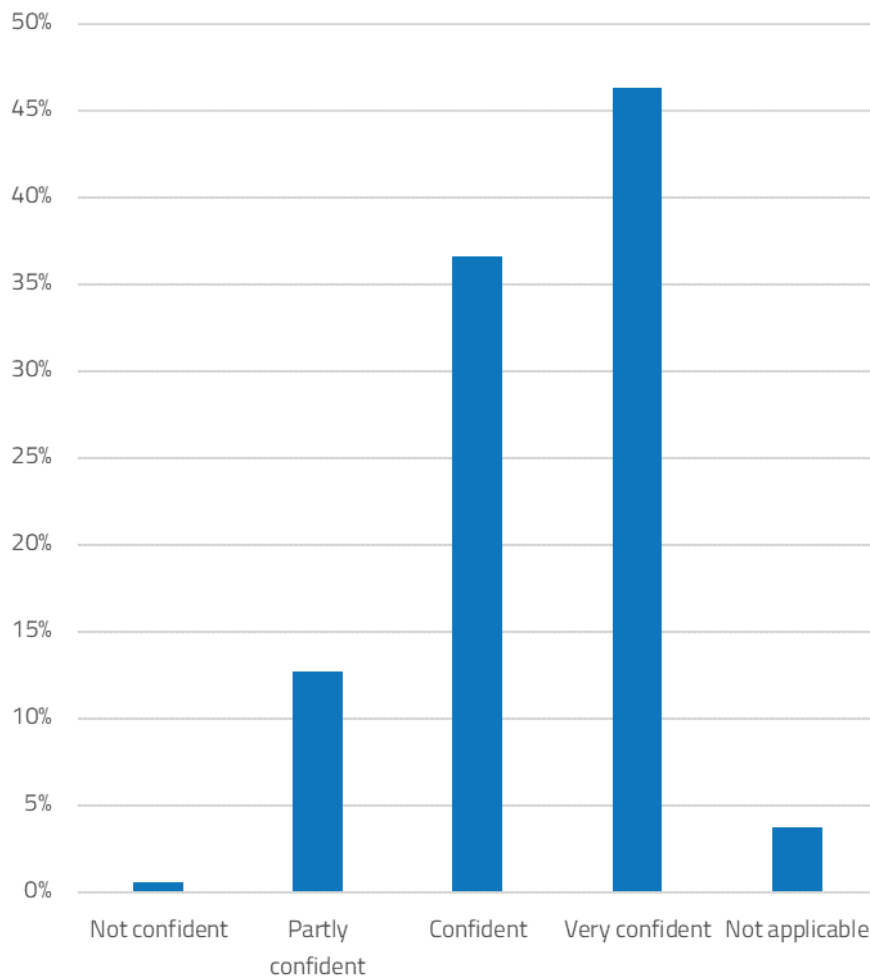
When dealing with a third party it should be a given that all possible technical safeguards have been put in place to protect your data, however, as recent headlines have shown, this is not always the case. Organisations need to impose the same strict security policies for all third party suppliers and partners as they do for themselves.



SECURITY IN DEPTH

TRUSTING THIRD PARTIES WITH YOUR DATA

HOW CONFIDENT ARE YOU IN THE CYBER-SECURITY OF YOUR THIRD PARTIES?



Number of survey respondents: 1894

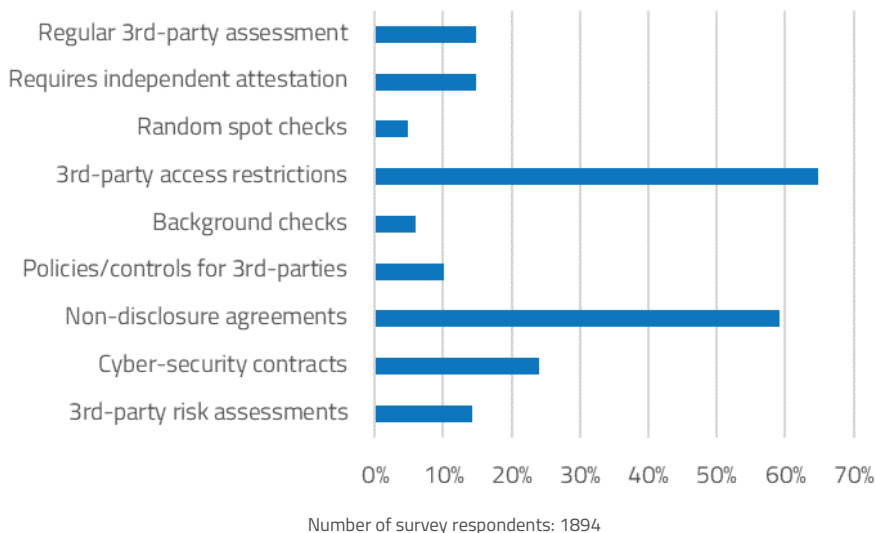
Today's business leaders, when asked how secure do they believe the organisations they are sharing data with are, believe everything is fine. Most organisations surveyed, of which 82%, responded said they are confident to very

confident the data they are sharing will be looked after. Yet, according to the latest Ponemon report, 59% of these organisations had data lost through a data breach in the last 12 months.



TRUSTING THIRD PARTIES WITH YOUR DATA

HOW DO YOU ENSURE CYBER-SECURITY WITH THIRD PARTIES?



Fifty-nine percent of all companies surveyed, have experienced a third-party breach during the last 12 months, a 3% increase on the previous year*. Data breaches caused by third parties cost millions of dollars to large companies. Third parties include a broad range of entities a company has directly worked with, like data management companies, law firms, email providers, web hosting companies, subsidiaries, vendors, sub-contractors - any company whose employees or systems have access to a company's systems or data. However, third-party cyber risk is not limited to these companies. Any external software or hardware used in business also poses a cyber risk.

The importance of working with & sharing data with suppliers is now a day-to-day business requirement, and yet, the data on how

organisations within Australia review these organisations, are in Security In Depth's opinion, appalling –84% of Australian companies have conducted no formal review on the practices of companies they share data with. The research highlights organisations are failing to utilise modern day business requirements to assess cyber risk, instead, they focus on basic contractual requirements for assessing and mitigating risk. The adage "trust but validate" should be the starting point for where organisations begin when sharing data. Not putting in place non-disclosure agreements 59% of organisations, or cyber-contracts 22%.

These figures highlight during the next 12-months, 59% of organisations who have had data compromised by third party breaches will continue to grow and organisations will continue to be challenged with third party data breaches.

*Ponemon Institute Cost of Data Breaches 2018/2019



OUR METHODOLOGY

The purpose of this study is to highlight the dependencies between the attitudes of Australian Corporate Boards, Senior C-Level executives and ICT departments towards the challenge of cybersecurity. With this purpose, the study was conducted through both qualitative and quantitative research, which we believed allowed gaining the most relevant results about the relations between the cybersecurity challenges and corporate performance.

Research Approach

The respondents to this study represented 1894 organisations across Australia with a minimum of fifty staff. Respondents included Board members, CEOs, Managing Directors, CIOs, CISOs and IT Managers. The organisations were selected without regard to their existing cybersecurity practices or technologies.

Questionnaire

The method of the questionnaire enables the research to be more quantitative because it requires the collation of standardised information from a specific number of people. The method also enables the data to be both qualitative and quantitative, which is the most appropriate way to research the connection between cybersecurity technologies, processes and organizational performance.

Security In Depth sent the questionnaire to 23,433 executives across 19,887 organisations without regard to their age, gender or performance.

The questionnaire asked questions that revealed the respondents' information on position, experience, performance and use of technology as well as information about Security Governance. One thousand, eight hundred and ninety-four responses were received with 922 providing detailed answers to both the qualitative and quantitative questions. The data obtained allowed Security In Depth to build cause and effect relationships based on the answers. Our research considers organisational structure, people, technology, processes and experience in our results.

Statistical Data Analysis & The Documentary Analysis

The method enables obtaining additional data from documents and studies that already exist. This fills any informational gaps that may not be revealed by the responses to the questionnaire. The research uses documents to describe the background of cyber Challenges across Australia as well as to complement the results with reliable scientific findings. Further, the documentary analysis enables obtaining various statistical data, which adds more credibility to the research. Examples of this information has been compiled accessing information from the following sources. Notifiable Data Breaches quarterly statistics reports, June 2018, Sept 2018, Jan 2019, April 2019, Verizon Enterprise Data Breach Report 2019, Webinsurance List of Data Breaches in Australia 2018 and 2019, Ponemon Institute and Accenture's 2019 cost of Data Breach, and Security in Depth State of Cyber Security Research 2019.





SECURITY IN DEPTH

1300 041 042

www.securityindepth.com.au

Level 2, 1 Southbank Blvd, Southbank, Melbourne 3006

Level 9, 50 Clarence St, Sydney 2000

Level 2, 37 Barrack St, Perth 6000

Level 9, 204 Alice St, Brisbane 4000

276 5th Av, New York, NY 10001

20-22 Wenlock Rd, London, N1 7GU