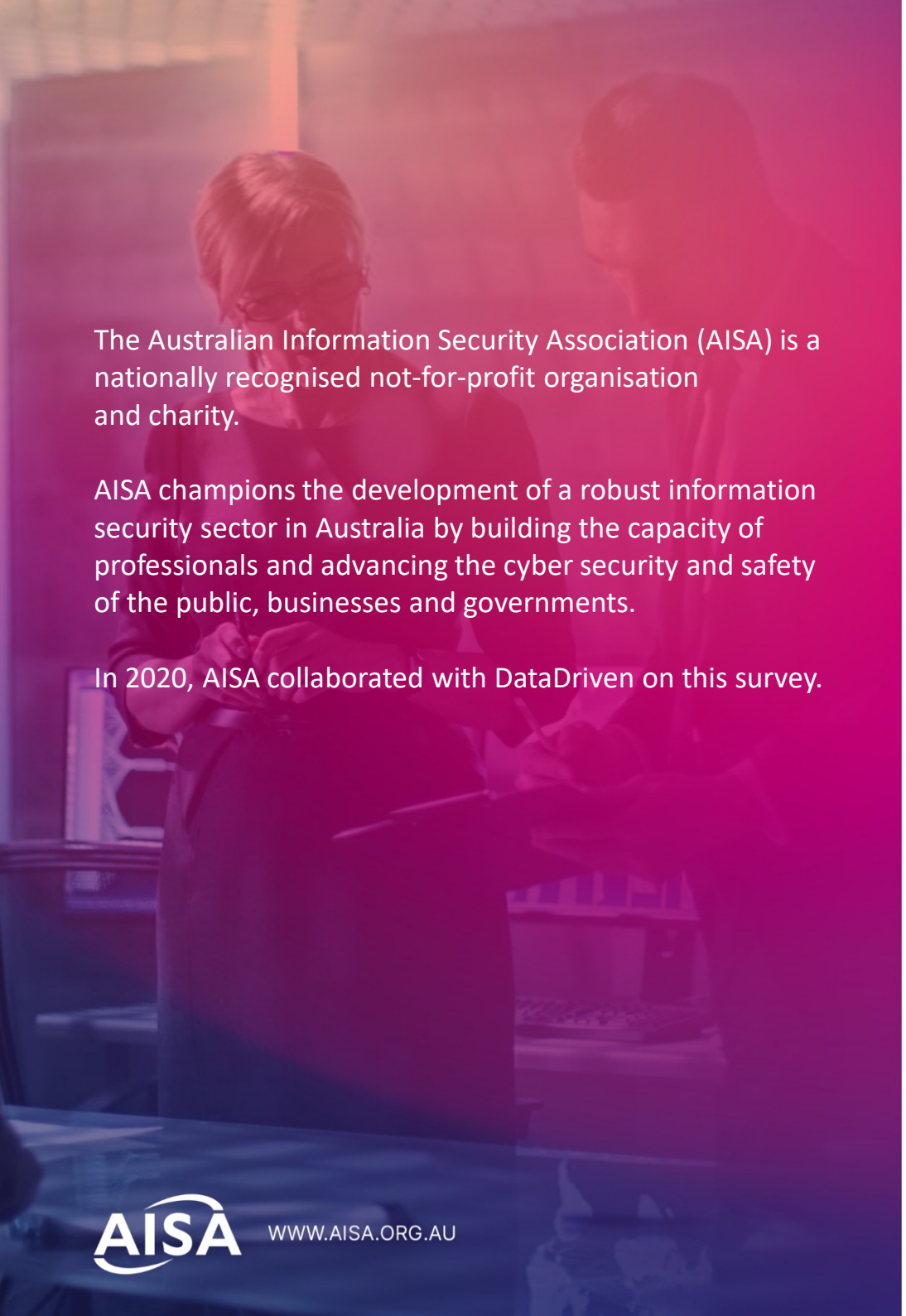
STATE OF THE DIGITAL NATION:

CYBER SECURITY IN AUSTRALIA 2020

AISA



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 2020, AISA collaborated with DataDriven on this survey.

AISA WWW.AISA.ORG.AU

TABLE OF CONTENTS

FOREWORD

STATE OF THE DIGITAL NATION: CYBER SECURITY IN AUSTRALIA 2020

To add value to our members and partners ongoing understanding of cyber security, AISA has partnered with research company DataDriven for this survey of 125 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 – that the hype around cyber security seems to be aligned to its importance for decision makers. Members may find this to be encouraging.

This survey was conducted just as the COVID-19 pandemic was taking hold in Australia. 2020 has been a dramatic year of change. Meeting the cyber security and business continuity needs of your organisation is critical, but the rapidly changing and increasingly dangerous security environment has increased the challenges for today's ICT decision maker.

Fortunately, the range of cyber security offerings and related services also continues to increase at a similar rate, 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 2020.

With 2020 behind us, we look forward to a better 2021.

.

MICHAEL TROVATO, DIRECTOR
Australian Information Security Association

DAMIEN MANUEL, CHAIR
Australian Information Security Association

INTRODUCTION AND KEY FINDINGS

After the COVID-19 pandemic hit Australia in February 2020, DataDriven conducted an extensive survey of ICT leaders about their organisation's Digital Transformation (DX) and ICT practices. Seven levels of selection, screening and validation questions were applied data scrubbing and removal of non-representative data and outliers was completed.

The result is a highly qualified and reliable study based on responses from Australian ICT decision makers, with a strong focus on cyber security. Subsequently AISA collaborated with DataDriven to provide this focused survey for its members and partners.

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

CYBER SECURITY IS A BUSINESS ISSUE, NOT JUST A TECHNOLOGICAL ONE

There is an increased understanding at the board level and by C-level executives in Australia of the financial and reputational risks posed by cyber security breaches. Increased publicity about and awareness of cyber attacks, and stricter regulations and legislation, are increasing maturity levels.

CYBER SECURITY IS TOP OF MIND

Information systems security was once a specialised activity and a third order concern. Today it is central to all aspects of information processing. Eight of ICT decision-makers' top ten challenges are directly concerned with cyber security, which is now the biggest issue facing Australia's ICT professionals.

CYBER SECURITY IS INTEGRAL TO INFORMATION-PROCESSING

Computer 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. Cyber security is increasingly being built into Information systems.

THE AUSTRALIAN GOVERNMENT HAS MADE CYBER SECURITY A NATIONAL PRIORITY

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

KEY FINDINGS (CONTINUED)

> **"The COVID-19 pandemic is having a positive effect on cyber security investment."**

ONLINE BUSINESSES TAKE CYBER SECURITY MORE SERIOUSLY

Online businesses are much more likely to be using backup and recovery services that are based in the cloud, while offline 'bricks and mortar' based businesses are much more likely to use more conventional methods such as offsite storage and backup sites. Overall cyber security services are growing strongly.

TECHNOLOGY INVESTMENTS ARE CHANGING TO MEET RISING THREATS

New technologies are constantly changing the cyber security landscape, posing new threats and leading to the development of new products and strategies. Important technologies for the future of cyber security include blockchain, artificial intelligence and machine learning, and the Internet of Things. Specialised cyber security services are a major growth area.

THE RISE OF THE ZERO TRUST ARCHITECTURE (ZTA)

The COVID-19 pandemic and advances in cyber security technology and practices have led to the emergence of the concept of the Zero Trust Architecture. With a ZTA no component of a corporate network is trusted, and every access by or to every component must be verified. This is a very different concept to the traditional paradigm of perimeter security. The old concept of 'trust and verify' is replaced with the new concept of 'never trust and always verify'.

COVID-19 PANDEMIC HAS INCREASED SECURITY CONCERNS

The medical impact of the COVID-19 virus on Australia has been slight by international standards, but the economic consequences of the lockdown have been severe and will be felt for years to come. The much greater numbers of employees working from home has led to a significant increases in cyber attacks. This is a permanent change and is having a significant effect on the cyber security landscape, with positive effects on investment.

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 examined all areas of ICT expenditure and investment, and found that by far the most important, with the highest expenditure and greatest strategic focus, were cyber security and related areas.

"Cyber security issues are at top of mind for the great majority of Australia's ICT professionals. Spending is increasing dramatically in all areas."

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. This means cyber security is no longer a technical issue, but a business issue.

The results of the survey provide tangible evidence that this 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.

BUSINESS OBJECTIVES

ICT IS ALL ABOUT MEETING BUSINESS OBJECTIVES

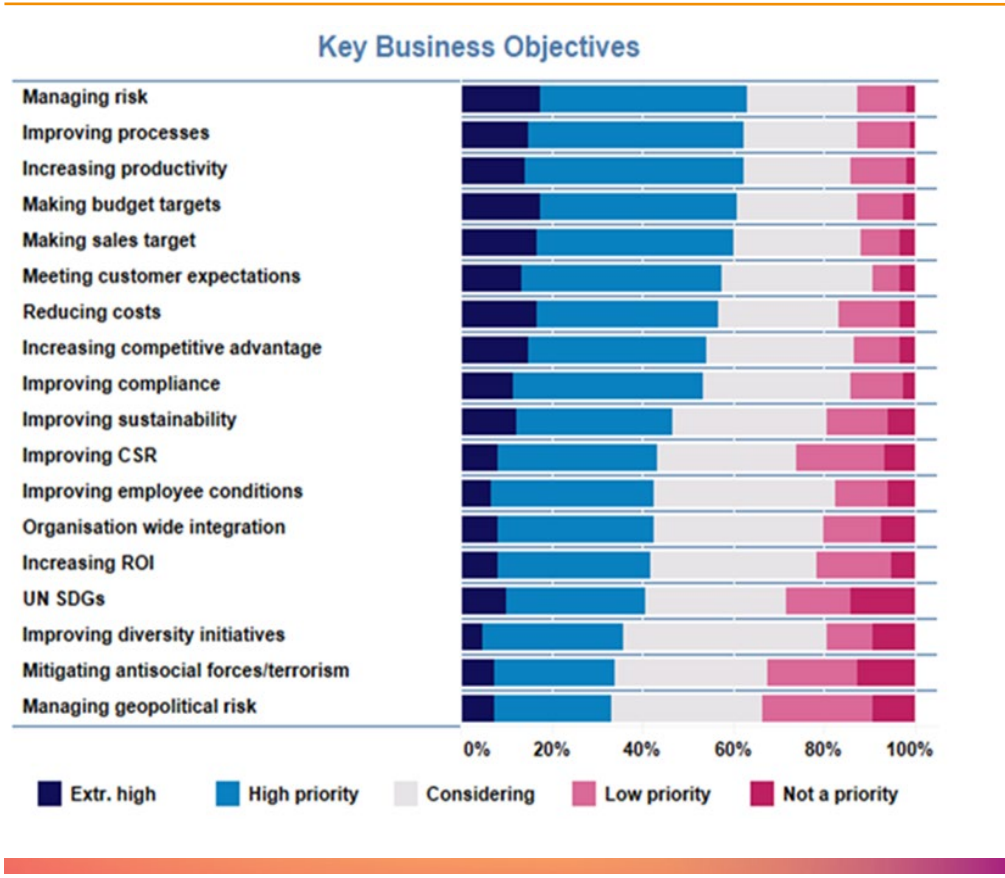
Respondents were asked to rate a number of key business objectives to rank them from ‘extremely high priority’ to ‘not a priority at all’. The chart shows the priorities sorted from the top down (grouped as ’extremely high priority’ plus ‘high priority’).

The greatest risks are seen to be those related to cyber security. Risk management outrates conventional objectives such as meeting budgets and increasing productivity, although the following top three objectives – improving processes, increasing productivity, making budget targets may also have an important risk component.

Cyber security has become an important risk factor and is now a serious issue at the board and senior management level.

These are, of course, ICT decision makers’ understanding of their organisations’ business objectives. Nevertheless, they clearly show the importance of risk management as a factor in modern business.

The bottom line: Cyber security is no longer all about technology. It is a first order business management issue.



“Managing the risk from cyber security is the top business objective.”

ICT STRATEGIC CHALLENGES

CYBER SECURITY OUTRATES ALL OTHER CONCERNS

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

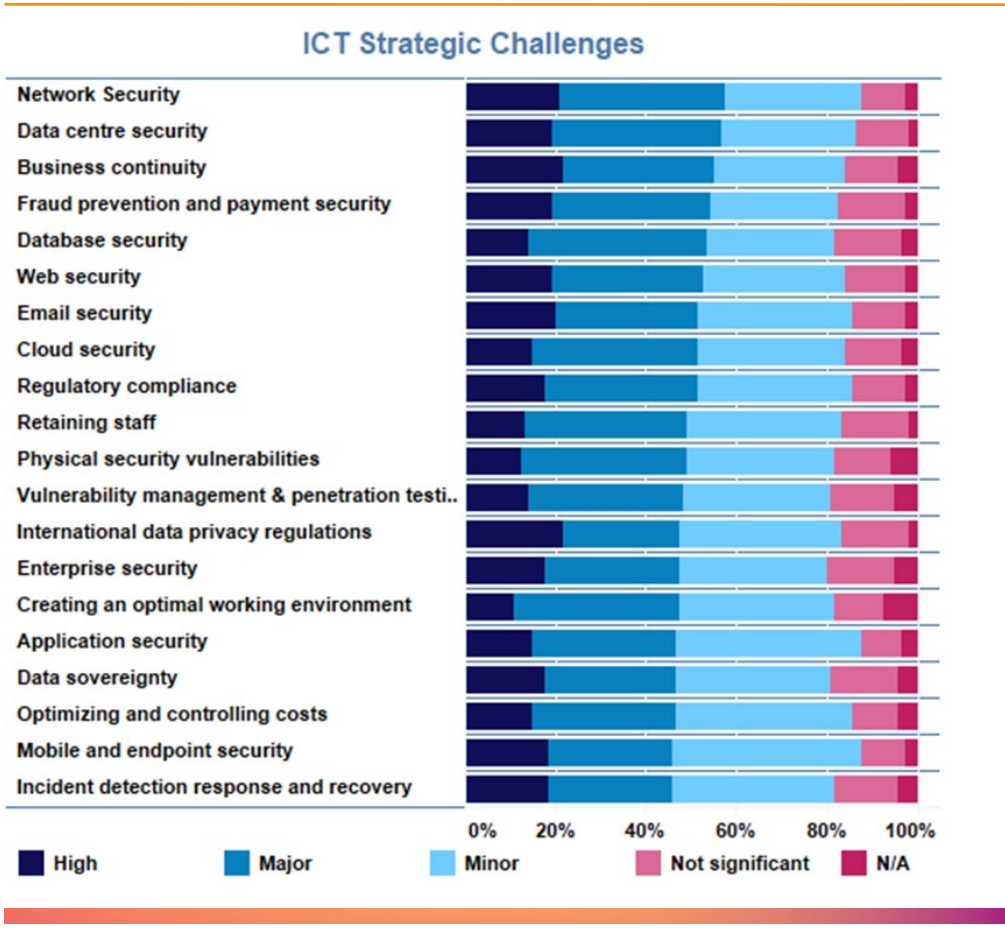
The chart shows the top 20 challenges, sorted from the top down ('high significance' plus 'major significance').

Eight of the top ten challenges are directly concerned with cyber security, and the other two are related issues (business continuity and regulatory compliance). Security issues also rate strongly in the other major concerns. Cyber security is easily the biggest issue facing Australia's ICT professionals.

The results show the dominant position cyber security has attained as a challenge to Australia ICT professionals and decision makers. Once a second- or third-order issue, it is now the single most important challenge they face.

The respondents may be discounting the importance of application, mobile and end point security as well as incident detection response and recovery at this critical time of increased working from home.

The bottom line: Cyber security can longer be separated from other challenges – it permeates all facets of ICT.



"Almost all the key ICT strategic challenges have to do with security."

EVENTS IN 2021

JOIN US IN 2021

March 16 - 18
Australian Cyber Conference – Canberra Edition
www.cyberconference.com.au

March 26
BrisSEC - Brisbane
www.aisa.org.au

October 15
PerthSEC - Perth
www.aisa.org.au

November 15-17
Australian Cyber Conference – Melbourne Edition
www.cyberconference.com.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 our extensive research process, DataDriven surveys hundreds of ICT decision makers in specific markets. 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 DataDriven Technology 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

HYPE-DIALS: DX, CYBER SECURITY AI/ML, BIG DATA

These charts show the Hype-Dials for digital transformation, cyber security, AI/machine learning and big data/analytics.

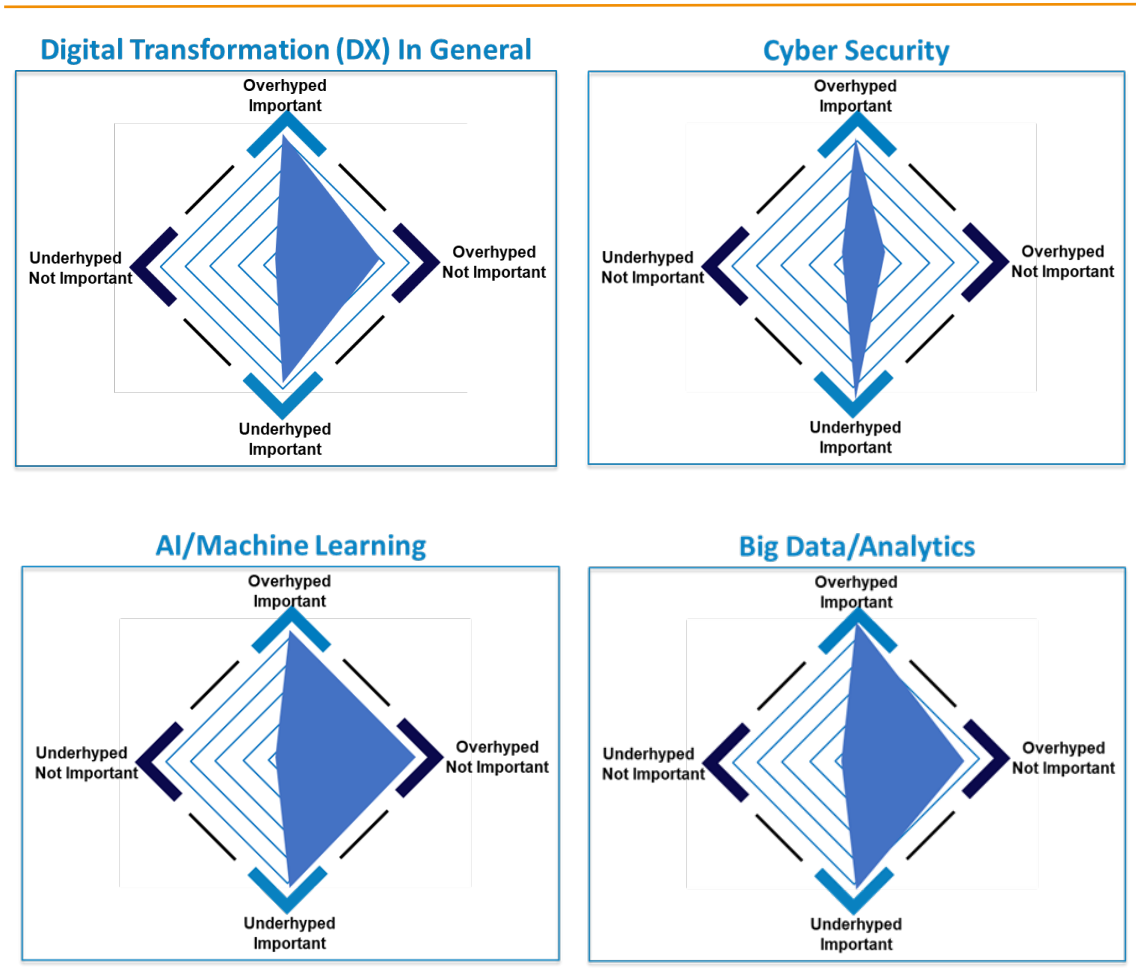
All four Hype-Dials have a strong vertical axis, indicating that all technologies are regarded as important.

All Hype-Dials except that of cyber security also have a strong horizontal bulge to the right, indicating that many people believe them to not be important.

There is no such a bulge on the cyber security Hype-Dial, which indicates that virtually all respondents believe it be important to their organisation.

The bottom line: There is almost universal acceptance amongst ICT decision makers of the critical importance of cyber security.

"Despite cyber security's high profile, many ICT decision makers still believe it to be under-hyped."



DIDataDriven Technology Hype-Dials

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 have higher degrees of cyber maturity than those with most of their business conducted offline (bricks and mortar)."

CYBER SECURITY MATURITY

Maturity levels are examined for each of four separate areas:

- Cyber Security Ecosystem (overall cyber security implementation),
- Technology and Products,
- Cyber Security Services,
- Backup and Recovery.

Scores are expressed using a standard Capability Maturity Model as a rating between 1 ('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 in an offline or 'bricks and mortar' mode. Just over two thirds (70.8%) of respondents work for organisations with less than half their revenues online, and just under one third (29.2%) work for organisations with more than half their revenues generated online.

ECOSYSTEM MATURITY LEVEL

THE BIG PICTURE

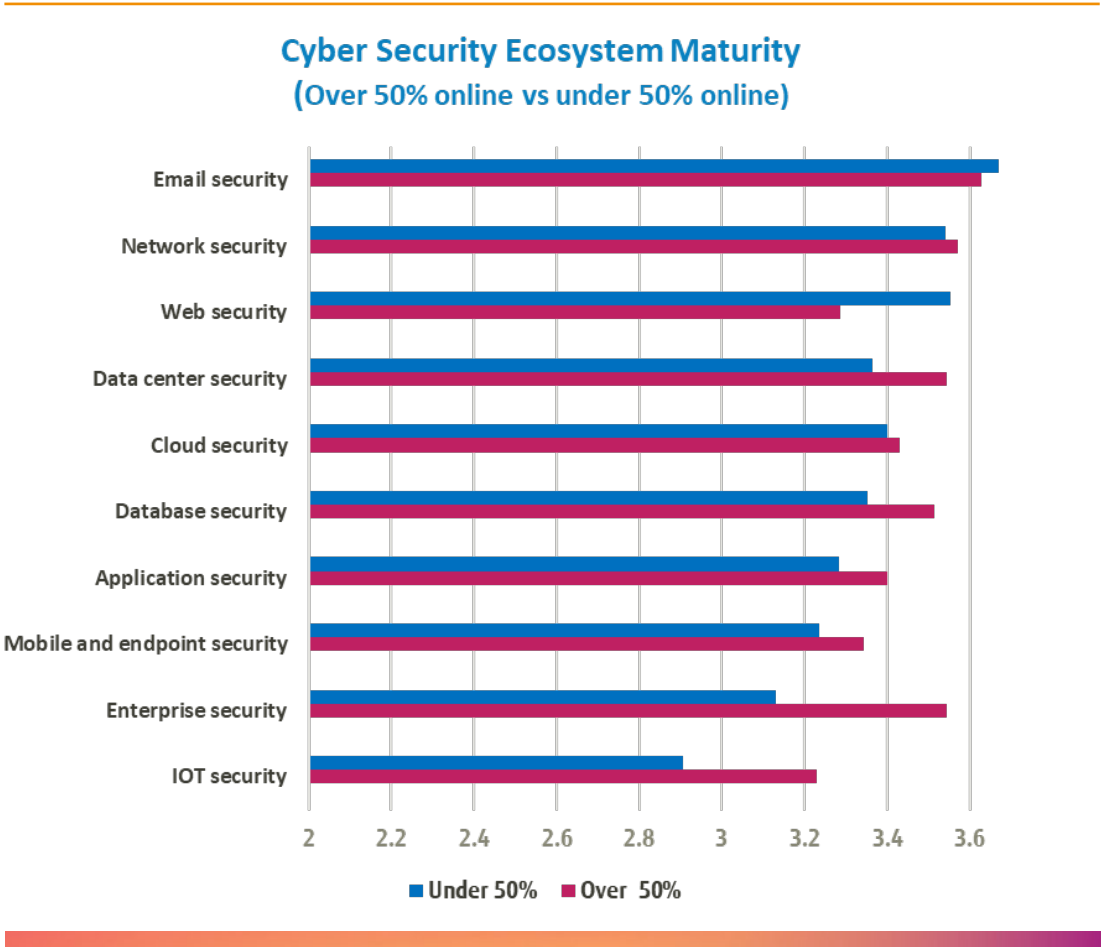
The cyber security ecosystem refers to general areas of cyber security, rather than specific products.

The areas with the highest maturity levels are email and network security, where there is little difference between online and off-line businesses. In most other areas of cyber security, online businesses tend to be significantly more mature than off-line businesses.

The surprising exception is web security, where offline businesses are more mature, This is because online businesses tend to see cyber security in more holistic terms than just through the lens of web security.

Note also the much higher level of IoT maturity in online enterprises, which are significantly more advanced in their usage of the technology.

The bottom line: Cyber security maturity levels are still too low. Too few organisations regard it holistically, or are struggling to muster a comprehensive, risk based capability.



"Online businesses display greater maturity in cyber security than traditional bricks and mortar enterprises."

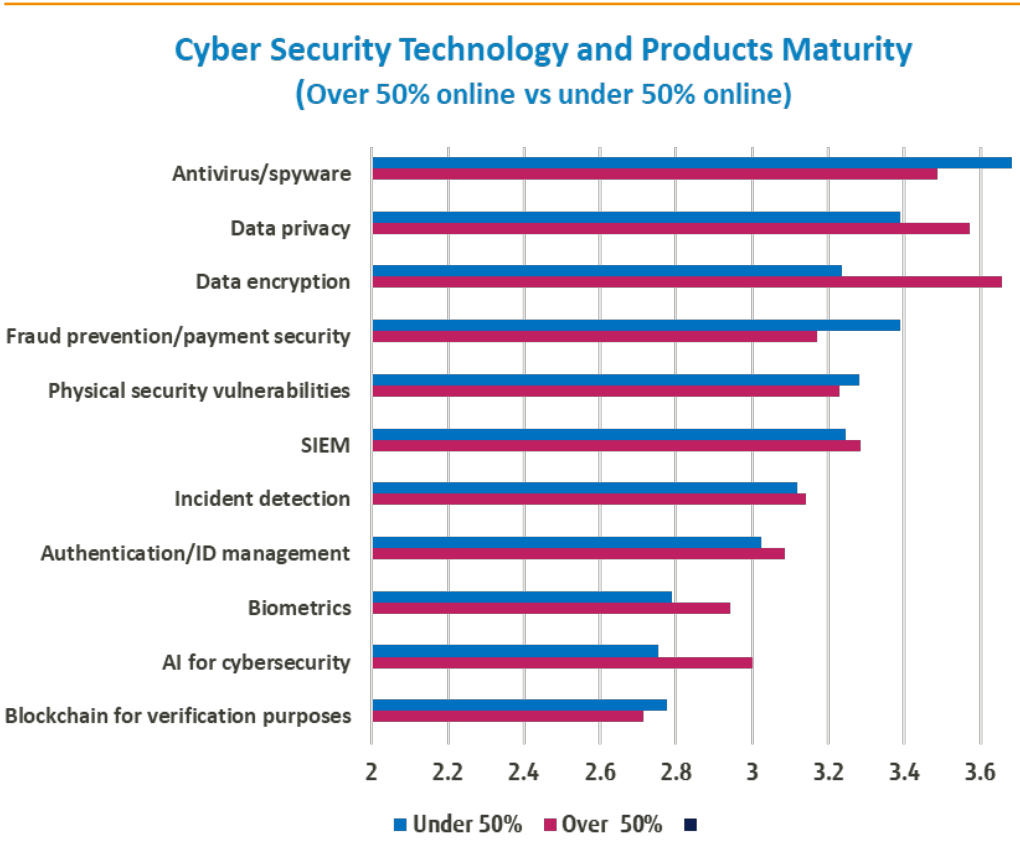
TECHNOLOGY AND PRODUCTS MATURITY LEVEL

CYBER SECURITY TECHNOLOGY AND PRODUCTS

Online businesses are more aware of the limits of implementation of antivirus/spyware software, as well as fraud prevention and payment security systems, than traditional businesses. They are significantly ahead in other areas, especially data privacy, data encryption and the use of biometrics and artificial intelligence for cyber security protection. This indicates potentially a more sophisticated view of online businesses towards cyber security and privacy.

Data encryption is particularly important for online businesses and is much more likely to be embedded into their infrastructure. It is a key technology that must be introduced in an integrated rather than a piecemeal fashion.

The bottom line: Online businesses are more mature in their usage of newer technologies like biometrics and AI.



"Data encryption has become a key technology for online businesses."

SERVICES MATURITY LEVEL

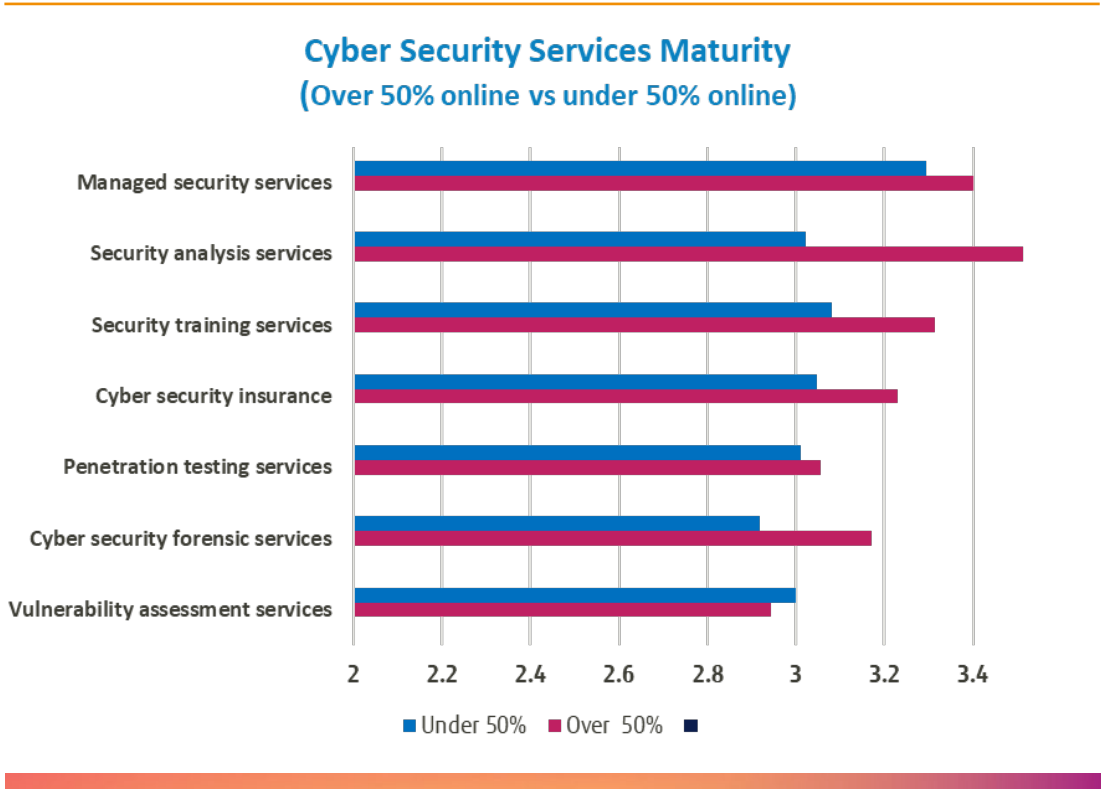
CYBER SECURITY SERVICES

As cyber security becomes more important, services proliferate. Organisations that do most of their business online are much more mature users of cyber security services than those that do not, especially in the area of security analysis, where online users are significantly ahead.

Managed security services have grown strongly in recent years, with many enterprises outsourcing all or part of their cyber security operations to specialist vendors and consultants. The range of services is now substantial and includes the relatively new field of cyber security insurance.

The increasing importance of cyber security services brings more challenges to ICT decision makers, who are now faced with the job of evaluating and managing the growing number of service providers.

The bottom line: Bricks and mortar businesses are lagging in their usage of cyber security services.



"The managed security services market is growing strongly."

BACKUP AND RECOVERY MATURITY LEVEL

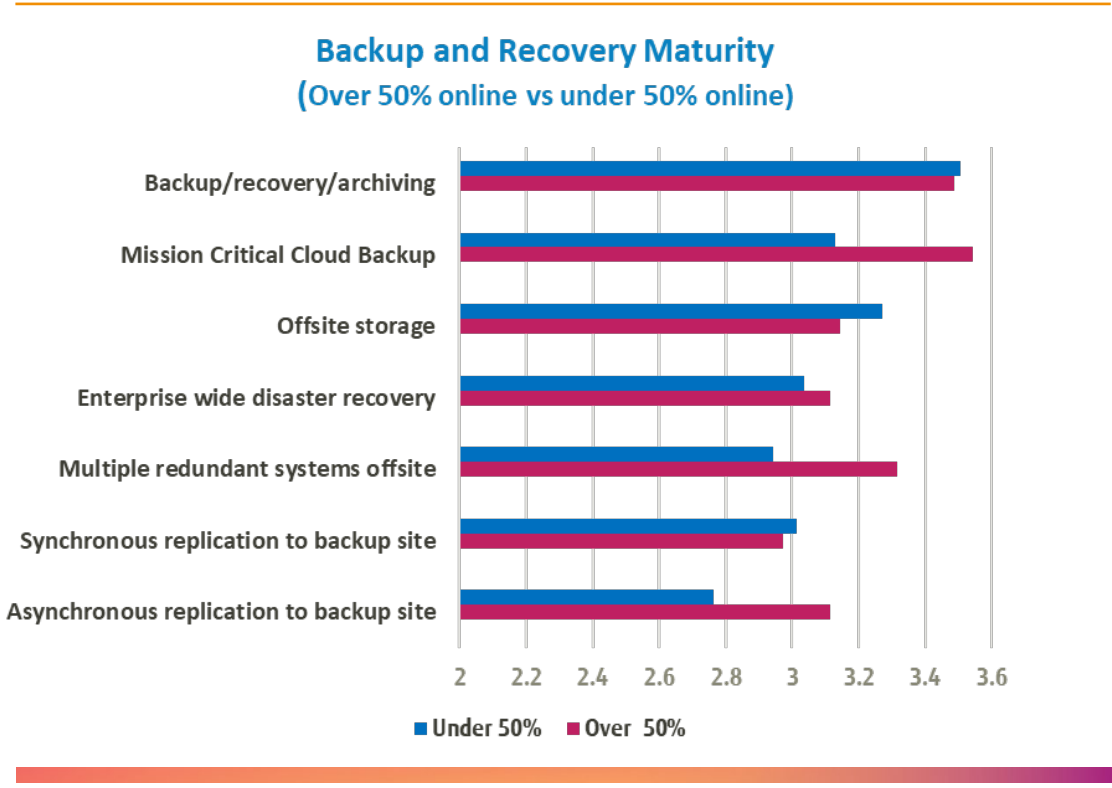
BACKUP AND RECOVERY SERVICES

Backup and recovery have been important functions since the beginning of commercial computing. Practices changed little for many years until the arrival of cloud computing. It is now an important component of cyber security.

Online businesses are much more likely to be using backup and recovery services that are based in the cloud, while offline businesses are much more likely to use more conventional methods such as offsite storage and backup sites.

High availability for systems has become a key requirement for online businesses – it is not only for critical infrastructure, but necessary for digital commerce.

The bottom line: Backup and recovery is more important than ever, but too many enterprises are not moving with the times.



"Backup and recovery techniques vary significantly by type of organisation."

CYBER SECURITY IMPLEMENTATION AND INVESTMENT

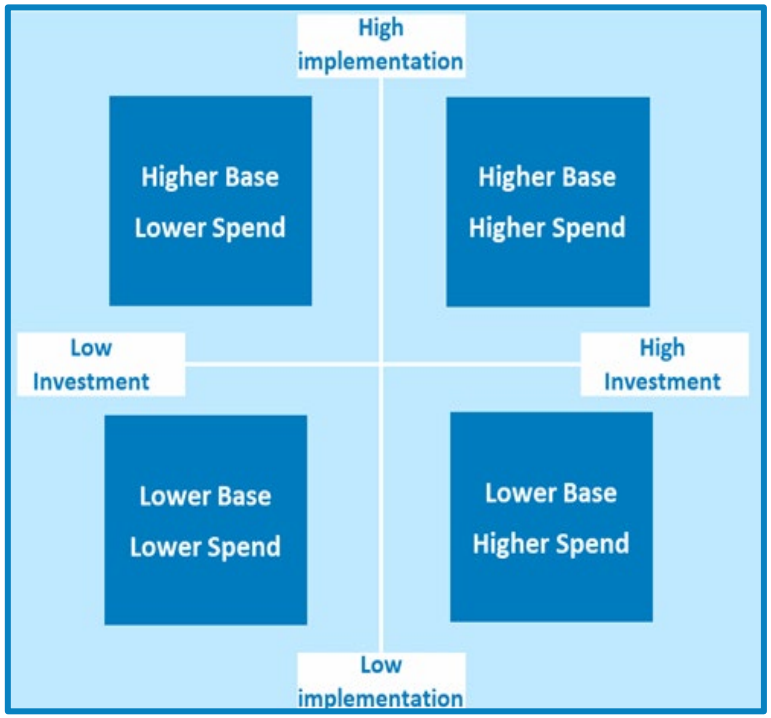
This section of the report examines the extent of organisations' cyber security implementation versus planned investment in four areas: ecosystem, technology and products, services, and backup and recovery.

Note that the survey was conducted just as the COVID-19 pandemic was taking hold in Australia, and that significant changes may occur in future.

"There are high degrees of both implementation and planned investment for most areas of cyber security."

IMPLEMENTATION VS INVESTMENT MATRIX (I^2M)

The I^2M 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 I^2M shows their status relative to each other and is not designed to reflect actual market shares.



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. Many areas with comparatively low implementation show high degrees of planned investment.

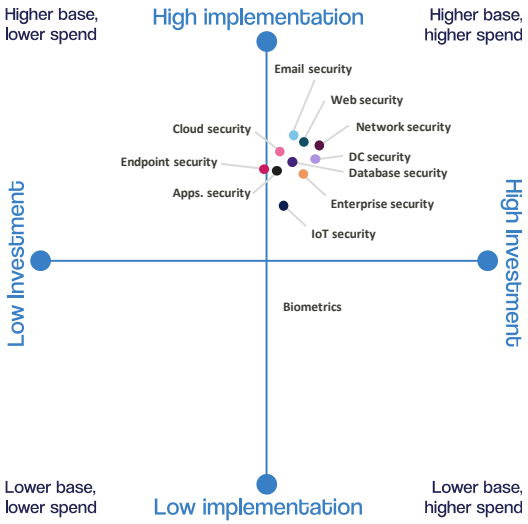
The bottom line: There will be strong continued investment in all aspects of cyber security.

CYBER SECURITY TECHNOLOGY AND PRODUCTS

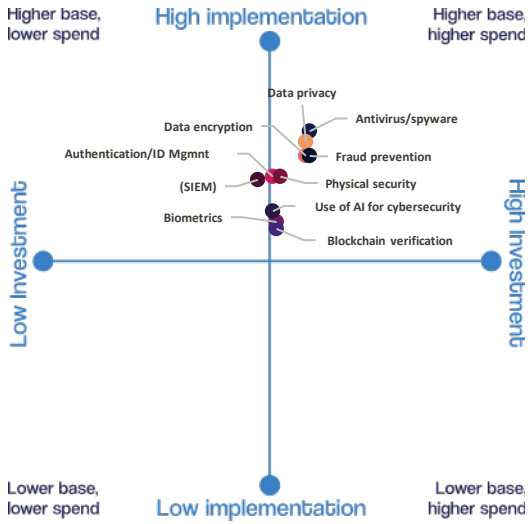
Implementation and Investment levels vary by product type. Blockchain, AI and biometrics are still not widely implemented, though many organisations are looking at these technologies.

The bottom line: There are many paths to the future. Users are considering a range of different products and technologies.

Cyber Security Ecosystem



Cyber Security Technology & Products



> **"Most organisations are planning significant further investments in cyber security."**

IMPLEMENTATION VS INVESTMENT MATRIX (I²M)

CYBER SECURITY SERVICES

Usage of cyber security services is growing significantly, with high levels of both implementation and planned investment in most areas.

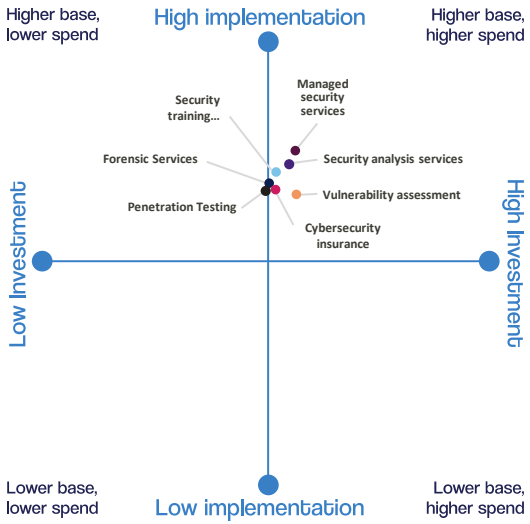
The bottom line: Services are the fastest growing area of cyber security.

BACKUP AND RECOVERY

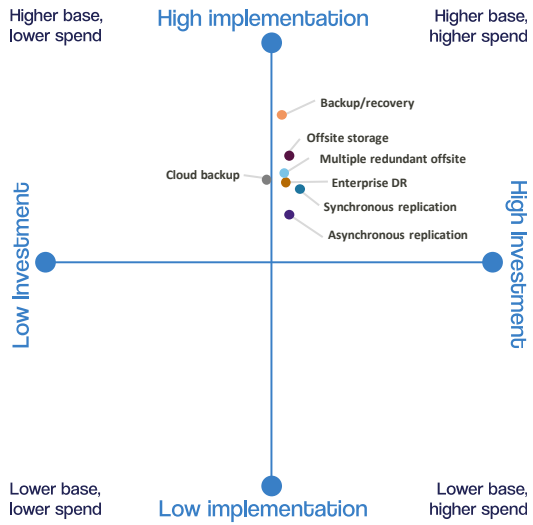
Many organisations have implemented backup and recovery technologies, but the level of planned investment is comparatively low.

The bottom line: Many organisations are underinvesting in backup and recovery.

Cyber Security Services



Backup and Recovery



"Most organisations are planning significant further investments in cyber security."

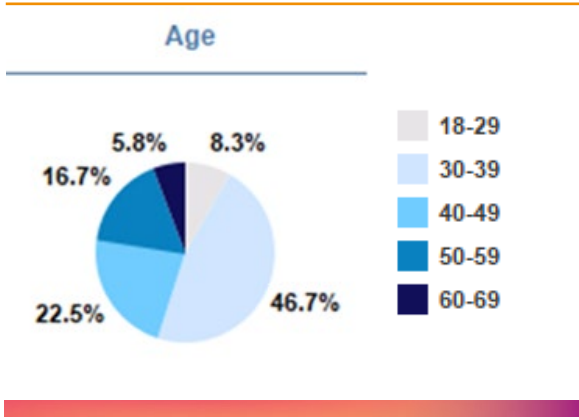
PROFILE OF AN ICT DECISION MAKER

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, but not by a large margin. They span all age groups and have a diversity of views.

"Australian ICT decision makers are very well educated, and feel well placed to deal with future challenges"

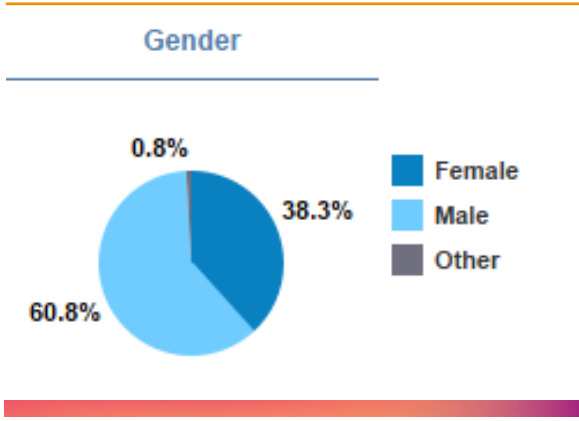
AGE

Almost half (46.7%) of respondents to the survey are in their 30s, and almost one quarter (22.5%) in their 40s. One in six (16.7%) are in their 50s, with smaller numbers older (5.8%) or younger (8.3%).



GENDER

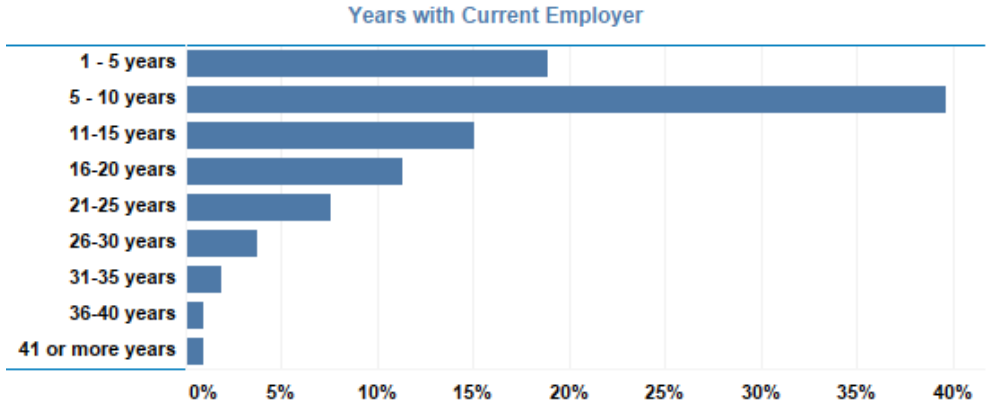
ICT is still heavily gender biased to males. But for this survey well over one third (38.3%) of respondents are female.



PROFILE OF AN ICT DECISION MAKER

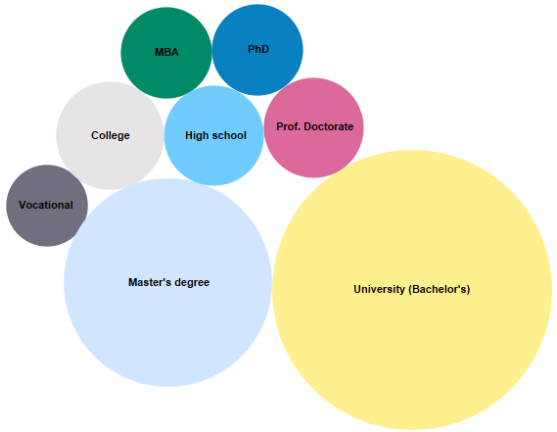
YEARS WITH CURRENT EMPLOYER

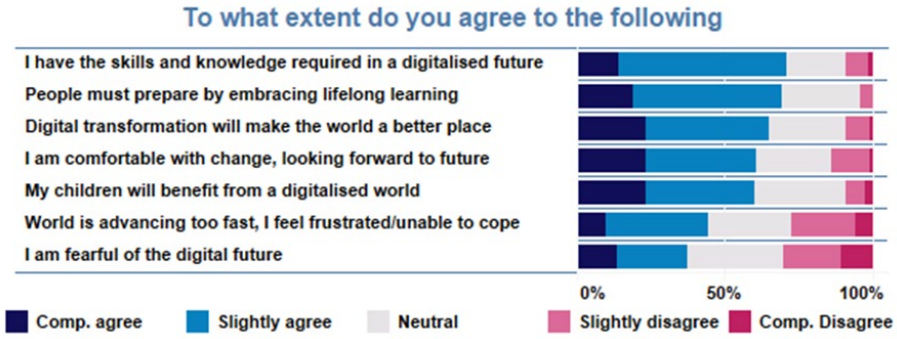
Australia's ICT decision-makers tend to stay with their employers a long time. Fully 41.5% have been with the same organisation for more than ten years, and almost as many (49.6%) between five and ten years. Only 18.9% have been with their employer for less than five years.



EDUCATION LEVEL

Australia's ICT decision makers are very well educated. Nearly half (44.3%) of respondents to the survey have at least a Bachelor's degree, and more than one third have higher academic qualifications: MBA (4.7%), other Masters degree (24.5%) or PhD (5.6%).





VIEWS ON TECHNOLOGY

Most ICT professionals believe they are equipped with the skills and knowledge required in a digitalised future. They agree that technology will make the world a better place and will benefit their children. They agree that learning is a lifelong process. They are generally comfortable with the pace of change but almost around one third believe that things are happening too quickly for them to keep up.

DEALING WITH DISASTERS

Australia has had its share of disasters in recent times. It seems they have become everyday occurrences, dulling our capacity to be shocked and impacting people and organisational resilience.

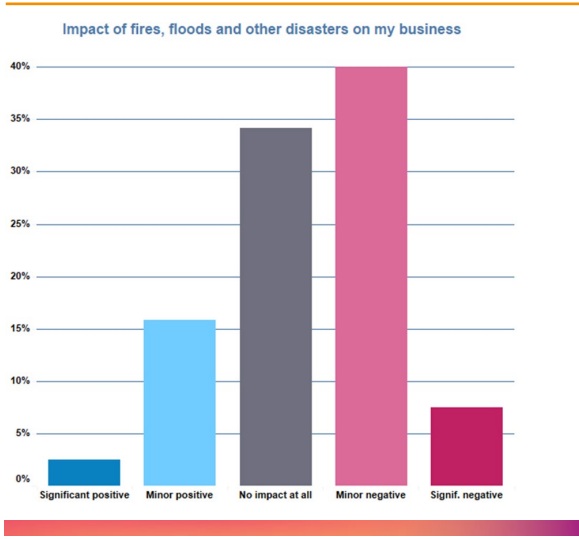
The survey asked about the effect of disasters on respondents' organisations. Perceptions of negative impacts for both natural disaster and COVID-19 were much higher than positive perceptions.

"Disasters are generally bad for business, but not for everyone."

NATURAL DISASTERS

Around half of respondents believe that natural disasters such as bushfires and floods will have a negative impact on their business.

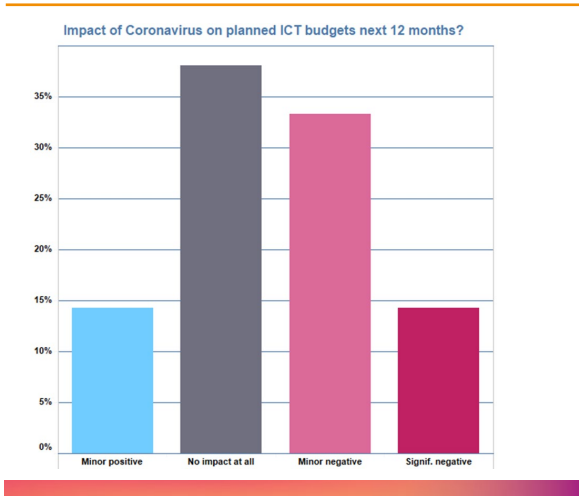
Around one third see no effect, while one in six see a positive impact.



COVID-19

The survey was conducted at the beginning of the COVID-19 crisis.

Most respondents believed it would have a negative impact on their business, but some people saw a minor positive impact.



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 will also be useful to attackers also), and IoT because of increased vulnerabilities at an ever expanding edge.

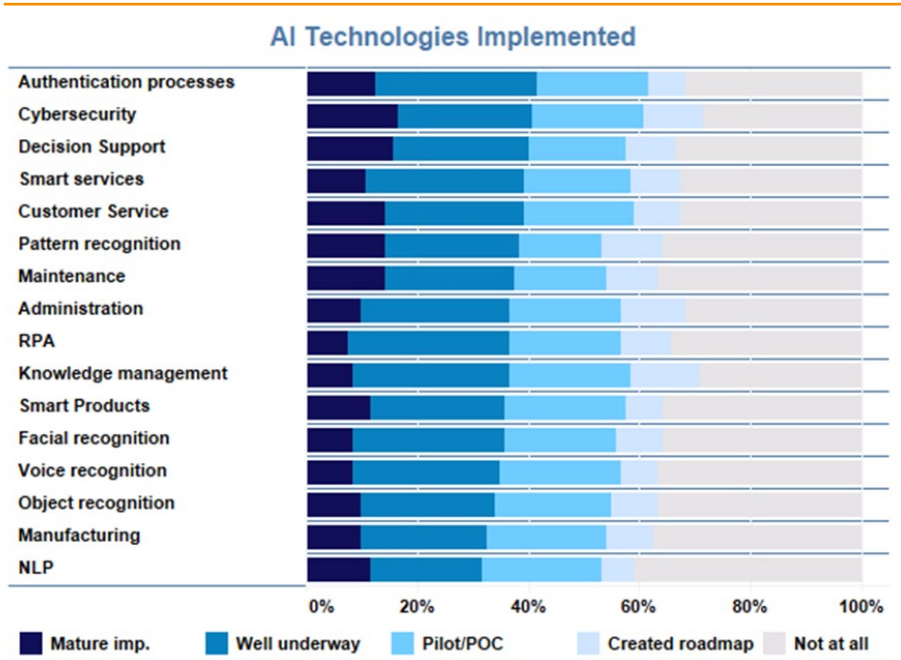
"New technologies such as AI and IoT are generally beneficial, particularly for authentication and cyber security"

AISA WWW.AISA.ORG.AU

ARTIFICIAL INTELLIGENCE

The survey asked about the implementation of a range of AI-related tools and technologies. The use of AI for cyber security and related purposes such as authentication are at the top of the list. AI has been talked about for years, but for many organisations implementation is still in its infancy.

The results show that cyber security is proving to be a major driver for the implementation of the technology

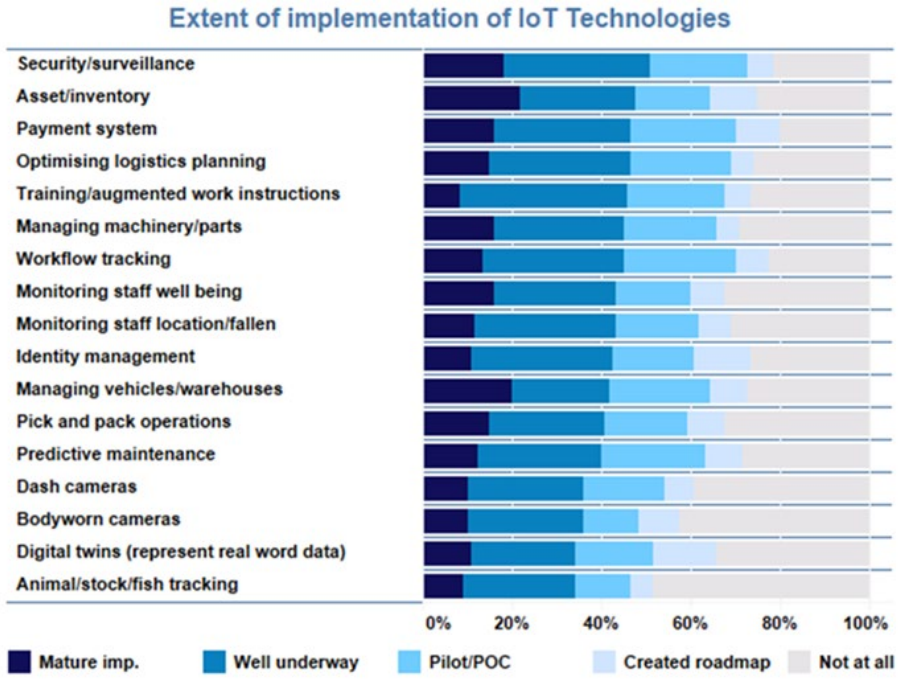


AI AND IoT

INTERNET OF THINGS

The survey asked about the implementation of IoT technologies and applications. The use of the technology for security and surveillance is at the top of the list, and identity management also figures strongly.

IoT, with its massive increase in enterprise endpoints, will introduce challenges for cyber security, but will also feature strongly as a solution.



"The use of IoT technology for surveillance and identity management will likely have massive privacy impacts on individuals."

SUPPLIER SATISFACTION AND PREFERENCES

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

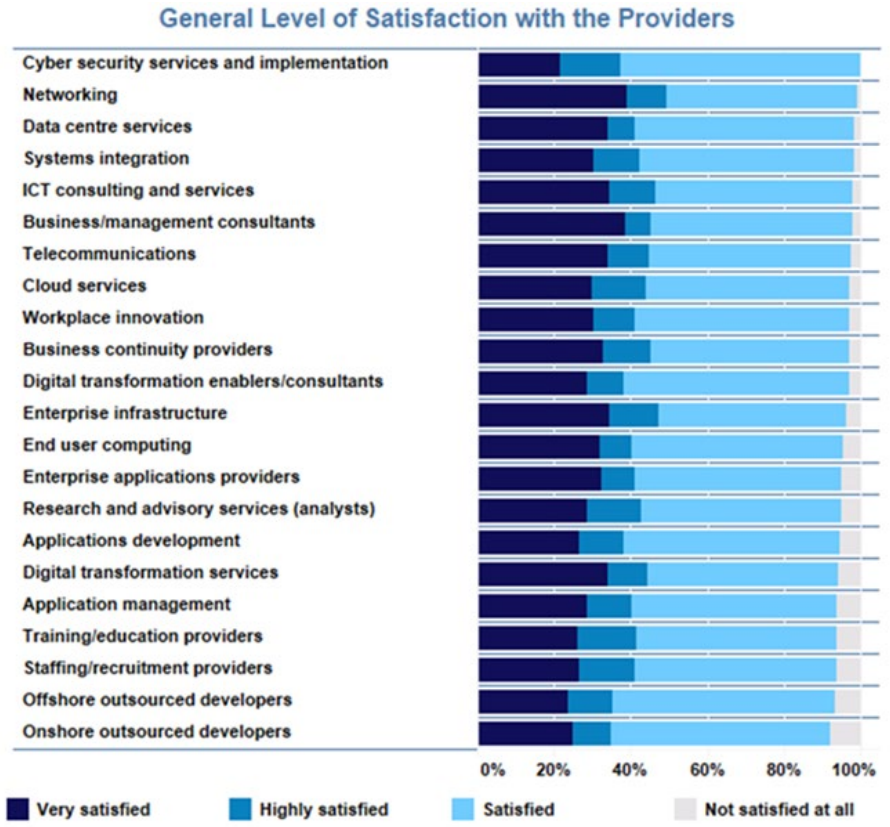
"ICT decision-makers in Australia are generally satisfied with their cyber security suppliers."

AISA WWW.AISA.ORG.AU

LEVEL OF SATISFACTION

The survey asked about respondent's level of satisfaction with providers in a range of product and service areas. There are generally high levels of satisfaction.

Cyber security services and implementation providers have the highest levels of satisfaction (all three categories added), followed by Networking and Data centre services providers. Not a single respondent said they are 'not satisfied' with their cyber security providers, but comparatively few of them said that they are 'very satisfied'.

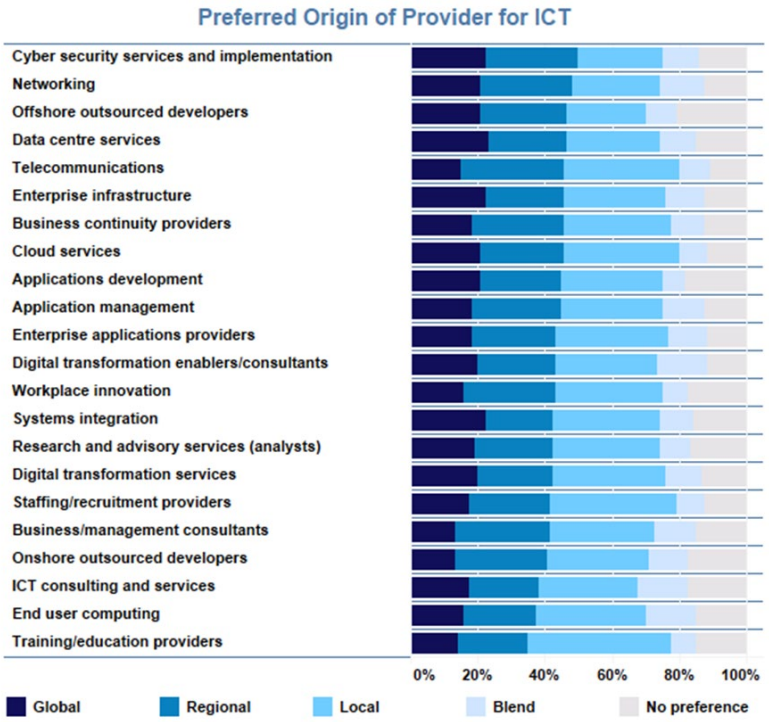


SUPPLIER SATISFACTION AND PREFERENCES

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 other global local, or whether they prefer a blend or have no preference.

They are more likely to prefer their cybersecurity suppliers to be global or regional, though many prefer local suppliers or a blend.



"There is no strong preference for global, regional or local cyber security providers. The most important factor is their performance."

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

AISA WWW.AISA.ORG.AU

THE MANY FACETS OF CYBER SECURITY

Cyber security is everywhere, and has many facets. Point solutions are still common, but most organisations with a comprehensive cyber security strategy have adopted a more integrated approach. There is no one size fits all solution and every organisation will need a different combination of cyber security products and services. That is all the more reason to adopt a coherent strategy rather than rely on piecemeal tactical fixes.

Cyber security is a broad term. It ranges from the safeguard of individual devices to the protection of the enterprise and even the nation state. A complete cyber security taxonomy includes many different product areas. A popular classification is that devised by NIST, the US National Institute of Standards and Technology, which identifies five main categories of cyber security: identify, protect, detect, respond, and recover. This widely used taxonomy identifies the key areas – many cyber security products straddle multiple NIST categories.

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).

THE CYBER SECURITY LANDSCAPE IN AUSTRALIA – GOVERNMENT INITIATIVES

AUSTRALIAN GOVERNMENT INITIATIVES

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' cybersecurity 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.
- The creation of AustCyber and Australia's Cyber Security Sector Competitiveness Plan 2019 is intended to grow a vibrant and competitive cyber security sector that generates increased investment and jobs for the Australian economy.
- 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 cybersecurity 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$3.6billion 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 – 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.

"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 new challenges and opportunities for cyber crime."

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

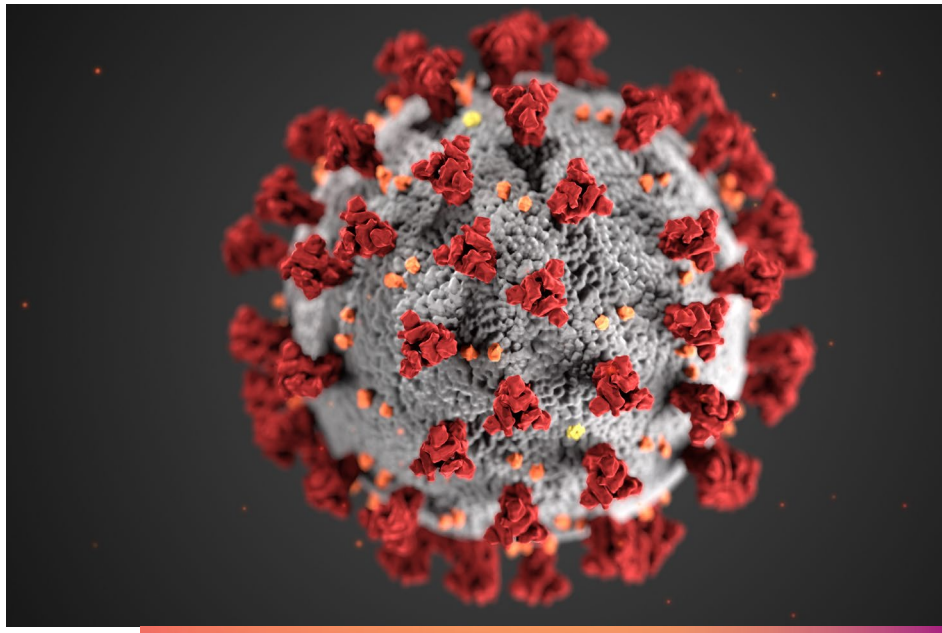
THE COVID-10 PANDEMIC

The first cases of COVID-19 were reported in Australia in January 2020, and the virus quickly took hold during the survey period for this report. The impact of the virus itself on Australia was slight by international standards, but the economic consequences of the lockdown were 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.

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 within the organisation.



"This survey was conducted just as Covid-19 took hold in Australia. What will the landscape look like in 2021?"

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. New technologies such as artificial intelligence provide many opportunities, but they also pose significant challenges.

Those best equipped to meet these challenges will be those who keep abreast of the technologies and best practice, and who maintain constant vigilance.

"Cyber security is a journey, not a destination. It is a constant challenge, to ICT decision makers and to business leaders. It requires constant vigilance."

CYBER SECURITY IS NOW WOVEN INTO THE FABRIC OF BUSINESS

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 findings show that cyber security has become an integral part of systems design and operation, and that cyber security issues are at top of mind for the great majority of Australia's ICT professionals. The survey also shows that cyber security is now very much viewed as a business issue by senior management.

But cyber security is a journey, not a destination. Even as the level of maturity in the usage of the many facets of cyber security increases, so do their range of threats and their sophistication. New technologies and new techniques must be employed to confront the evolving threat landscape.

The increased importance of cyber security has led to a raft of new providers of products and service, presenting ICT decision makers with a bewildering array of options. Developing and executing the right strategy is a constant challenge. Investment in cyber security has never been higher, but the report shows that much more needs to be done.

Compared to other ICT and Digital Transformation product categories surveyed, cyber security may also be over-hyped. But decisions makers see it of critical importance, with increasing implementation and investment. Whether this will continue will depend on the level of increased digital investment, the growth in threats, and the likely rise of the importance of return on investment as a result of the pandemic.

DEMOGRAPHICS

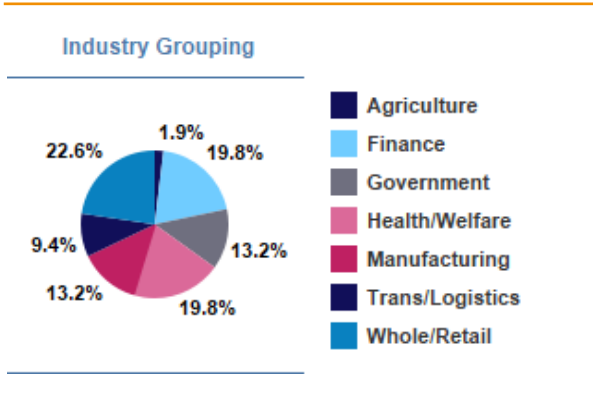
Over 1,000 potential respondents were contacted, with the aim of identifying 125 key ICT Decision makers.

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

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

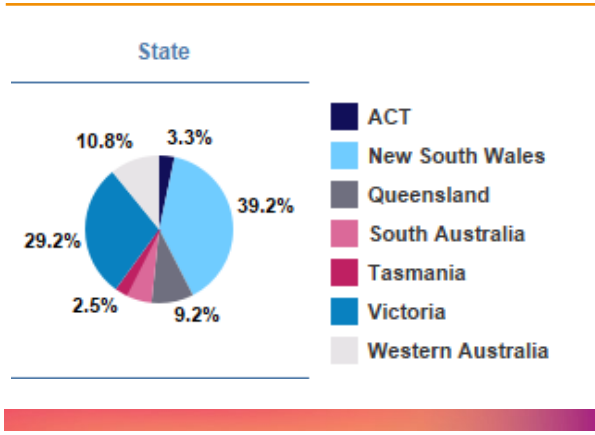
RESPONDENTS BY INDUSTRY

Six broad industry verticals are represented: Finance (19.8%), Government (13.2%), Health and Welfare (19.8%), Manufacturing (13.2%), Transport and Logistics (9.4%), and Wholesale and Retail (22.6%).



RESPONDENTS BY STATE

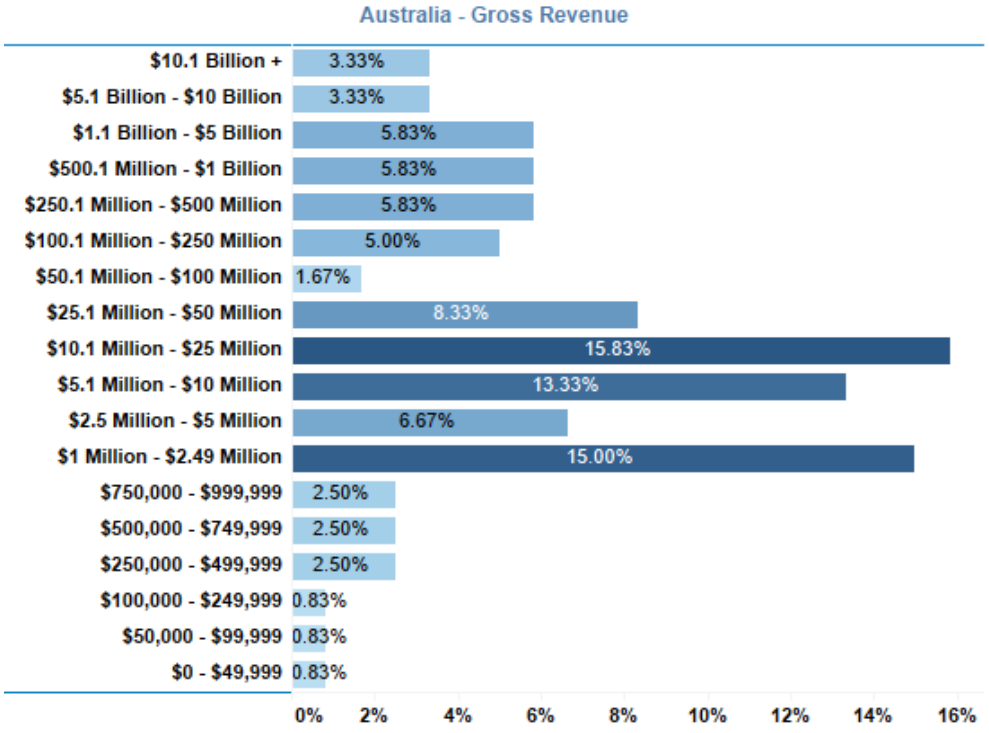
The breakdown by State is broadly representative of the overall distribution of Australia's population., with the largest proportion from NSW (39.2%) and Victoria (29.2%).



BY REVENUES AND EMPLOYEES

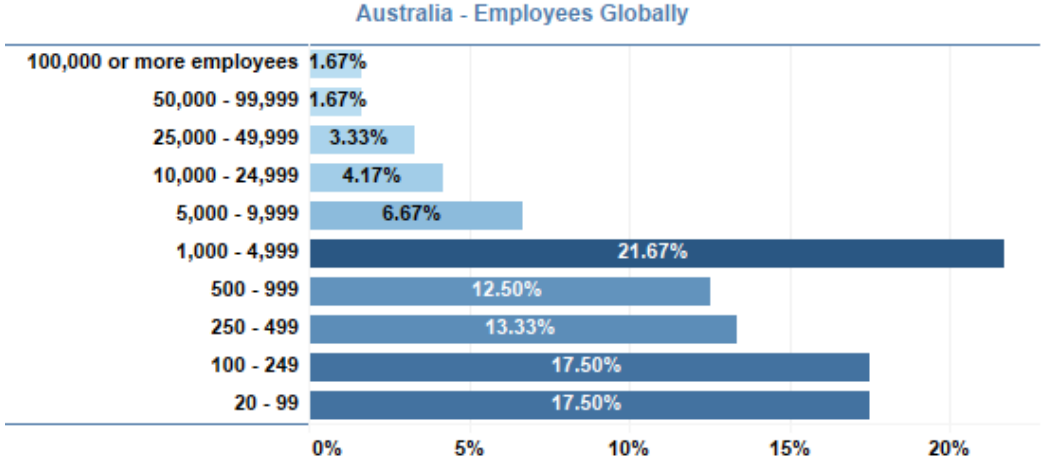
RESPONDENTS BY GROSS REVENUE IN AUSTRALIA

Respondents come from all sizes of organisation. Two metrics were collected: annual gross revenue and number of employees. By revenue, most respondents work for organisations with between $1 million and $50 million in revenues. Nearly one in five (18.3%) work in organisations with over $1 billion in revenues.



RESPONDENTS BY NUMBER OF EMPLOYEES GLOBALLY

Less than one fifth (17.5%) of respondents work for organisations with fewer than 100 employees. A similar proportion work for organisations with 250-999 employees. Almost half (47.4%) work for organisations with between 250 and 5,000 employees, and 17.5% work for organisations with more than 5,000 employees.



"Almost half work for organisations with between 250 and 5,000 employees."

RESEARCH FRAMEWORK, METHODOLOGY AND APPROACH

The DataDriven Digital Transformation Technology Matrix (DXTM) drives all of our research.

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.

"A common taxonomy drives higher quality survey results and outcomes."

A COMPREHENSIVE RESEARCH FRAMEWORK

The Digital Transformation Technology Matrix (DXTM) comprises five user groups, from the individual to the wider society:

- **Individual:** The effect of Digital Transformation on individuals, at work and in their personal lives.
- **Workplace**: The effect of Digital Transformation on individuals and workgroups within the workplace.
- **Intra-Enterprise:** The effect of Digital Transformation on business practices and business models within the organisation.
- **Extra-Enterprise:** The effect of Digital Transformation on the way the organisation interacts with other organisations.
- **Society:** The effect of Digital Transformation on the economy, government and the wider community.

DataDriven DIGITAL TRANSFORMATION TECHNOLOGY MATRIX (DXTM)

FOUR MAJOR CLASSES OF APPLICATION OR TECHNOLOGY

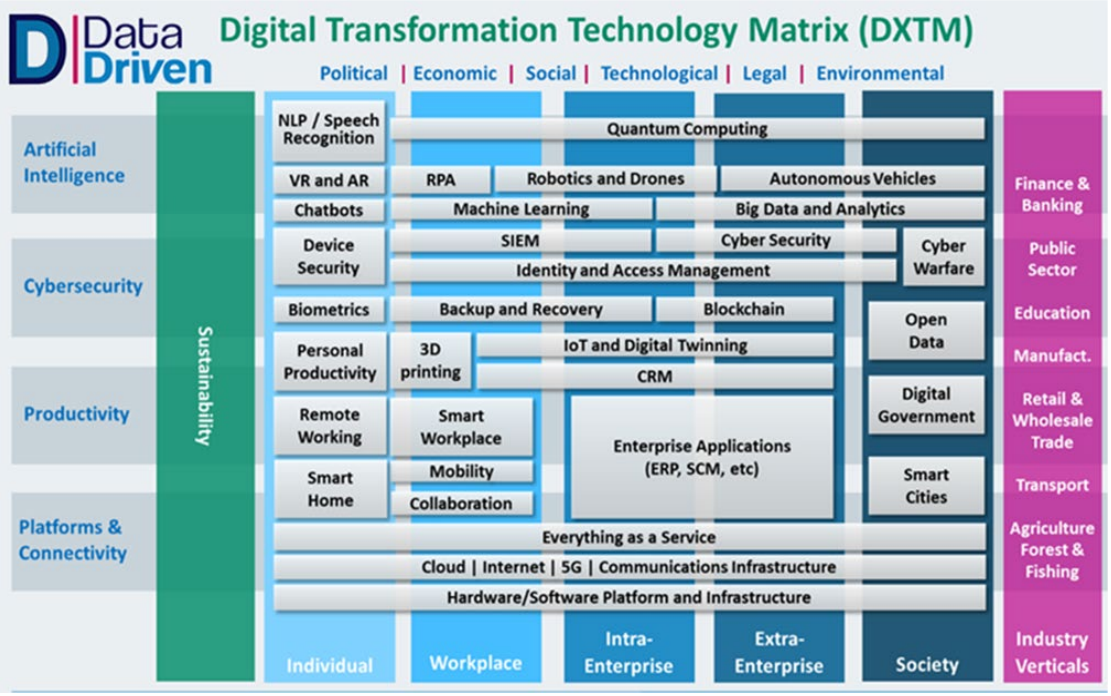
Four classes of technology are overlaid on five user groups. Some of these have their primary effect on only one level, some affect two or more. The four application or technology areas are:

Platforms and Connectivity: Technologies which enable individuals and organisations within each level to communicate and interact with others at their level and beyond. At the base are the underlying connectivity technologies – Cloud/Internet/5G/Comms infrastructure/Hardware and Software Platforms – which sit across all five user groups and are the key enablers of the interconnected world at every level.

Productivity: Technologies which enable and increase the productivity across functions at every level and across levels.

Cyber Security: Technologies which prevent unwanted intrusions, and which enable the efficient and continued operation of the other technology areas.

Artificial Intelligence: Machine based technologies which enable new applications through the simulation of human reasoning.



"The comprehensive DXTM research framework comprises four classes of technology overlaid on five user groups. Some of these have their primary effect on only one level, some affect two or more."

RESEARCH APPROACH BASED ON DXTM

THE DATADRIVEN DIGITAL TRANSFORMATION TECHNOLOGY MATRIX (DXTM)

Our 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 then 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 organisation 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 and 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."

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 decison 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 7000 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