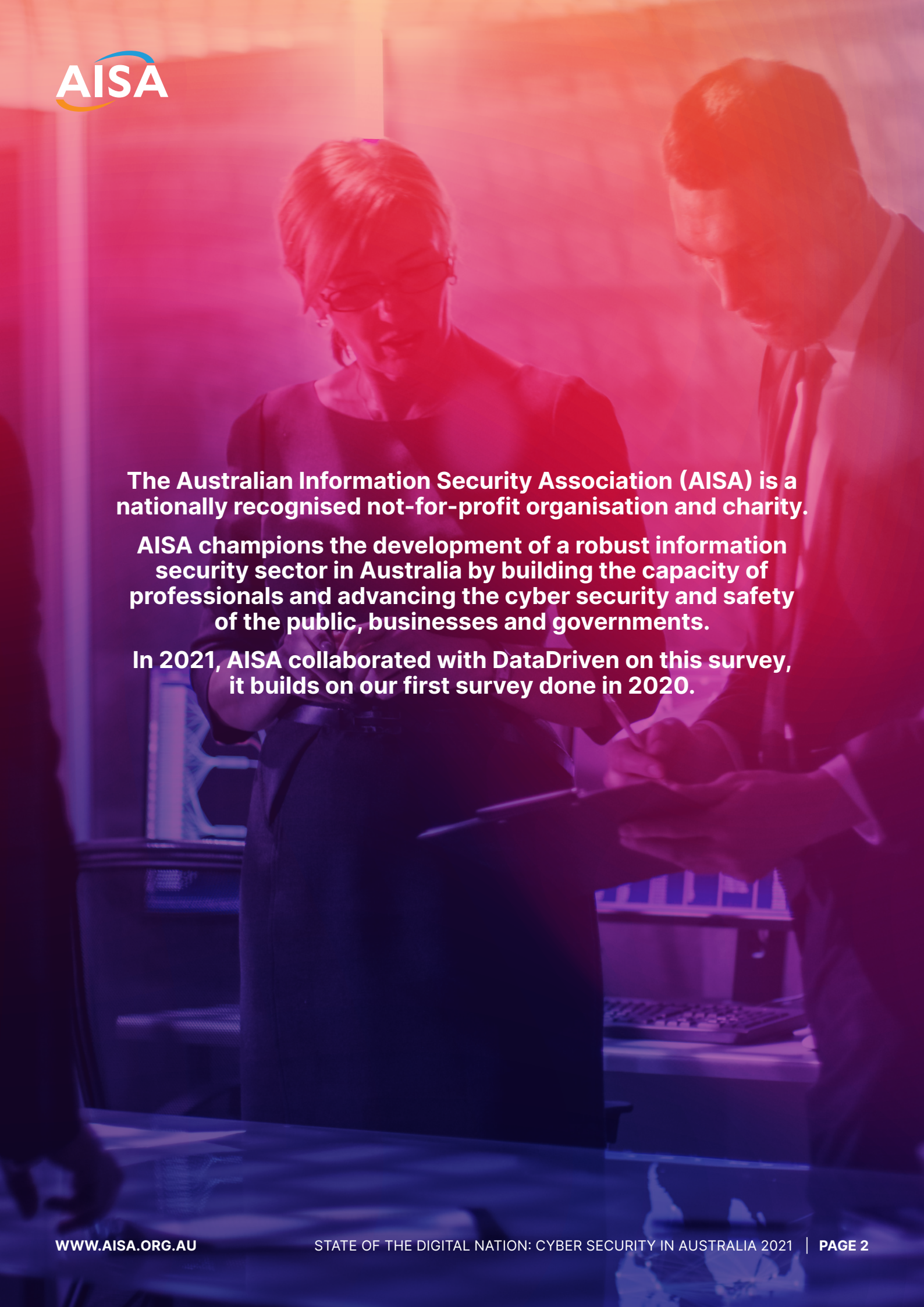
STATE OF THE DIGITAL NATION:

CYBER SECURITY IN AUSTRALIA 2021



The Australian Information Security Association (AISA) is a nationally recognised not-for-profit organisation and charity.

AISA champions the development of a robust information security sector in Australia by building the capacity of professionals and advancing the cyber security and safety of the public, businesses and governments.

In 2021, AISA collaborated with DataDriven on this survey, it builds on our first survey done in 2020.

TABLE OF CONTENTS

FOREWORD

STATE OF THE DIGITAL NATION: CYBER SECURITY IN AUSTRALIA 2021

To add value to our members and partners ongoing understanding of cyber security, AISA has partnered with research company DataDriven for a second year in this survey of 120 ICT decision makers in Australia. It is a drill-down into the area of cyber security and related technologies and services through the eyes of the people who manage, deliver and purchase these technologies – the ICT decision makers.

AN INDEPENDENT PERSPECTIVE

The technology and services available to meet mission critical enterprise wide security needs of organisations is changing dramatically as are the delivery and commercial models and new challenges arise daily. To shed light on these challenges AISA is proud to deliver to you this independent report on the state of cyber security in digital and related ICT services in Australia.

WHAT THIS REPORT COVERS

The report provides key findings from the survey – some of which will confirm what we already know and some which will surprise. Last year, the hype around cyber security seemed to be aligned to its importance for decision makers. Members may have found this to be encouraging, but possibly as digital initiatives progress and with the pandemic, fewer, 44% said it was important this year.

This survey was conducted as the COVID-19 pandemic was well progressed and it is likely these decision makers had to dramatically shift their focus. The pandemic accelerated the adoption of digital technologies and remote work, putting pressure on executives to do more with less to serve their customers.

Meeting the privacy, cyber security, and business continuity needs of their organisations is critical, and the rapidly changing and increasingly dangerous security environment has increased the challenges for today's ICT decision maker. Recent damaging ransomware attacks and data breaches demonstrated to leaders and legislatures that they must do more and boards and executives fully expect increased compliance requirements in the coming year.

Fortunately, the range of cyber security offerings and related services also continues to increase in this second year, but this has also increased the range of choices. We trust that this report will go some way towards clarifying these issues and augmenting your understanding of what your peers in Australia are actually doing in this area.

We welcome feedback on this survey and hope you enjoy some of the different perspectives delivered in the survey data graphs, CMM measures, Hype-dials and Implementation vs Investment Matrices. These provide a provocative perspective on ICT decision makers perspectives in 2021.

With 2021 behind us, we look forward to a better 2022.

MICHAEL TROVATO, DIRECTOR

Australian Information Security Association

DAMIEN MANUEL, CHAIR

Australian Information Security Association

INTRODUCTION AND KEY FINDINGS

For the second year, AISA commissioned DataDriven to produce a report based on an extensive survey of ICT leaders which was conducted in March 2022 about their organisation's Digital Transformation (DX) and ICT practices.

The resulting report focused on Australian ICT decision makers, with a strong focus on cyber security.

> **"This report is primary research based on the views of the people who use the technology – Australia's ICT decision makers."**

SECURITY THREATS INCREASE, BUSINESS AND GOVERNMENT RESPONDS

A lot of water has flowed under the bridge since the 2020 edition of this study. Security threats are growing, many organisations - especially small and medium businesses (SMBs) - continue to be less well protected than they should be, and the Australian and State Governments have accelerated the review and development of policy and legislation for privacy and cyber security.

SECURITY CUTS ACROSS ALL ASPECTS OF LIFE IN THIS COUNTRY

With the growing threat landscape, the Australian Government over the past year has released a number of reviews and proposed changes to privacy and security regulation. The frequency of reviews and updates is critical due to increased adoption of digital technologies and the fast-changing nature of the threats. The diversity of government departments involved shows how essential security is to all aspects of life.

AISA AND MEMBERS ARE ACTIVE

The AISA has been conspicuous in consultation processes, representing the views of its 7,500-plus Members as well as drawing on feedback from member research studies. We encourage Members to see our submissions, published on our website.

KEY FINDINGS (CONTINUED)

MANAGING RISK AND SECURITY IS RIGHT AT THE TOP OF THE BUSINESS AGENDA

ICT Leaders who responded to the survey say managing risk and security issues is among their top three business objectives – along with increasing productivity and collaboration and increasing competitive advantage.

DEPLOYMENT OF SECURITY SOLUTIONS HAS RAMPED UP

Three-quarters or more of all respondents have implemented all 12 of the cyber security technologies researched – either as mature implementations, or ones that are underway, or at pilot/Proof of Concept (POC) stage. Deployment of security solutions has shot up in the past year across almost all categories.

RANSOMWARE HAS GOT EVERYONE'S ATTENTION

Nothing could be more a sign of the times than ransomware protection being the most widely implemented technology (at 84% of organisations), and also the technology that will attract the most widespread investment over the next 12 months (84% of respondents are investing). The industrialisation of cyber crime has the Australian Cyber Security Centre (ACSC) concerned and Home Affairs focused on Strengthening Australia's Cyber Security Regulations and Incentives.

SECURITY SPENDING WILL BE MUCH HIGHER THROUGH 2021/22

Despite widespread current deployment, businesses understand they still need to invest more in cyber security to continue to address the growing magnitude of the risk. As a result, planned investments in cyber security technologies are higher in 2021 across the board than in 2020. Of the cyber security technology items researched in 2020 and 2021, the planned investment in 2021 is higher by a margin of 22 percentage points (that's the lowest increase) and extends up to 36 percentage points for the largest increase.

CYBER SECURITY SERVICES ARE ALSO SURGING

Cyber security services use is growing too. As cyber security changes and becomes more complex, businesses often need specialist help to assess, transform and respond to risks. For all seven of the services researched in both 2020 and 2021, the 2021 deployment levels are notably more advanced.

E-COMMERCE BUSINESSES ARE MORE ADVANCED WITH SECURITY

Organisations that generate 50% or more of their revenues online are generally further advanced with deployment of security, backup and recovery solutions, and with their use of cyber security services than those who source less than 50% of revenues online.

COVID-19 HAS MOSTLY ACCELERATED ICT BUDGETS

More than two-thirds of respondents said COVID-19 had a positive impact on their planned budget over the last 12 months. The majority of respondents believe COVID-19 will continue to have a net positive impact on budgets over the next 12 months (from March 2021).

"Businesses understand they still need to invest more in cyber security to continue to address the growing magnitude of the risk. As a result, planned investments in cyber security technologies are higher in 2021 across the board than in 2020."

BUSINESS OBJECTIVES AND ICT CHALLENGES

The survey asked a range of questions about the organisation's business objectives and ICT challenges, to help place cyber security within the larger business and technology contexts.

The survey found that cyber security and related areas were among the most important objectives, and constituted by far the most strategic ICT challenges.

CYBER SECURITY AND BUSINESS

ICT exists to help organisations achieve their business objectives. In an era of digital business and digital transformation, ICT systems are central to the enterprise's ability to function. By extension, this means cyber security is no longer a technical issue, but a business issue.

The results of the survey provide tangible evidence that this change in mindset has occurred in Australia in recent years. Risk management is regarded as a key business objective, and cyber security issues are more important to ICT professionals than almost all traditional concerns.

"Cyber security issues are at top of mind for the great majority of Australia's ICT professionals."

BUSINESS OBJECTIVES

PRODUCTIVITY, SECURITY AND COMPETITIVENESS ARE PRIORITIES

Respondents were asked to rate key business objectives from 'extremely high priority' to 'not a priority'. The key business objectives chart is sorted in descending order – showing the sum of 'high priority' and 'extremely high priority' at the top.

Business leaders are juggling a range of objectives including increasing productivity and collaboration (a high or extremely high priority for 72%), increasing competitive advantage (66%), and managing risk and cyber security (also 66%). Staying on the theme of security, 65% say improving all aspects of security is also a key business objective.

The table to the left of the chart shows results for both the 2020 and 2021 survey, and changes are indicated in the middle column. Managing risk and cyber security is considered of high or extremely high importance by 66% of respondents in 2021 compared to 63% in 2020. There is no comparison for 'improving all aspects of security' as that question was not asked in 2020 (indicated by the "x" in the 2020 column).

These results underscore how security has moved from being primarily a technical issue to become a central and key objective for the whole business – ahead of traditional objectives like reducing costs and making revenue/budget targets.

Aside from the focus on security and productivity, business leaders are also prioritizing a range of objectives aimed at making their businesses more successful in an increasingly competitive environment: 65% want faster innovation; and the same proportion wants to implement organisation-wide integration.

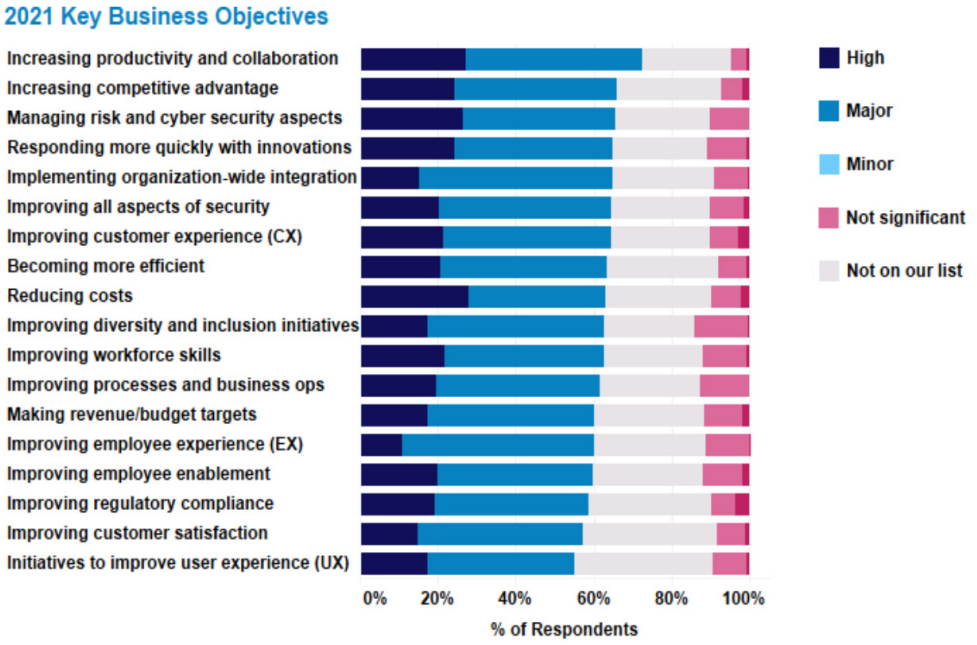
The other key focus for respondents is improving customer experience (CX).

The bottom line: security is ranked 2nd equal as a business priority, and is unquestionably a driving force for almost all Australian businesses.

> **"Managing risk and cyber security, and improving all aspects of security are key objectives for business leaders."**

Key Business Objectives

2020	Change	2021	
63%	↑	72%	Increasing productivity and collaboration
54%	↑	66%	Increasing competitive advantage
63%	↑	66%	Managing risk and cyber security aspects
x	✖	65%	Responding more quickly with innovations
43%	↑	65%	Implementing organization-wide integration
x	✖	65%	Improving all aspects of security
x	✖	64%	Improving customer experience (CX)
x	✖	63%	Becoming more efficient
57%	↑	63%	Reducing costs
36%	↑	63%	Improving diversity and inclusion initiatives
x	✖	63%	Improving workforce skills
63%	↓	62%	Improving processes and business ops
61%	↓	60%	Making revenue/budget targets
43%	↑	60%	Improving employee experience (EX)
x	✖	60%	Improving employee enablement
53%	↑	59%	Improving regulatory compliance
x	✖	57%	Improving customer satisfaction
x	✖	55%	Initiatives to improve user experience (UX)



ICT STRATEGIC CHALLENGES

CYBER SECURITY IS A STRATEGIC CHALLENGE

The survey provided respondents with a comprehensive list of ICT strategic challenges and asked them to rank the challenges, from 'high significance' to 'not on our list of challenges'.

The chart shows the top challenges, sorted from the top down ('high significance' plus 'major significance').

Cyber security is clearly the biggest issue facing Australia's ICT professionals. While 74% of respondents say applications development is the #1 ICT strategic challenge, eight of the other top ten challenges are directly concerned with cyber security, or directly related to it (e.g., regulatory compliance, business continuity and privacy regulations).

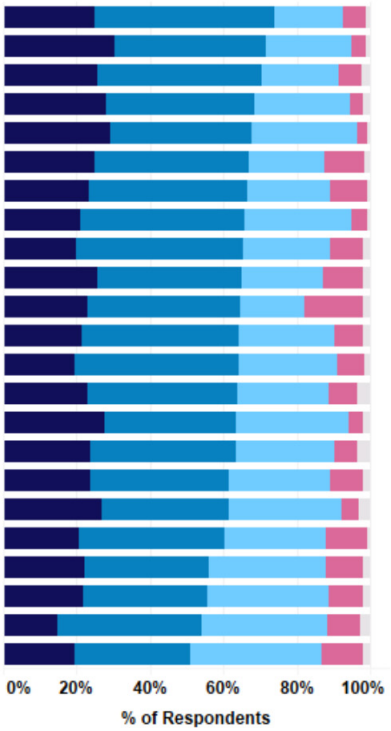
Application security has jumped up the list of ICT strategic challenges with 72% rating it a major or high challenge compared to 47% in 2020. This is the result of accelerating digital transformation (DX) across all industries as businesses rush to provide improved CX via better web and mobile apps. Businesses are hyper aware that applications directly used by their customers must have robust security.

Network security is ranked the #3 challenge this year, with 70% rating it a major or high challenge compared to 58% in the 2020 study. This is a prominent challenge due to the burgeoning extended networks businesses have deployed to support working from home (WFH) during the COVID-19 disruption.

The bottom line: Cyber security is a leading challenge across all aspects of ICT.

ICT Strategic Challenges

2020	Change	2021	2021 ICT Strategic Challenges
x	✖	74%	Applications Development
47%	⬆	72%	Application security
58%	⬆	70%	Network security
52%	⬆	68%	Regulatory compliance
43%	⬆	68%	Accessing quality cloud services
53%	⬆	67%	Web security
55%	⬆	67%	Business continuity
45%	⬆	66%	Cyber security
52%	⬆	65%	Email security
48%	⬆	65%	Data privacy regulations
x	✖	64%	Low/Code, No Code, Citizen Development
52%	⬆	64%	Cloud security
46%	⬆	64%	Training and developing staff
46%	⬆	64%	Incident detection response and recovery
53%	⬆	63%	Database security
39%	⬆	63%	Increased prices from suppliers/SIs
43%	⬆	61%	Improving service/support responsiveness
47%	⬆	61%	Data sovereignty (keeping data onshore)
48%	⬆	60%	Vulnerability mgmt & penetration testing
57%	⬇	56%	Data centre security
48%	⬆	56%	Creating an optimal working environment
x	✖	54%	Applications Management Services
39%	⬆	51%	Changing business and market requirements



"Eight of the top ten ICT strategic challenges have to do with security."

EVENTS IN 2022

JOIN US IN PERSON IN 2022

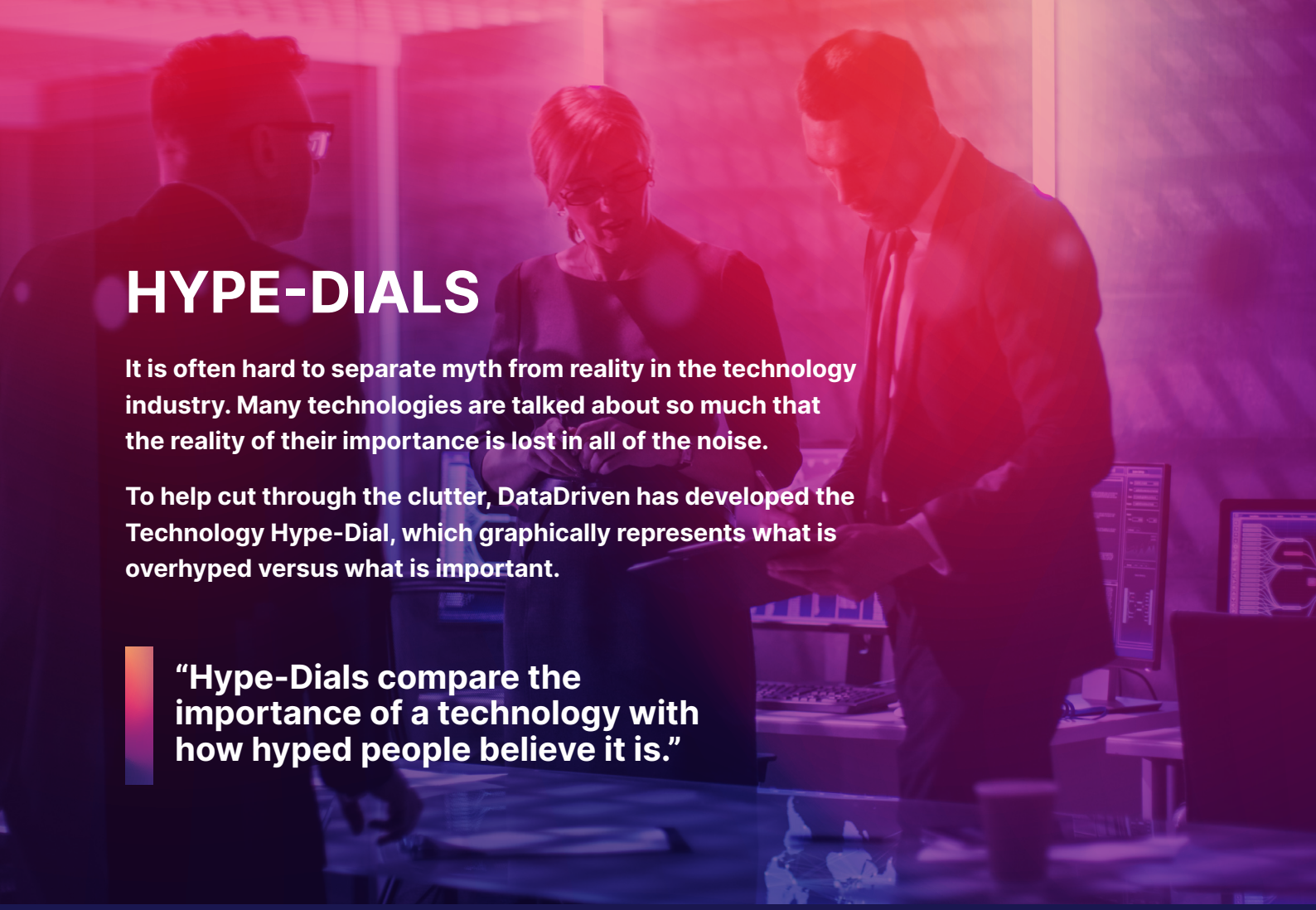
MARCH 7-9
Australian Cyber Conference - Canberra Edition
www.cyberconference.com.au

APRIL 29
BrisSEC - Brisbane
www.aisa.org.au

JUNE 22
CyberCon Connect - Sydney
www.cyberconconnect.com.au

OCTOBER 11-13
Australian Cyber Conference - Melbourne Edition
www.cyberconference.com.au

NOVEMBER 25
PerthSEC - Perth
www.aisa.org.au



HYPE-DIALS

It is often hard to separate myth from reality in the technology industry. Many technologies are talked about so much that the reality of their importance is lost in all of the noise.

To help cut through the clutter, DataDriven has developed the Technology Hype-Dial, which graphically represents what is overhyped versus what is important.

> **"Hype-Dials compare the importance of a technology with how hyped people believe it is."**

OVERHYPED OR UNDERHYPED? IMPORTANT OR NOT IMPORTANT?

As an integral part of the extensive research process, hundreds of ICT decision makers in specific markets were surveyed. We ask respondents to rate a number of technologies or business trends in terms of whether they believe them to be 'overhyped' or 'underhyped', and whether they are 'important' or 'not important'.

THE SHAPE OF THE DIAL INDICATES THE LEVEL OF PERCEPTION

Overall results are analysed and expressed as a four-point radar diagram for each technology or trend. The shape is reminiscent of an old style 'sun-dial'. The thinner the shape the more important ICT decision makers believe the technology to be. The higher the shape the more the technology is believed to be overhyped.

THE HYPE-DIAL EVALUATES TECHNOLOGY BASED ON MERIT

The Hype-Dial allows ICT decision makers to consider or reject a new technology or business trend based on its merits as identified by their peers. ICT decision makers evaluate the benefits of technologies in terms of their enablement of business and ICT objectives, which evolve over time, but which do not change nearly as quickly as technology.

TECHNOLOGY HYPE-DIALS

The DX Hype-Dial shows that a majority of respondents consider DX important, but a majority also believe it's somewhat over-hyped.

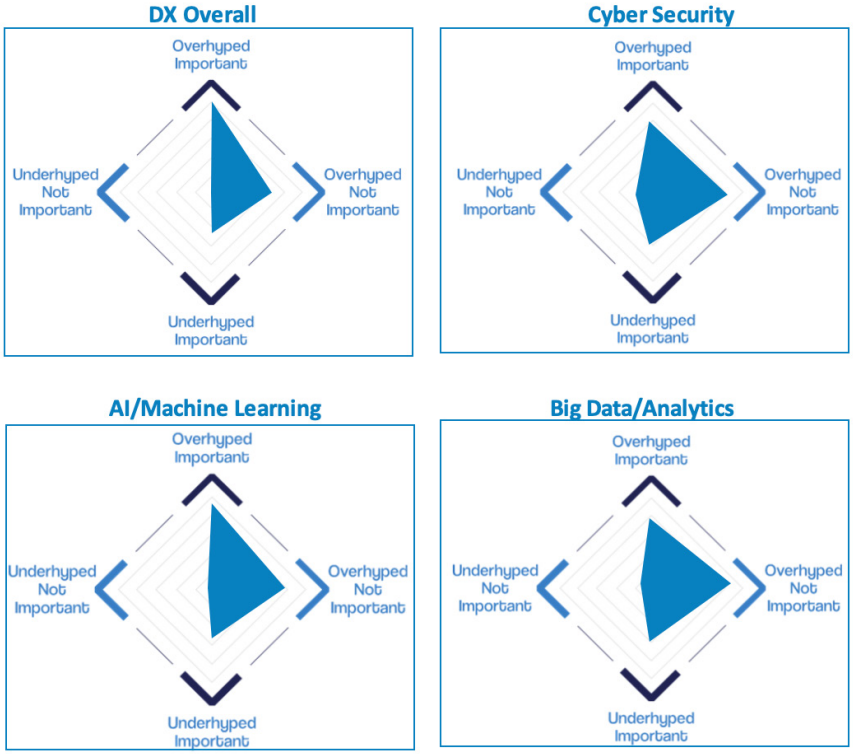
The cyber security Hype-Dial reveals a majority of respondents (54.3%) believe it is over-hyped. More respondents (44%) believe cyber security is important than unimportant (33%), with 23% expressing no opinion.

The 33% is a somewhat concerning finding, and in contrast to cyber security's prominent ranking in this study as a key business objective. It may also reflect increased confidence in some participants.

It's also possible that some respondents have got a bit of "security fatigue" given the repeated media reporting on security threats. In the 2020 study respondents did not believe cyber security was over-hyped and were almost unanimous that cyber security was important.

Big Data/Analytics is considered overhyped and has a similar profile to the cyber security Hype-Dial.

AI/Machine Learning is considered relatively more important, but a majority of respondents say it's overhyped



Technology Hype-Dials

The bottom line: many business leaders believe most technology is overhyped despite their acknowledgement that it is important.

"Cyber security professionals must communicate clearly and candidly about security threats but avoid overhyping the message."

CYBER SECURITY MATURITY

This section of the report examines the level of maturity of organisations' cyber security implementation in four separate areas of cyber security. Maturity levels are compared for online businesses versus traditional 'bricks and mortar' or offline operations.

"Online businesses usually have higher degrees of cyber maturity for cyber security products, services and backup than businesses that generate most of their revenues offline."

CYBER SECURITY MATURITY

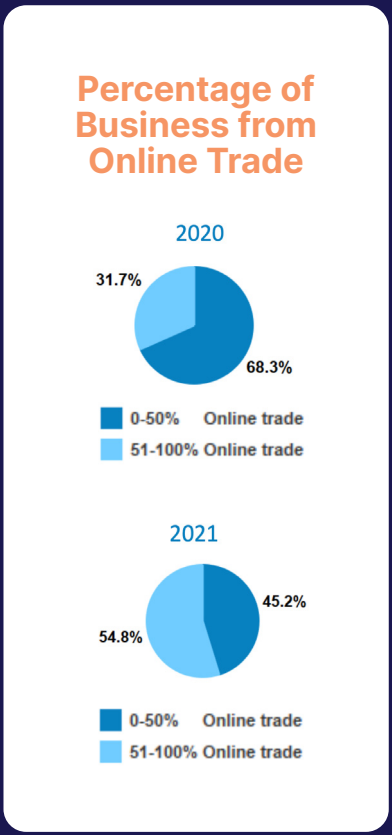
Maturity levels are examined for each of four separate areas:

- Cyber Security Ecosystem (general areas of security)
- Technology and Products
- Cyber Security Services
- Backup and Recovery.

Scores are expressed using a standard Capability Maturity Model as a rating between 0 ('not implemented at all') to 5 ('mature implementation').

Responses are compared for organisations which do more than half their business online, compared with those that do less than half of their business offline.

More than one-half (54.8%) of respondents work for organisations that generate more than 50% of their revenues online, and 45.2% work for organisations with less than 50% of revenues from online. This is significant growth compared to the 2020 survey where only 31.7% of respondents generated more than 50% of revenues from online trade and reflects the growth of ecommerce due to the restrictions imposed by COVID-19.



ECOSYSTEM MATURITY LEVEL

THE BIG PICTURE

The cyber security ecosystem refers to general areas of cyber security, rather than specific products. The elements in the chart are sorted from the highest maturity level (based on the combined responses from respondents with both >50% and <50% of their revenues generated online). That's also the score listed for 2020 and 2021 in the comparison table on the left of the chart.

The areas with the highest maturity levels are web security, cyber security of building infrastructure, and network security. Cloud security is also progressing in maturity and has leap-frogged data centre security in contrast to the 2020 study. This change reflects the ongoing migration of applications and workloads from on-premises to cloud infrastructure.

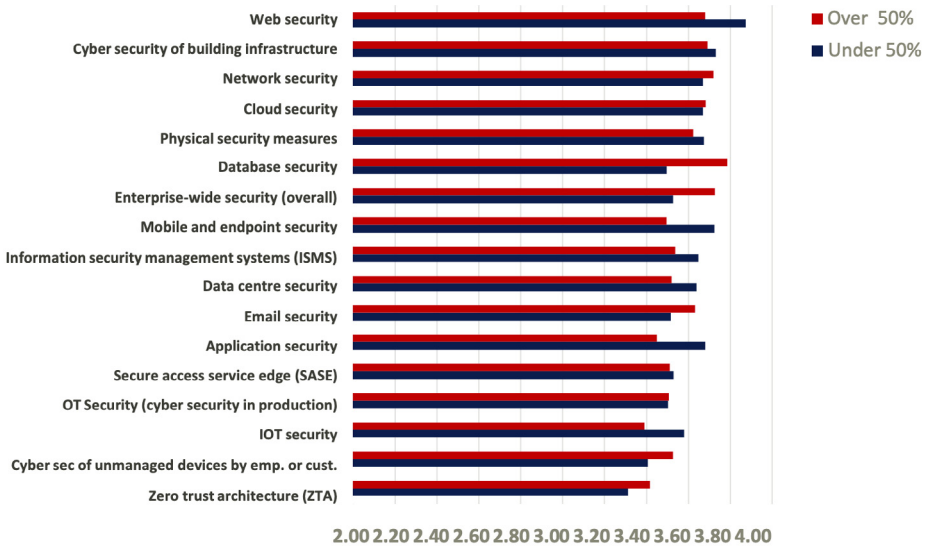
Zero Trust Architecture (ZTA) is the least mature ecosystem element, suggesting some businesses are lagging in moving away from legacy perimeter security approaches.

At this macro level of analysis, there is not much difference between the cyber maturity of businesses that transact most of their business online compared to those who do most business offline – in fact mostly-online businesses reported higher maturity in 8 out of the 17 categories we asked about. However, when we analyze maturity in more detail (in terms of products, services and backup as shown on the following 3 pages), the mostly-online businesses almost always report higher cyber maturity than their mostly-offline counterparts.

The bottom line: while businesses are clearly prioritizing security as a key objective this hasn't fully translated into sufficiently mature deployments. Further deployment is required in ZTA and authentication technologies.

Cyber security Ecosystem Maturity (Over 50% online vs under 50% online)

2020	Change	2021
3.48	↑	3.77
x	✖	3.71
3.55	↑	3.70
3.41	↑	3.68
x	✖	3.65
3.40	↑	3.66
3.25	↑	3.64
3.27	↑	3.60
x	✖	3.59
3.42	↑	3.58
3.66	↓	3.58
3.32	↑	3.56
x	✖	3.52
x	✖	3.51
3.00	↑	3.48
x	✖	3.47
x	✖	3.37



"Cloud security maturity is now ahead of data centre security maturity – the reverse of the 2020 study."

TECHNOLOGY AND PRODUCTS MATURITY LEVEL

CYBER SECURITY TECHNOLOGY AND PRODUCTS

Respondents have taken action to address some of the fastest growing security threats, with ransomware protection the most wisely deployed cyber security technology - equal with data encryption. Data encryption is especially prominent at businesses with the majority of sales online.

Blockchain is the third most mature cyber technology, becoming much more prominent compared to its 11th ranking in 2020. Blockchain's decentralised storage approach makes it much harder for hackers to access critical data.

Recently commercialised technologies like blockchain, AI and biometrics are increasingly being used to mitigate risk. At the same time, criminals are leveraging AI to automate and massively increase numbers of intrusion attempts.

It's surprising to see such an essential technology as authentication/identity management so far down the maturity scale, especially for businesses that transact a lot online.

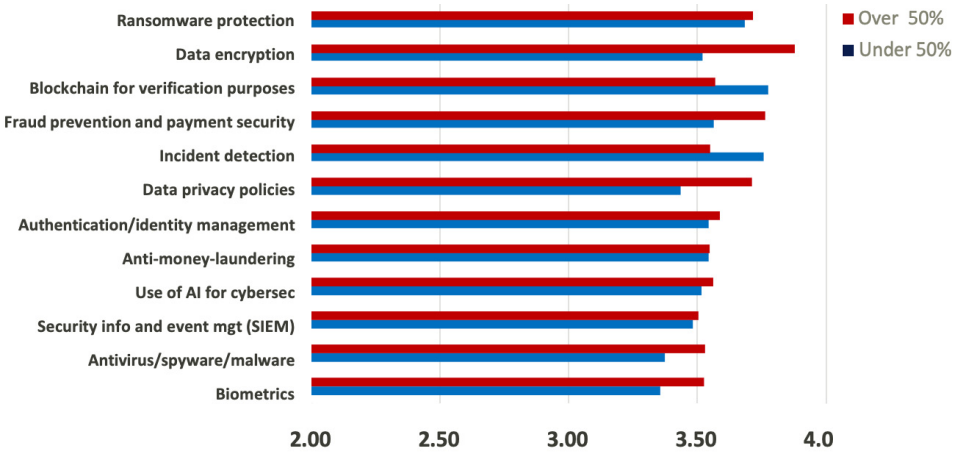
In 10 out of the 12 cyber security technologies we asked about, businesses that make most of their revenues online are more mature than those who make most of their revenues offline. The difference in maturity is most pronounced in data encryption, data privacy policies, and biometrics. The less-online businesses have more maturity for blockchain and incident detection response and recovery.

The bottom line: Online businesses are more mature in their use of cyber security technologies, especially data privacy, data encryption, fraud protection and payment security, malware detection, and biometrics.

> **"Businesses are taking action to address the growing threat of ransomware."**

Cyber security Technology and Products Maturity (Over 50% online vs under 50% online)

2020	Change	2021
x	✖	3.72
3.36	↑	3.72
2.76	↑	3.67
3.33	↑	3.68
3.13	↑	3.65
3.44	↑	3.59
3.04	↑	3.57
x	✖	3.55
2.83	↑	3.54
3.26	↑	3.50
3.63	↓	3.46
2.83	↑	3.45



SERVICES MATURITY LEVEL

CYBER SECURITY SERVICES

As cyber security changes and becomes more complex, businesses often need specialist help to assess and respond to risks. This has led to a proliferation of services across the security landscape, and businesses are significantly more advanced in using cyber security services now than was reported in our 2020 study. For all seven of the services we researched in both 2020 and 2021, the 2021 maturity levels are notably more advanced than in 2020.

In 8 out of the 9 services we asked about, businesses with a majority of their revenues from online are at a more mature stage in using cyber security services.

Under 50% online respondents say they're most advanced in using cyber security insurance services, followed by security analysis services. Cyber security insurance is the only service where businesses with lower online revenues are at a more mature stage – most likely because they feel more at risk due to having less mature cyber security technology and backup deployments.

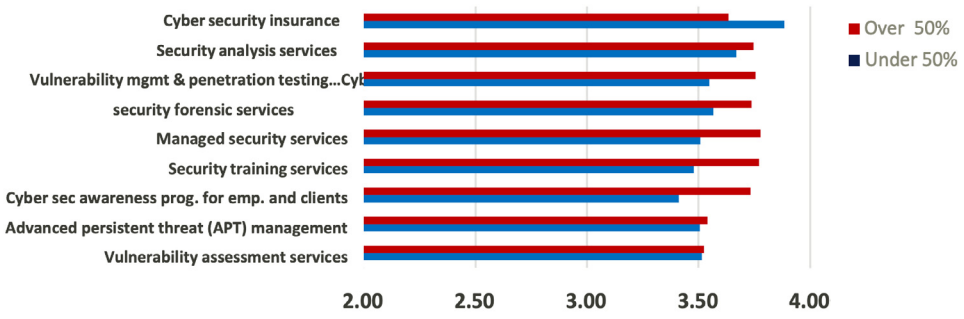
Cyber security awareness programs for employees and customers are increasing in maturity as respondents (especially those generating the bulk of revenues online) strive to enlist all their stakeholders in the task of recognising and thwarting threats. These programs are increasingly essential as it takes a whole organisation to fight security threats, including sophisticated spear-fishing attacks.

The bottom line: Businesses are stepping up their use of cyber security services to identify and mitigate risk, including human centric security.

> **"Businesses are significantly more mature in using cyber security services now than a year ago."**

Cyber security Services Maturity (Over 50% online vs under 50% online)

2020	Change	2021
3.10	⬆	3.75
3.17	⬆	3.71
3.03	⬆	3.66
2.99	⬆	3.66
3.33	⬆	3.66
3.15	⬆	3.64
x	✖	3.59
x	✖	3.53
2.98	⬆	3.52



BACKUP AND RECOVERY MATURITY LEVEL

BACKUP AND RECOVERY SERVICES

Backup and recovery have been important functions since the beginning of commercial computing. Best practice has changed over time as technology leaders took advantage of improvements in data storage technologies, especially in the move from tape to disk, and also through the massive cost improvement in storage technology over the past decade or so.

These technological and cost improvements have essentially enabled organisations to set more ambitious recovery point and recovery time objectives.

The most mature backup and recovery element is synchronous replication to backup site, which, in simultaneously writing data to production and backup storage directly enables an improved recovery point objective. This has become essential for mission-critical online commerce applications. Synchronous replication maturity score has increased substantially from 3.0 in 2020 to 3.71 in 2021.

Offsite backup/storage is in widespread use via: multiple redundant systems offsite; offsite storage; and cloud backup.

Businesses with a majority of their revenues from online are at a more mature stage in using backup and recovery for all 7 of the 7 capabilities we researched.

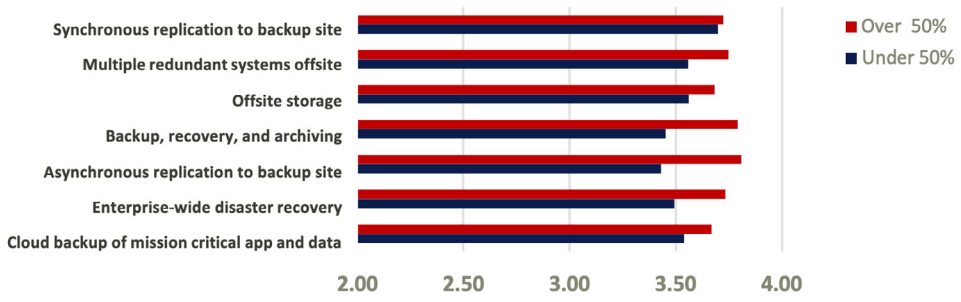
Businesses have progressed their backup and recovery maturity substantially compared to the result in the 2020 study. Ransomware may be the main motivator.

The bottom line: Businesses with mostly online revenues are at a more mature stage in using backup and recovery and ransomware may be propelling investments.

"Synchronous replication maturity has increased substantially from 2020 to 2021, improving resilience."

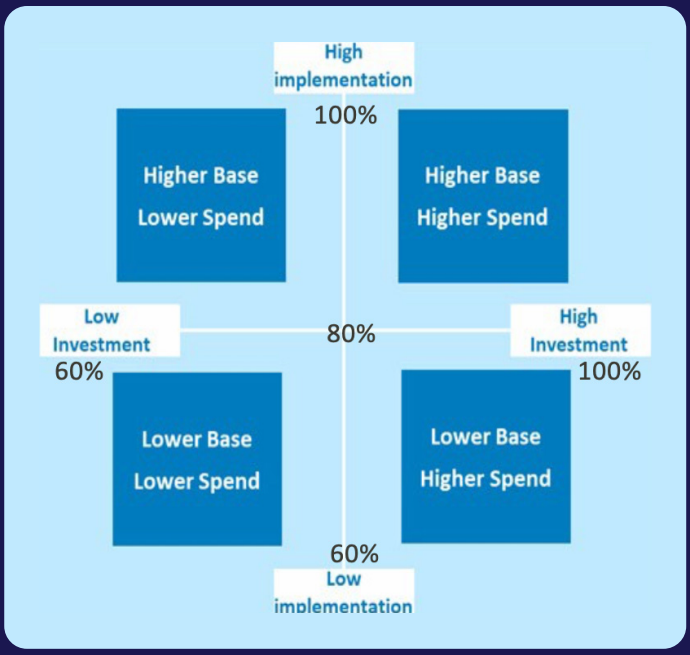
Backup and Recovery Maturity (Over 50% online vs under 50% online)

2020	Change	2021
3.00	⬆	3.71
3.05	⬆	3.66
3.23	⬆	3.63
3.50	⬆	3.64
2.87	⬆	3.64
3.06	⬆	3.62
3.25	⬆	3.61



CYBER SECURITY IMPLEMENTATION AND INVESTMENT

This section of the report examines the extent of organisations' cyber security implementation versus planned investment in four areas: ecosystem, technology and products, services, and backup and recovery.



"More than 73% of organisations are planning further investments in all areas of cyber security."

IMPLEMENTATION VS INVESTMENT MATRIX (I2M)

The I2M allows overall results to be analysed and expressed as a matrix which maps actual implementation (low to high) against planned investment (low to high). The positioning of technologies within the DataDriven I2M shows their status relative to each other and is not designed to reflect actual market shares.

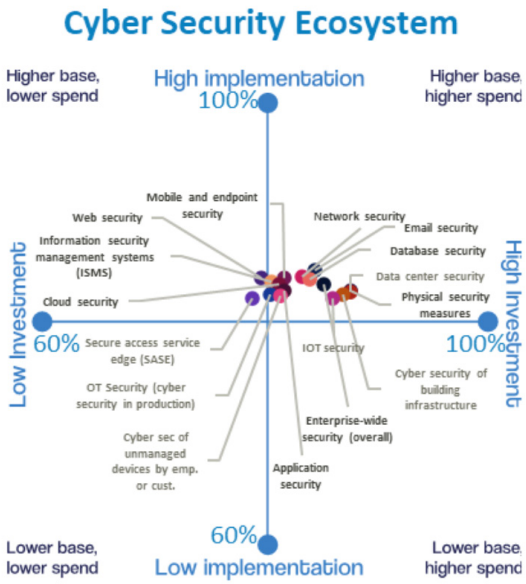
The axes scales start at 60% and go up to 100% of respondent organisations with the axes cross-point at 80%. That emphasises the widespread current deployment of cyber security capabilities (76% or more of respondents have deployed every one of the security capabilities we researched), and the strong planned investment (73% or more will invest across the board in cyber security).

IMPLEMENTATION VS INVESTMENT MATRIX (I2M)

CYBER SECURITY ECOSYSTEM

There is a high degree of both implementation and planned investment across all aspects of the cyber security ecosystem. Email security, network security and mobile and endpoint security have the widest current deployment – at 85% and above of respondents. The most common investments will be on data centre security, physical security measures, and cyber security of building infrastructure.

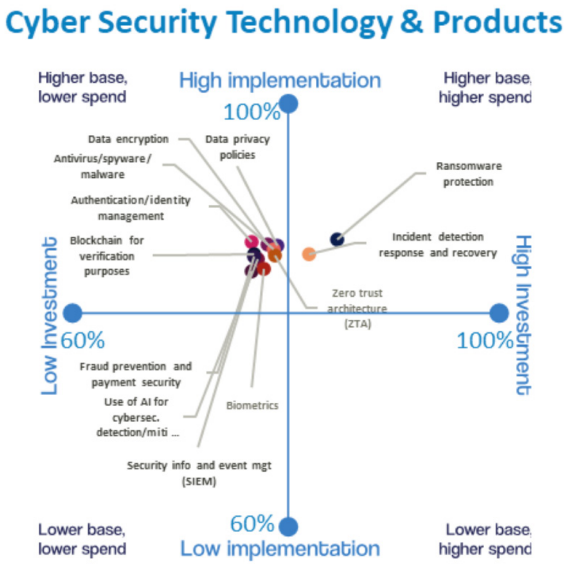
The bottom line: investment will continue across all aspects of cyber security, despite economic pressure.



CYBER SECURITY TECHNOLOGY AND PRODUCTS

Three-quarters or more of all respondents have already implemented all the cyber security technologies at some level. Ransomware protection is the most widely implemented technology and will also attract the heaviest investment over the next 12 months. Respondents are also investing heavily in incident detection, and zero trust architecture (ZTA).

The bottom line: Despite widespread deployment, businesses still need to invest more in cyber security to address the magnitude of the risk.



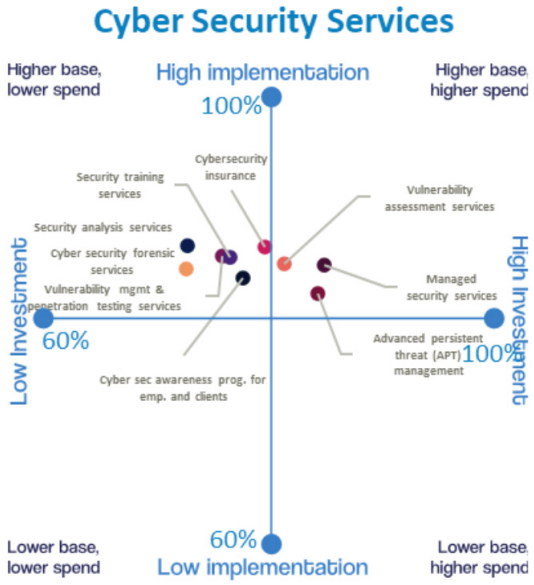
"More than three-quarters of organisations are planning further investments in cyber security."

IMPLEMENTATION VS INVESTMENT MATRIX (I2M)

CYBER SECURITY SERVICES

Usage of cyber security services is growing significantly due to the ever-increasing scale and complexity of the security landscape. Cyber security insurance and security analysis services are the most widely used services currently, while managed security services and advanced persistent threat (APT) management will attract the highest investment over the next 12 months.

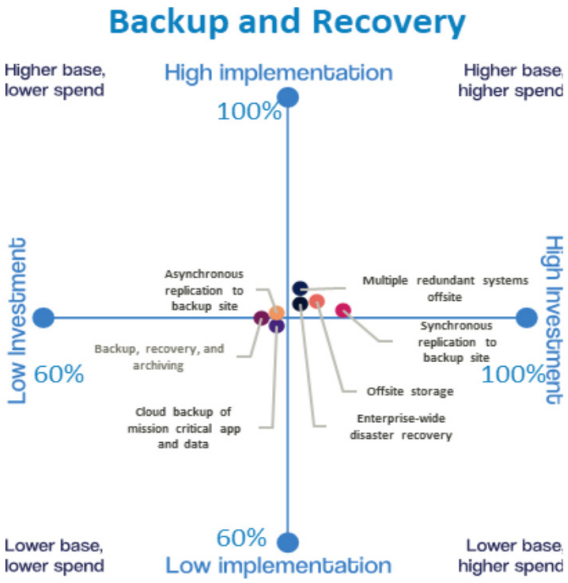
The bottom line: Managed security services will attract the highest investment over the next 12 months.



BACKUP AND RECOVERY

The level of planned investment in backup and recovery capabilities is around 10 to 15 percentage points higher in 2021 than it was in the 2020 study. Multiple redundant systems offsite and offsite storage are the most widely deployed capabilities while synchronous replication and offsite storage will attract the highest investment over the next 12 months.

The bottom line: Customer-facing commerce applications are spurring widespread implementation and continued investment in synchronous replication.



"Planned investment in backup and recovery capabilities is significantly higher in 2021 than it was in the 2020 study."

PROFILE OF AN ICT DECISION MAKER

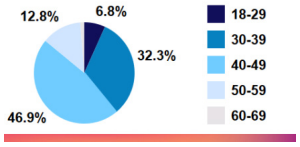
The survey asked a number of questions which enabled us to build a profile of Australia's ICT decision-makers. Most respondents to this survey are male, and mostly in their forties. However, they do span age groups and hold a diversity of views.

> **"Australian ICT decision-makers' sentiment about digital transformation is significantly more positive than in the 2020 study. It's likely that a year of living with COVID-19 has emphasised the positive aspects of DX"**

AGE

Almost one-half (46.9%) of respondents to the survey are in their 40s, and around one-third (32.3%) in their 30s. 12.8% are in their 50s, with 18-29 year-olds (6.8%) making up the numbers.

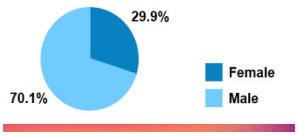
2021 Age



GENDER

The senior ranks of ICT are still largely populated by males. In this survey, 70.1% of respondents are male, an increase from 61.7% last year.

2021 Gender



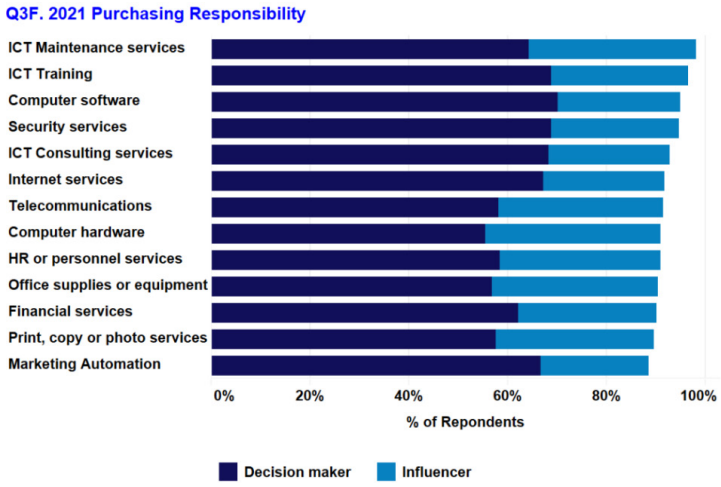
PROFILE OF AN ICT DECISION MAKER

PURCHASING RESPONSIBILITY

Australia's ICT leaders have wide responsibility for purchasing or influencing the purchase of all ICT products and services.

They have particular influence as decision-makers in software, ICT training, ICT consulting services, and internet services.

2021 Purchasing Responsibility

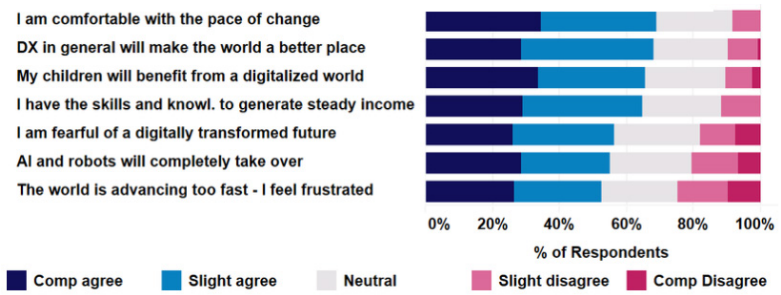


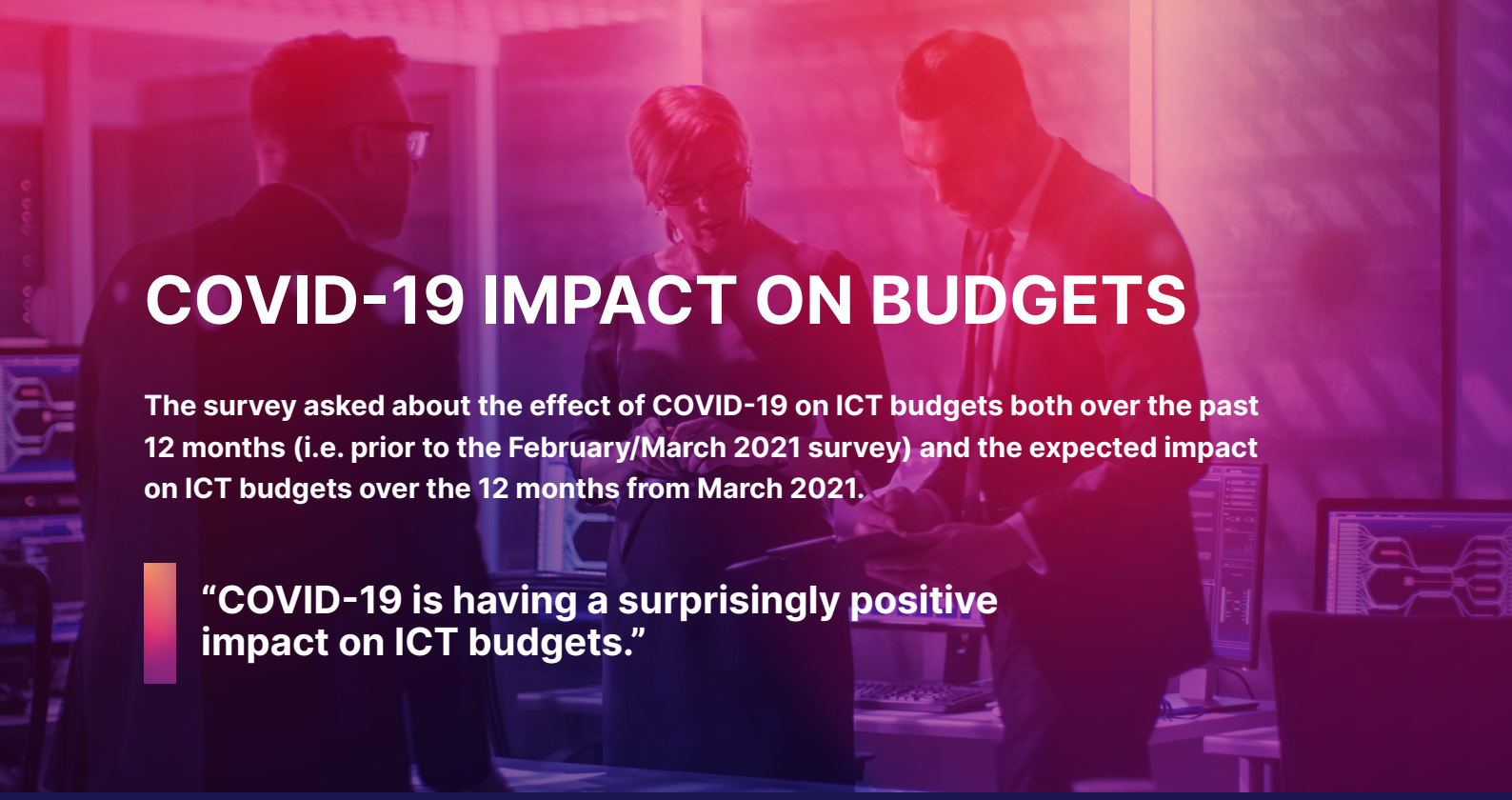
VIEWS ON TECHNOLOGY

ICT decision makers are broadly positive about the pace and impact of digital transformation, and their positive sentiment is significantly higher than in the 2020 study. It's likely that a year of living with COVID-19 has emphasised and accelerated the positive aspects of DX.

Almost 70% are comfortable with the pace of change and agree DX in general will make the world a better place, and a similar proportion expect their children to benefit from a digitalised world. Despite this, more than 50% say the world is advancing too fast and they feel frustrated, and a similar proportion is fearful of a digitally transformed future.

2021 IT Decision Maker Views on Impact of Technology on the Future





COVID-19 IMPACT ON BUDGETS

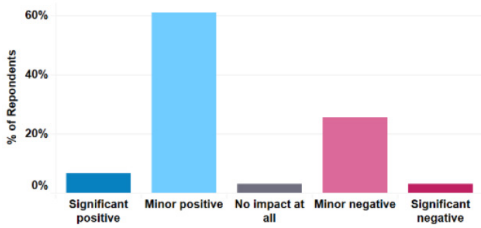
The survey asked about the effect of COVID-19 on ICT budgets both over the past 12 months (i.e. prior to the February/March 2021 survey) and the expected impact on ICT budgets over the 12 months from March 2021.

> **"COVID-19 is having a surprisingly positive impact on ICT budgets."**

COVID-19: IMPACT ON BUDGET OVER LAST 12 MONTHS

Perhaps surprisingly, close to two- thirds (61.4%) of respondents found COVID had a minor positive impact on their planned budget over the last 12 months. Around one-quarter said it had a minor negative impact. This was much more positive than expected (less than 15% in the 2020 study predicted a minor positive outcome).

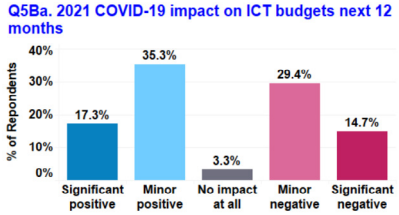
2021 COVID-19 Impact on ICT budgets over last 12 months



COVID-19: EXPECTED IMPACT ON BUDGET OVER NEXT 12 MONTHS

The majority of respondents believe COVID-19 will continue to have a net positive impact on budgets: 17% expect a significant positive impact and 35% a minor positive impact; 44% predict a negative impact.

2021 COVID-19 Impact on ICT budgets - Next 12 months



AI and IoT

Artificial intelligence (AI) and the Internet of Things (IoT) are two emerging technologies which have important ramifications for cyber security – AI as an aid to remediation (though it is extremely useful to attackers also), and IoT because of increased vulnerabilities at an ever-expanding edge.

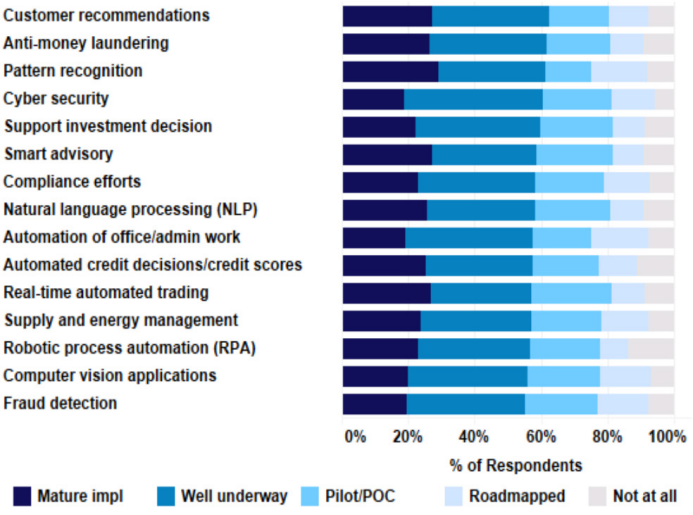
ARTIFICIAL INTELLIGENCE

The survey asked about the implementation of a range of AI-related tools and technologies. AI is most widely used for cyber security and related purposes such as anti-money laundering. AI has been talked about as a breakthrough technology for years, and although many organisations are now putting it to practical use, implementation is still in its infancy for around 30% to 40% of respondents.

The proportion of respondents deploying AI has increased markedly between 2020 and 2021 (for the five AI technologies we included in both surveys).

"New technologies such as AI and IoT are generally beneficial, particularly for authentication and cyber security"

2020	Change	2021	2021 Progress in AI Technologies or Initiatives
x	✖	62%	Customer recommendations
x	✖	62%	Anti-money laundering
38%	⬆	61%	Pattern recognition
41%	⬆	61%	Cyber security
x	✖	60%	Support investment decision
x	✖	58%	Smart advisory
x	✖	58%	Compliance efforts
32%	⬆	58%	Natural language processing (NLP)
37%	⬆	58%	Automation of office/admin work
x	✖	57%	Automated credit decisions/credit scores
x	✖	57%	Real-time automated trading
x	✖	57%	Supply and energy management
37%	⬆	57%	Robotic process automation (RPA)
x	✖	56%	Computer vision applications
x	✖	55%	Fraud detection



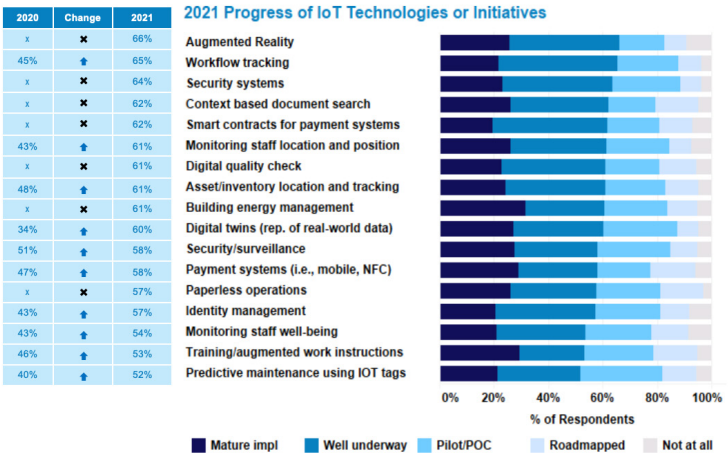
AI and IoT

INTERNET OF THINGS

The survey asked about the implementation of IoT technologies and applications. IoT is widely implemented in security systems (88% of respondents have a mature implementation, or one that's underway or at pilot stage) and in security/surveillance (also over 80%).

Other widespread uses of IoT are for workflow tracking, digital twins, and monitoring staff location and position.

2020	Change	2021
x	✖	66%
45%	⬆	65%
x	✖	64%
x	✖	62%
x	✖	62%
43%	⬆	61%
x	✖	61%
48%	⬆	61%
x	✖	61%
34%	⬆	60%
51%	⬆	58%
47%	⬆	58%
x	✖	57%
43%	⬆	57%
43%	⬆	54%
46%	⬆	53%
40%	⬆	52%



"The increasing use of IoT technology for surveillance, staff location tracking and monitoring staff well-being is likely to require delicate handling and negotiation by talent leaders."

SUPPLIER SATISFACTION AND PREFERENCES

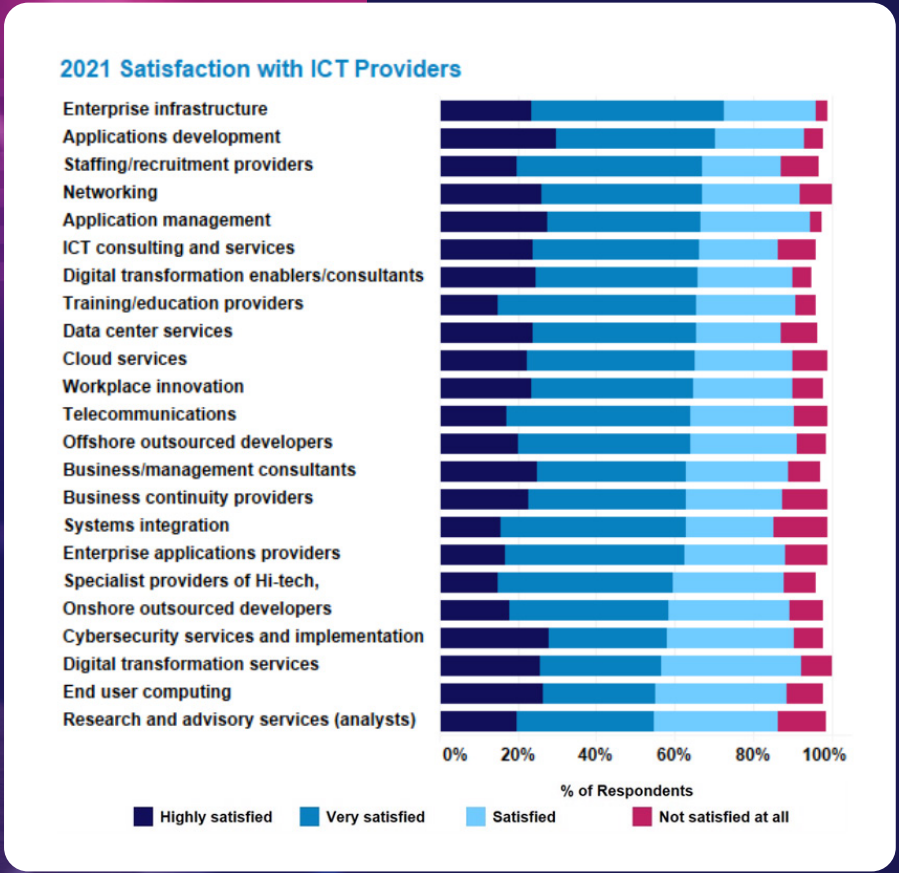
User organisations must deal with a multitude of suppliers, who compete fiercely for their attention and their business.

"ICT decision-makers in Australia are generally not as satisfied (although marginally so) with their cyber security suppliers than with most other providers."

LEVEL OF SATISFACTION

The survey asked about respondent's level of satisfaction with providers in a range of product and service areas. Providers are generally perceived to be doing a good job.

Enterprise infrastructure, applications development and recruitment providers have the highest levels of satisfaction followed by networking and application management providers. Around 60% of respondents are very or highly satisfied with cyber security services providers, but there's room for improvement given close to 10% are not satisfied at all.



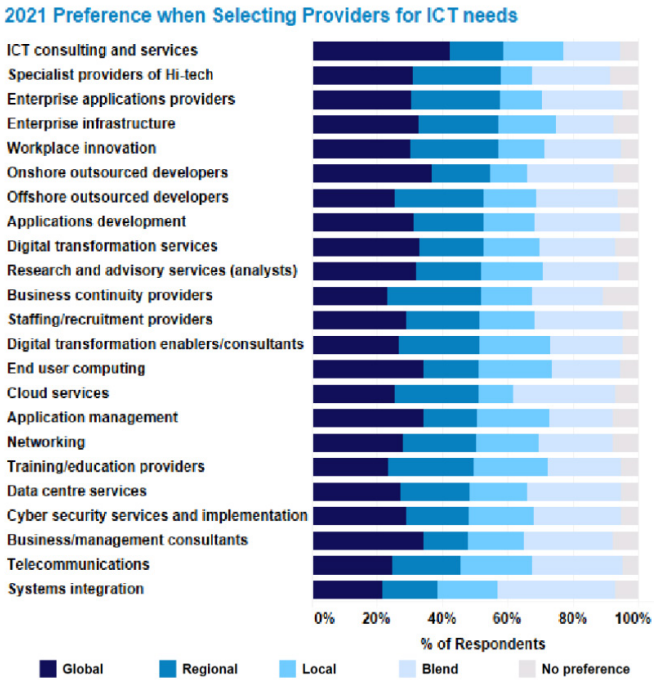
SUPPLIER SATISFACTION AND PREFERENCES

PREFERRED ORIGIN

The survey asked about respondents' preferred source of origin of a range of products and services: locally from Australia, from the Asia-Pacific region, or global, or whether they prefer a blend or have no preference.

Around 50% prefer their cyber security suppliers to be global or regional, around 20% prefer local suppliers and 25% prefer a blend.

"There is a preference for global or regional cyber security providers over their local counterparts."



THE CYBER SECURITY LANDSCAPE IN AUSTRALIA

Information systems security was once a specialised activity. Today it is central to all aspects of information processing.

Senior management in Australia is increasingly being involved in decision making around cyber security products and strategies, and is becoming much more interested in understanding cyber risks.

Increased publicity about and awareness of cyber attacks, and stricter regulations and legislation, are increasing maturity levels.

CYBER SECURITY IN AUSTRALIA

This section examines the specifics of cyber security in Australia – government initiatives, the components of cyber security, new technologies, the effects of the COVID-19 pandemic, and the emergence of the Zero Trust Architecture (ZTA).

"Cyber security is no longer an afterthought, something tacked on at the end. It is, or should be, an integral part of systems design and operation."

THE CYBER SECURITY LANDSCAPE IN AUSTRALIA – GOVERNMENT INITIATIVES

AUSTRALIAN GOVERNMENT INITIATIVES - 2014 TO EARLY 2020

A number of Australian Government initiatives have demonstrated the increased importance of cyber security to the country's economic infrastructure:

- In 2014 the Government established the Australian Cyber Security Centre (ACSC) within the Department of Defence's Australian Signals Directorate (ASD) to coordinate responses to cyber security incidents in government and business and to organise national cyber security operations and resources. It has been instrumental in raising awareness of the level of cyber threats to Australia. The ASD has developed the influential 'Essential Eight' cyber security mitigation strategies.
- In 2015 the Government announced a Critical Infrastructure Resilience Strategy to ensure the continued provision of essential services to businesses, governments and the community. The strategy is currently being reviewed for an update in 2021.
- In 2018 the strengthening of the Australian Privacy Act and Notifiable Data Breaches (NDB) made many enterprises much more aware of the need for compliance and data security. Many insurance companies are now demanding penetration test reports as a prerequisite for insuring against the consequences of cyber attacks.
- After the 2019 election the Government pledged $156 million to create jobs and provide training to the cyber security industry. The initiatives include the creation of a national cyber security workforce growth program ($50 million), new capabilities for countering foreign cyber crime ($40 million), further funding for the ACSC ($26 million) and funding for the Australian Defence Force to add over 200 new cyber warfare specialists over the next four years ($40 million).
- The Australian Cyber Security Strategy 2020 will invest $1.67 billion over 10 years to achieve its vision of creating a more secure online world for Australians, their businesses and the essential services upon which we all depend.
- The AustCyber and Australia's Cyber Security Sector Competitiveness Plan 2020 is intended to support a vibrant and competitive cyber security sector that generates increased investment and jobs for the Australian economy. According to the plan "Between 2017 and 2020, sector revenue has grown by A$800 million to A$3.6 billion across approximately 350 technology and service providers, who are supported by about 26,500 workers. Australia's economy is digitising and the cyber security sector must be capable of meeting its protection needs."

There have also been a number of significant investments in digital and cyber security at the state level, with NSW, Victoria, Queensland and Western Australia releasing cyber security strategies.

"Cyber security has become a significant issue for government."

THE CYBER SECURITY LANDSCAPE IN AUSTRALIA – RECENT GOVERNMENT INITIATIVES

AUSTRALIAN GOVERNMENT INITIATIVES – THE LAST 18 MONTHS

A lot of water has flowed under the bridge since the 2020 edition of this study. Security threats are growing, many organisations - especially small and medium businesses (SMBs) - continue to be less well protected than they should be, and the Australian Government has continued to review and develop policy and legislation for cyber security. Significant events include:

- One thing is clear – attacks are growing. In September 2021, The Australian Cyber Security Centre (ACSC) released its annual ACSC Annual Cyber Threat Report, revealing: "the ACSC received over 67,500 cybercrime reports over the last financial year - or one every eight minutes. This is an increase of nearly 13 per cent from the previous year."
- Back in November 2020 the ACSC also released the Cyber Security and Australian Small Business Report which surveyed 1763 SMBs and revealed some hard truths:
  - almost half of SMBs rated their cyber security understanding as 'average' or 'below average' and had poor cyber security practices
  - almost half reported they spent less than $500 on cyber security per year
  - 62% of respondents admitted experiencing a cyber security incident.
- With this growing threat landscape, the Australian Government has released a number of reviews and proposed changes to security regulation over the past 18 months. The frequency of reviews and updates is critical due to the fast- changing nature of the threats, while the number of government departments involved shows how security cuts across all aspects of life in this country.
- The Australian Information Security Association (AISA) has been conspicuous in submitting recommendations to government consultation processes, representing the views of its 7,500-plus members as well as drawing on feedback from member research studies. Some of the more prominent initiatives are listed below.
- The Australian Government's Attorney-General's Department announced a review of the Privacy Act 1988 as part of the government's response to the Australian Competition and Consumer Commission's Digital Platforms Inquiry. The review was announced in December 2019 with a submission deadline in November 2020. AISA contributed a detailed submission, calling among other recommendations for the review "to ensure privacy settings empower consumers, protect their data and best serve the Australian economy."

"The frequency of Australian Government security initiatives is essential due to the fast-changing nature of the threats, while the number of government departments involved shows how security cuts across all aspects of life in this country."

AUSTRALIAN GOVERNMENT INITIATIVES – THE LAST 18 MONTHS (CONT'D)

- In March 2020 the Treasury Department announced an inquiry into future directions for the Consumer Data Right which "gives customers, including individuals and business customers, the right to safely access certain data about them held by businesses, and direct that their information be transferred to accredited, trusted third parties of their choice." The Australian Government is slated to invest AU$111 million of the Digital Economy Budget 2021-2022 on the Consumer Data Right initiative over the next two years

- Treasury envisages the Consumer Data Right initiative can lead to consumer benefits such as – hypothetically "bringing together the consumer's data from their service providers across a number of sectors (including banking, energy and telecommunications), this business could give the consumer a single up-to-date dashboard of all of their products, contracts, and plans, including the cost and time remaining on each, account balances and bill due dates, and alert them in real time when better deals become available." The initiative is being rolled out sector by sector starting with the banking sector (underway) and followed soon by the energy and telecommunications sectors.

- In November 2020, the Australian Government's Department of Home Affairs released the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 for consultation. The proposed amendments to the Security of Critical Infrastructure Act 2018 place security obligations and potential penalties on 11 designated critical infrastructure sectors (CIS). AISA submitted views to the Department of Home Affairs on this draft amendment. In October, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) tabled an advisory report calling for the legislation to be split in two to allow for some of the most urgent new powers to be passed quickly in the coming Spring sittings and for the government to further consult with industry on the other aspects of the legislation before introducing it to Parliament in a separate bill.

- The Department of Infrastructure, Transport, Regional Development and Communications published the Exposure Draft for the proposed Online Safety Bill in December 2020. The intention is to build on the Enhancing Online Safety Act 2015 by beefing up protections against cyber-abuse, cyber-bullying and improper use or sharing of online "intimate images" and other content.

- In June 2021 the Australian Government's Digital Transformation Agency (DTA) published a Position Paper in relation to the Trusted Digital Identity Framework (TDIF) and associated legislation. One of the aims of the legislation is to govern how state and territory governments and the private sector will be accredited under TDIF. As per our submission, one of the reasons the TDIF is acceptable is that it does not require a single identity. This is absolutely critical for civil liberties, freedom, privacy and to avoid creating a single Digital God who has digital life and death power. Further that strong legislative support and enforcement of TDIF is vital if the system is to be sufficiently trustworthy.

- In July 2021, the Australian Government's Department of Home Affairs opened consultation on options for strengthening Australia's cyber security regulations and incentives. AISA provided a 39-page submission with feedback based partly on a recent member survey. Based on the findings coupled with the detailed comments received from directors and business executives, AISA proposed the five key principles be adopted by Government as it considers policy and regulatory reforms in relation to cyber security in Australia.

- AISA also released a joint statement with AustCyber in September 2021 to help inform policy development in strengthening Australia's cyber security regulations and incentives. The statement is based on an AISA survey of Directors of listed and non-listed Australian companies, as well as public institutions, NGOs, cyber professionals and executives across an audience of over 7,000 individuals. The statement outlines a number of common principles intended to assist decision-makers.

THE CYBER SECURITY LANDSCAPE IN AUSTRALIA – COMPONENTS

END-USER, ENDPOINT AND MOBILITY PROTECTION

End user protection systems guard against malware, viruses, spyware, trojan horses and the like at the individual user level. They are typically point products that can be employed by individual users, but which are also integrated into enterprise cyber security solutions.

This includes mobile security. Smart phones and other mobile devices are often the preferred interface to many corporate systems. Most endpoint security systems now include mobile cyber security functionality. End user applications also need to be secured, particularly those used for collaboration. This includes email workflow, and workplace applications.

IDENTITY AND ACCESS MANAGEMENT

Identity management systems straddle a range of technologies intended to ensure that only validated individuals have access to the appropriate levels of information. They are often now being implemented at the national level with the increasing popularity of e-government systems.

Many identity management systems include a biometric component, using voice or facial recognition, fingerprints and other distinctive physical attributes to verify and identify individuals.

Pending legislation to enforce the Trusted Digital Identity Framework seeks to facilitate more trustworthy exchange. For the TDIF to survive and thrive, legislative backing is a must. A strong legal framework and related technologies to protect the users is critical for a trusted and trustworthy system.

"The rise of identity solutions will result in many challenges to privacy."

THE CYBER SECURITY LANDSCAPE IN AUSTRALIA

– COMPONENTS (CONTINUED)

SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT)

SIEM techniques and technologies are employed to ensure that enterprise information systems are secured from outside interference. SIEM systems are one of the fastest growing product area in cyber security. They have three major components:

- Data collection: Gathering data about system activity from syslogs, firewalls, application monitors, and operating system and network traffic logs.
- Data analysis: Log management and retention, event correlation, user activity monitoring, and predictive and forensic analysis.
- Reporting: Real-time dashboard alerts, email and SMS with alerts, analytical reporting, auditing and governance, and compliance.

VULNERABILITY MANAGEMENT

Vulnerability management is an important class of cyber security tools and are designed to assess an organisation's vulnerability to cyber attacks. These tools and services include penetration testing and vulnerability assessment, and often include remediation capabilities.

"There is a movement away from point products and towards integrated solutions."

THE CYBER SECURITY LANDSCAPE IN AUSTRALIA – COMPONENTS (CONTINUED)

DATA CENTRE AND CLOUD SECURITY

The disciplines of data centre security have now been extended to the cloud. Most organisations operate a hybrid environment of in-house and cloud processing. It is important for the whole processing ecosystem to be treated as a single environment for security purposes.

Cloud data centre service providers have in most cases implemented sophisticated security practices, but the ultimate responsibility remains with the user.

DATA ENCRYPTION

Encryption provides an extra level of security and has become a major product set in its own right. Encryption ensures that even if an intruder breaches an organisation's security systems, they are unable to use information because it is coded. Encryption and decryption tools have become a significant industry sector.

CYBER SECURITY SERVICES

Many vendors offer specialised cyber security services. Some suppliers offer a total solution, from endpoint security to SIEM to disaster recovery and forensic and analysis services. This often includes a specialised Security Operations Centre (SOC), which monitors and manages cyber defences on behalf of clients. There is also a large specialist cyber security training industry.

NEW TECHNOLOGIES

New technologies are constantly changing the cyber security landscape, posing new threats and leading to the development of new products and strategies.

Important technologies to the future of cyber security include:

- Blockchain: a technology that provides an unalterable audit trail for data. It is increasingly being used in the financial services industry to provide secure transactional systems, though it comes at a cost in performance. Blockchain brings its own cyber security challenges.
- Artificial intelligence: Covers a range of technologies including machine learning, predictive analytics, pattern matching and behavioural mapping. But AI is also an enabler for hackers and cyber criminals.
- Internet of Things: IoT massively increases the number of endpoints in any network, leading to a new class of cyber security products.
- Biometrics: Technologies such as facial and fingerprint recognition are now being widely implemented, starting with smart phones.

"New technologies will drive a significant new wave of challenges and opportunities for cyber crime."

THE CYBER SECURITY LANDSCAPE IN AUSTRALIA – THE COVID-19 PANDEMIC

THE COVID-10 PANDEMIC

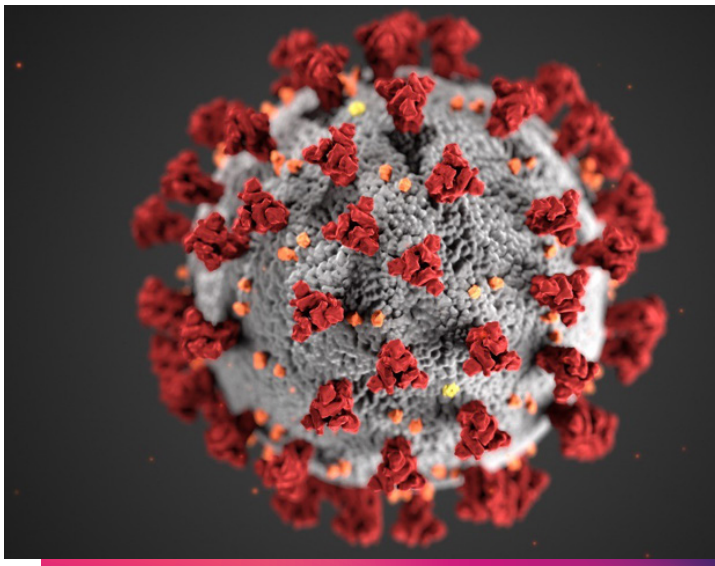
The impact of the virus itself on Australia was slight by international standards, but the economic consequences of lengthy lockdowns in both 2020 and 2021 are severe and will be felt for years to come.

Many Australian organisations accelerated their implementation of cyber security measures because of the consequences of the COVID-19 lockdown. In particular, the much greater numbers of employees working from home led to significant increases in cyber attacks. This is a permanent change and is having a significant effect on the cyber security landscape.

COVID-19 has mostly accelerated IT budget increases. Over two-thirds of respondents said COVID-19 had a minor positive impact on their planned budget over the last 12 months. The majority of respondents believe COVID-19 will continue to have a net positive impact on budgets over the next 12 months (from March 2021).

With the vastly increased numbers of remote workers, the number of pain points and vulnerabilities has proliferated in most corporate networks. This makes it easier for hackers and criminals to breach the perimeter. In recent years an increased number of these attacks are coming from nation states or cyber criminal groups sponsored by them.

Enterprises need to implement much more stringent systems and codes of practice than was the case in the past. The most important aspect of this strategy is building a security culture across the entire organisation, and deploying appropriate defences to protect devices of all the workers now working from anywhere.



"With the vastly increased numbers of remote workers, the number of pain points and vulnerabilities has proliferated in most corporate networks.

THE CYBER SECURITY LANDSCAPE IN AUSTRALIA – ZERO TRUST ARCHITECTURE

INVERTING THE ONUS OF TRUST

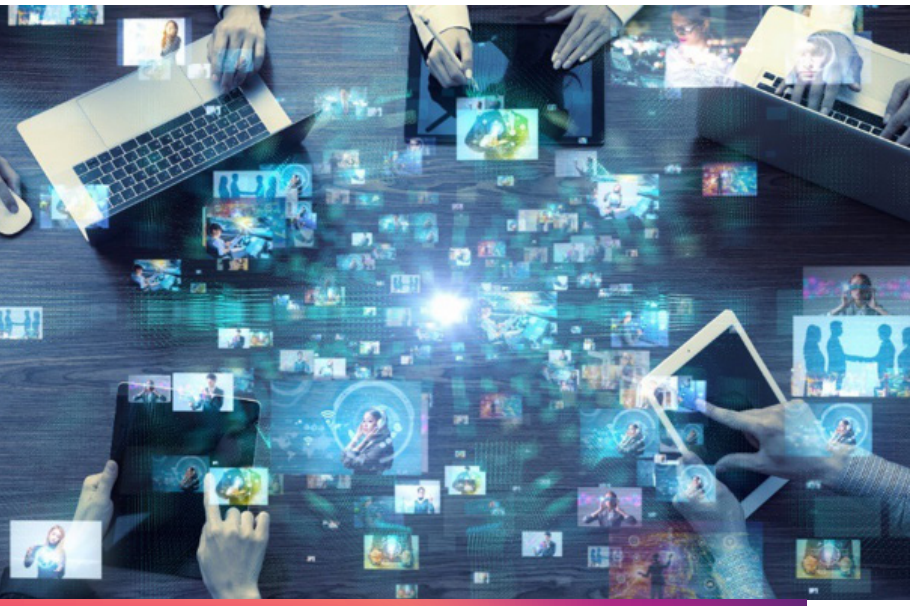
A ZTA, as the name suggests, means that no component of a corporate network is automatically trusted, and that every access by every component must be verified. This is a very different concept to the traditional paradigm of perimeter security.

With a ZTA, the old concept of 'trust and verify' is replaced with the new concept of 'never trust and always verify'. There is no longer a perimeter within which transactions are trusted and which acts as a barrier against attacks. A ZTA is enabled by the verification of the user's identity, at every stage. No user is trusted by default. Verification is required at every step. This makes it much easier to track any attempted intrusion.

There is no standard method for implementing a Zero Trust Architecture. There are many products and services that enable a ZTA to be built. But any ZTA is built around three fundamental levels of verification: the verification of the identity of the user, the verification of the user's device, and the verification of the user's access privileges. There are various methods for verifying and authenticating the user's access.

These include encryption, behavioural profiling, and two factor or multifactor authentication.

In August 2020 the National Institute of Standards and Technology (NIST), part of the US Department of Commerce, published a detailed overview of the core logical components that make up a ZTA network strategy. The goal of a ZTA enabled system, says the report, should be to prevent unauthorised access to data and services, coupled with making the access control enforcement as granular as possible. Authorised users, applications, services or devices can access other components of the network to the exclusion of all other subjects.



"ZTAs are just beginning to be implemented in Australia. Look for increased hype and investment in 2021."

CONCLUSIONS

Cyber security is an arms race, a constant evolution of threats and counter-measures. Criminal gangs and hostile foreign nations with substantial resources and ingenuity keep finding new ways to attack businesses in Australia and elsewhere.

Given the growing cyber security threat, Australian business must evolve their defences against attacks.

Those best equipped to meet the challenges will be those with a risk management and security strategy backed and funded by the board, and who can inculcate a strong security culture throughout their organisations.

"Board backing and funding of security strategy is the starting point for building the defences and counter measures needed to contain cyber threats."

BUSINESSES TAKE CYBER SECURITY SERIOUSLY, HAVE INCREASED SECURITY DEPLOYMENTS AND PLAN FURTHER INVESTMENTS

The report comprises primary research based on the views of the people at the front line of the purchase and usage of cyber security technology – Australia's ICT decision makers.

The study shows Australian ICT leaders grasp the magnitude of current threats and take security very seriously. They are treating cyber security as a priority for the whole business, not just for ICT.

Managing risk and security issues is among the top three business objectives – right up there as a priority with increasing productivity and collaboration, and increasing competitive advantage.

Respondents readily acknowledge the scale of the security challenge: eight of their top ten ICT strategic challenges have to do with security, the top 3 being application security, network security and regulatory compliance.

Some of the significant changes from the 2020 study include:

- Cloud security maturity is now ahead of data centre security maturity – the reverse of the 2020 study – as the migration from on-premises to cloud continues.
- Businesses are making additional investment to address the growing threat of ransomware.
- Businesses are also significantly more likely to use cyber security services now than a year ago.

Businesses have substantially increased deployment of security technologies, services and backup capabilities over the past 12 months, and they are ramping up their security investments heavily over the next 12 months to further protect and secure their infrastructure and assets. This is encouraging news given the continued rise in security incidents over the past year.

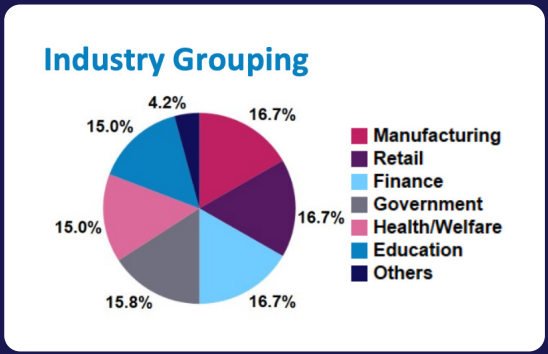
DEMOGRAPHICS

Over 1,000 potential respondents were contacted, with the aim of identifying 120 key ICT Decision makers.

DataDriven applied seven levels of exhaustive screening and validation questions, then conducted extensive data scrubbing and removal of non-representative data and outliers using research analytics tool SPSS. The result is a highly qualified and reliable set of complete responses.

RESPONDENTS BY INDUSTRY

Six broad industry verticals are represented: Manufacturing (16.7%), Retail (16.7%), Finance (16.7%), Government (15.8%), Health and Welfare (15.0%), Education (15.0%) plus 'Other' (4.2%).



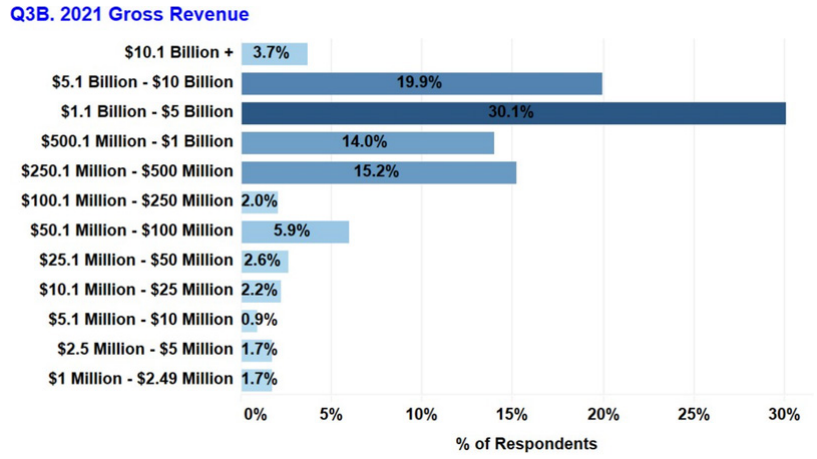
"The respondent base is very representative of Australia's ICT decision makers."


AISA

BY REVENUES AND EMPLOYEES

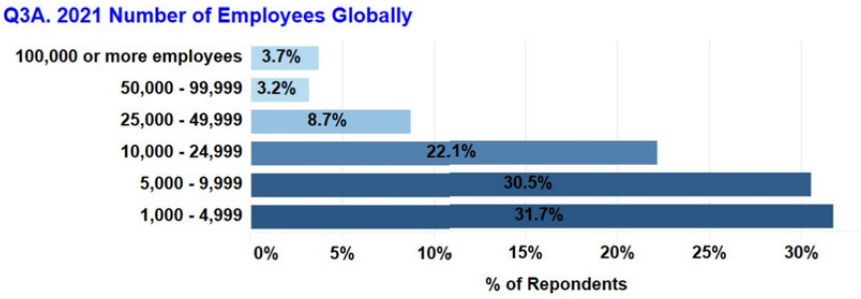
RESPONDENTS BY GROSS REVENUE IN AUSTRALIA

Respondents come from all sizes of organisation. Two metrics were collected: annual gross revenue and number of employees. Over 80% work in organisations with $250 million or more in revenues. More than one in five (23.8%) work in organisations with over $5.1 billion in revenues, and 30.1% work for organisations with between $1.1 billion and $5 billion in revenues.



RESPONDENTS BY NUMBER OF EMPLOYEES GLOBALLY

More than one-third of respondents (36.7%) work for organisations with 10,000 employees or above. Approximately one-third work at businesses with between 5,000 and 9,999 staff and a similar proportion work at organisations boasting between 1,000 and 4,999 staff.



"More than one-half work for organisations with over $1 billion in revenues."

RESEARCH FRAMEWORK, METHODOLOGY AND APPROACH

DataDriven has developed a proprietary taxonomy of technologies and trends to ensure consistency of terminology. The DataDriven Digital Transformation Technology Matrix (DXTM) provides a comprehensive model for our research focus and survey design, and ensures consistency of approach.

Five user groups are analysed at the levels of:

- Individuals
- Workplace
- Intra-Enterprise
- Extra-Enterprise
- Society as a whole

Then four application or technology areas are overlaid on this analysis:

- Artificial Intelligence and Machine Learning
- Cyber security
- Productivity: and Collaboration
- Platforms & Connectivity

Additional overlays for Sustainability/ CSR Initiatives and specific Industry Sectors are also applied for more granular analysis.

THOUGHT LEADERSHIP BASED ON FACTS ELICITED FROM DECISION MAKERS

DataDriven's unique methodology enables us to clearly and consistently identify key technologies and the groups they affect. We discover the trends in each area through primary research – comprehensive and intensive large-scale surveys of IT decision makers across major industry sectors and geographic markets.

Extensive demographic grouping and analysis based on the DXTM framework allows us to measure and compare the effect of each technology in each industry sector and also to compare their impact across different sizes of organization and different markets. Primary research of this nature is based on what the users of the technology are thinking and doing.

This quantitative analysis is complemented by qualitative research based on interviews with key players in the user, vendor, industry and government communities and secondary research from reputable and peer reviewed sources.

Our research is based on **highly reliable and valid facts** ... not opinion. Our proven methodology offers insights simply not available with secondary research.

It **is the users of technology** that ultimately determine the success and speed of its implementation. When predicting futures there is no substitute for asking the users of the technology about their attitudes, behaviours and intentions.

"The users of technology are the final arbiters and the ultimate source of truth for understanding the global ICT market."

CYBER SECURITY IN AUSTRALIA 2021

HOW TO CONTACT US

ACKNOWLEDGEMENT TO ICT DECISON MAKERS

AISA and DataDriven would like to thank the many hundreds of people and organisations involved in the production of this report. We would particularly like to thank the ICT decision makers/CIOs and senior ICT managers who responded to the survey upon which it is based.

ABOUT THE AISA

The AISA champions the development of a robust information security sector by building the capacity of professionals in Australia and advancing the cyber security and safety of the Australian public as well as businesses and government. Established in 1999, AISA has become the recognised authority on information security in Australia with a membership of over 7500 individuals and strategic, corporate and training partners and sponsors across the country and globally. For more information, please see www.aisa.org.au or email info@aisa.org.au

ABOUT DATADRIVEN

DataDriven is an Australian based global research and advisory services company specialising in ICT strategy for technology users and providers, research-based thought leadership, market and competitive intelligence, and marketing and technology strategy consulting projects. In addition, DataDriven associates are skilled at the delivery of presentations at events ranging from facilitation of small C-level roundtables, through to 'big-tent' major keynotes with audiences in the thousands. For more information, please see www.datadrivenservices.com.au

COPYRIGHT INFORMATIION

AISA Australian Information Security Association

Data Driven
RESEARCH | INSIGHTS | STRATEGY
THOUGHT LEADERSHIP | MARKETING

datadrivenservices.com.au