November 2016

Cybersecurity

Threats
Challenges
Opportunities

> "It is only when they go wrong that machines remind you how powerful they are."
>
> Clive James

Contents

Foreword

Protecting that upon which we depend should be front of mind for government, business and industry, academia and every individual with a smartphone in their pocket.

You've seen documents like this pass your desk before, but we hope this one is a little different. You can gloss over it, seeking the diamonds in the rough, but take the time to delve into the information presented here and you will walk away with a different appreciation of the laptop on your desk, the car that you drive, and the phone that you carry.

Not to mention the planes you fly, the banks that hold your money, the hospitals that keep you alive and the very infrastructure that makes our cities run. In short: the basis of our modern lives.

It can be hard to not overuse a word that's become popular thanks to public awareness, but 'cyber' is now firmly entrenched in our language and our mindset, by virtue of the fact that our society today depends so much on technology.

So we're going to talk about cyber with respect to security, as the two are intimately intertwined. In this guide we aim to break down what is sometimes a large and complex issue into an easy to read and digestible summary that should – if we've done our job well – give you the tools to both talk confidently about the issues, as well as equip you with the core information required to make decisions around cybersecurity.

Because, despite the technical nomenclature, the issue of cyber-security is as vital to our way of life as technology itself. In fact, they can't be separated: our economic health, our national security, and indeed the fabric of our society is now defined by the technology we depend on every day.

What's left unsaid here, however, is the assumption that this technology will continue to work as we intend – but this is only true if we can protect it from being hacked, manipulated, and controlled.

Logically, then, protecting that upon which we depend should be front of mind for government, business and industry, academia and every individual with a smartphone in their pocket.

Which is to say, all of us.

If you are part of government, this primer serves as a guide to the greater sphere of cybersecurity and how it relates to our national security, our national interest, and our economic prosperity.

If you are an executive, board member, business leader, or IT professional this is an opportunity to verse yourself in the language and the ecosystem, the threats and the opportunities, and to better communicate the issues and responsibilities around cybersecurity within your organisation.

And if you are simply an individual interested in understanding more about the nature of our digitally-driven world, this guide will provide the basics and a clear overview of how cybersecurity relates to you.

At the ACS we welcome every opportunity to educate and assist. If you have any questions, or would like more information, please feel free to contact me at: anthony.wong@acs.org.au.

Enjoy this guide. We hope it will make a difference to you.

Anthony Wong
President, ACS

SECURING AUSTRALIA'S FUTURE

At ACS we are passionate about the ICT profession being recognised as a driver of productivity, innovation and business – able to deliver real, tangible outcomes.

This year ACS celebrates 50 years of advancing ICT in Australia. Our founders and pioneers worked on the first innovative computers in government, academia and industry, and our members now work at the coalface of technology development across every industry.

In 2011, ACS brought together its own Cyber Taskforce from our 23,000 members to respond to the Federal Government's new cyber discussion paper, 'Connecting with Confidence', where we highlighted the need to develop co-ordination and a focus on the pipeline of cyber professionals.

To play our part in securing Australia's future, we continue to perform the role of trusted advisor to government, and deliver services to identify and certify ICT professionals you can trust, including through the Professional Standards Scheme that assures professionals have the specialist skills business can rely upon.

ACS is part of the global federation of professional ICT societies, the International Federation for Information Processing (IFIP), and the first professional body to receive accreditation under the International Professional Practice Partnership (IP3) – providing a platform for accreditation for ICT professionals and mutual recognition across international boundaries. The ACS currently chairs IP3 and plays a leading role in the professionalism of the ICT workforce.

IP3 has since gained global attention after successful engagements at the World Summit on the Information Society (WSIS) Forum in Geneva and the United Nations in New York, where the importance of ICT professionalism was acknowledged by the UN General Assembly President in 2015.

In May 2016 the President of IFIP participated in the European Foresight Cyber Security Meeting where he advocated that professionalism of the ICT workforce is "a key element in building trustworthy and reliable systems" and that it is important to ensure that "cyber security and cyber resilience is also a duty of care of the individual ICT professional".

As we move forward another 50 years, ACS will be there at the forefront meeting the challenges and opportunities of ICT, and supporting the growth and potential of ICT professionals in Australia.

Executive summary

As technology continues to evolve so also do the opportunities and challenges it provides. We are at a crossroads as we move from a society already entwined with the internet to the coming age of automation, Big Data, and the Internet of Things (IoT).

But as a society that runs largely on technology, we are also as a result dependent on it. And just as technology brings ever greater benefits, it also brings ever greater threats: by the very nature of the opportunities it presents it becomes a focal point for cybercrime, industrial espionage, and cyberattacks. Therefore, protecting it is of paramount priority.

This guide looks at some of the concerns facing us in the near future that include:

- Attack vectors such as botnets, autonomous cars and ransomware.
- Threats including data manipulation, identify theft, and cyberwarfare.
- Tangential issues such as data sovereignty, digital trails, and education and awareness.

Additionally, it provides some background to the nature of digital ecosystems and the fundamentals of cybersecurity.

Critically, this document clarifies the importance for Australia to take responsibility for its own cybersecurity, especially with regards to essential infrastructure and governance.

On the flip side – and as one of the fastest growth industries globally – developing our own cybersecurity industry is also an opportunity for economic growth, job creation, and education – ensuring Australia is well positioned for a future as a digitally advanced nation.

Finally, we look at some of the challenges that countries worldwide are currently dealing with in regards to cybersecurity, including:

- The need for more collaboration in order to mitigate threats.
- Education and awareness.
- The balance between privacy and security, and

Our aim is that this document provides an informative primer on the relevant issues facing Australia in relation to cybersecurity, to generate discussion and debate, and to raise awareness with regards to a fundamental building block of the technologically-dependent society which we have already become.

As you will read in the following pages, cybersecurity is not optional. It must form part of the design of every product, of every database, of every electronic communication. And – through education, awareness, and proactive change – we can all play a part in securing our future.

A brave new world

You're reading this document written with, laid out by, and printed using computers. From start to finish it existed as 0s and 1s – the binary blood of our modern world.

In fact, our lives today are codified by data: almost everything we do, and everything we depend on, involves data and the technology that uses it – there are scant few areas not touched by this revolution we call the **information age**.

CYBER SPEAK!

Every industry has its own lexicon, and the cyber world is no different. While built on technological foundations that we all know – computers, the internet, smartphones, and similar – as you delve deeper into the subject you start to encounter acronyms and technical concepts that you may not be familiar with.

And, if we're all to communicate on the subject of cybersecurity – across all sectors of government, business, industry, and academia – then it can help to familiarise yourself with the nomenclature associated with this diverse and compelling subject.

To this end we've included a Glossary on page 57. Feel free to flick back and forth as you read to ensure you get the most out this document, spending more time expanding your knowledge and less time scratching your head!

46%

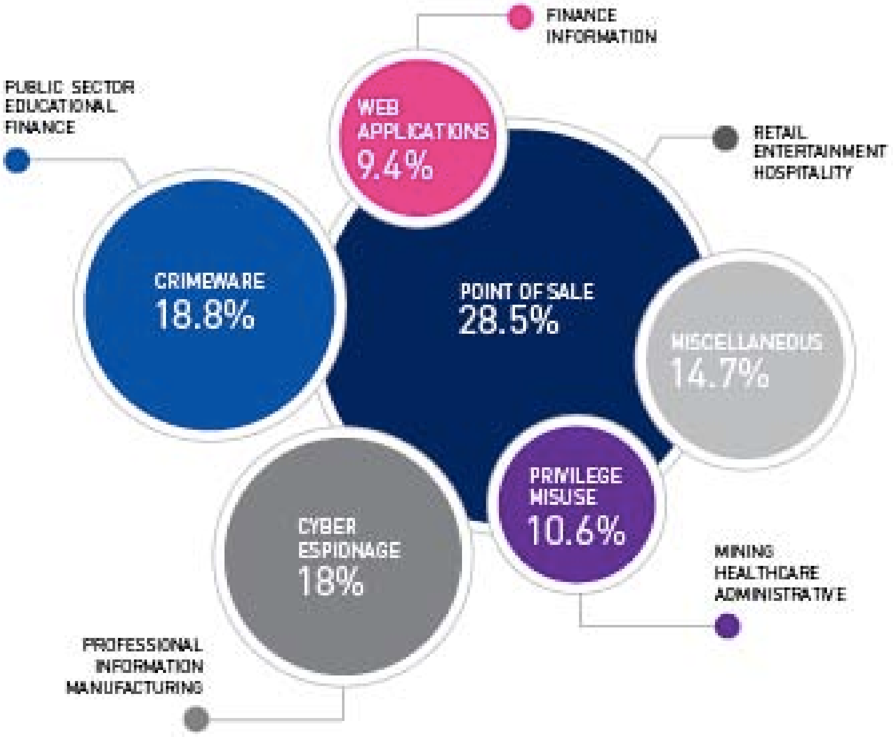
OF THE WORLD'S POPULATION IS CONNECTED TO THE INTERNET

What is cybersecurity?

As with any technological advance throughout history, whenever new opportunities are created, there will always be those that exploit them for their own gain.

THREAT VECTORS BY INDUSTRY

The vectors by which industries are compromised.
Source: Verizon 2015 Data Breach Investigations Report



LAST
TO KNOW

MORE THAN
90%
OF BREACHES ARE DISCOVERED BY EXTERNAL PARTIES

WHAT'S THE PASSWORD?

63%
OF BREACHES ARE CAUSED BY WEAK, DEFAULT, OR STOLEN PASSWORDS

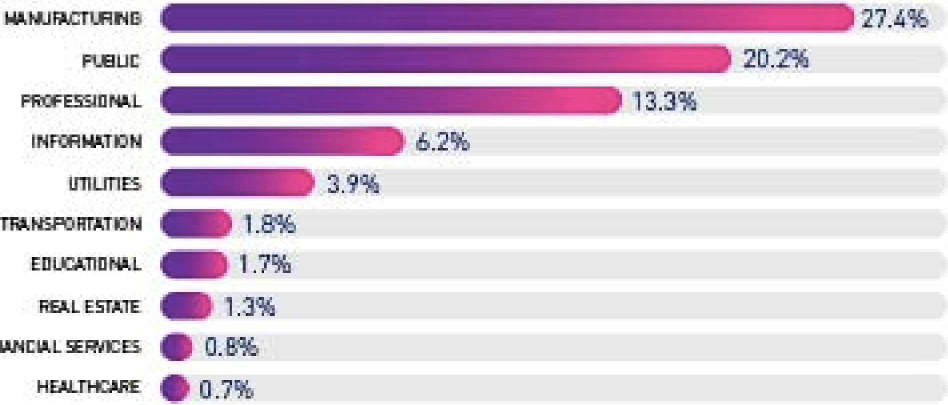
EASY HACKS, EASY BREACHES

Source: Verizon 2016 Data Breach Investigations Report

ES
reach

TOP 10 ESPIONAGE TARGETED INDUSTRIES

The most targeted industries in 2015.
Source: Verizon 2015 Data Breach Investigations Report



93% OF CASES HACKERS TOOK JUST MINUTES TO BREACH

WHILE COMPANIES TOOK WEEKS OR MONTHS TO DISCOVER

SHOW ME THE MONEY

95% OF WEB ATTACKS ARE FINANCIALLY MOTIVATED

EMPLOYEE MISTAKES

26% SEND SENSITIVE DATA TO THE WRONG PERSON

NEARLY 30% OPEN PHISHING EMAILS

12% DO CLICK THE LINK OR OPEN ATTACHED FILES

SIMPLE MISTAKES, COSTLY LOSSES

Source: Verizon 2016 Data Breach Investigations Report

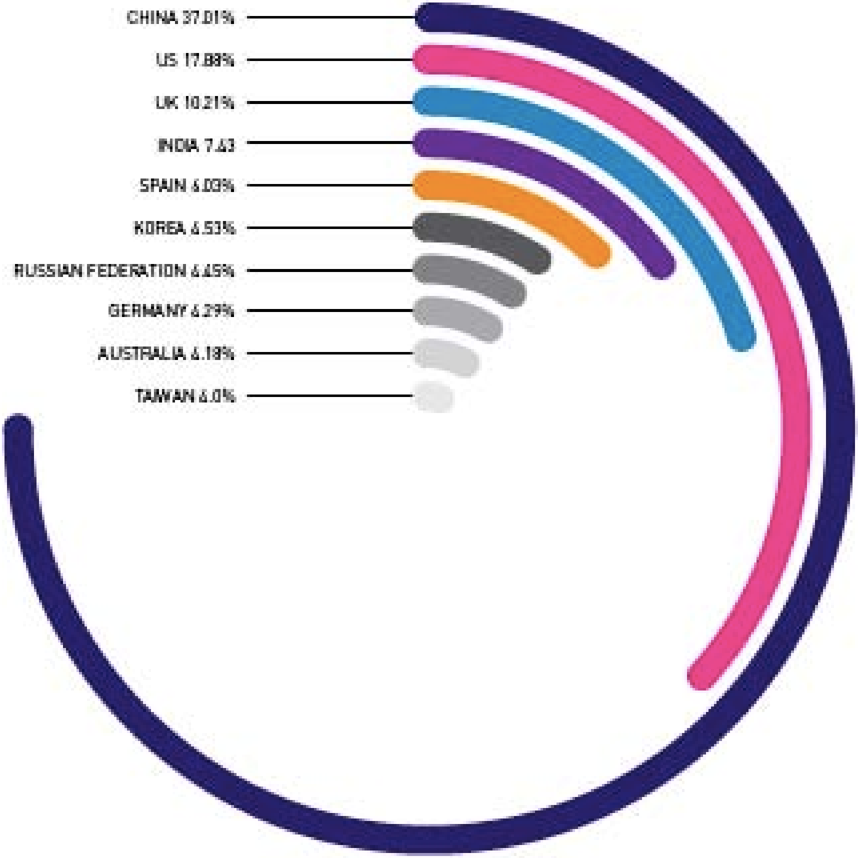
A world without cybersecurity

One the most damaging targets for a society embroiled in cyberwarfare is infrastructure.

Our reliance on automation focuses single points of failure that can have dramatic consequences if directed at power stations, communication networks, transport and other utilities.

Q2 2015 saw one of the highest packet rate attacks recorded... which peaked at 214 million packets per second (Mpps). That volume is capable of taking out Tier 1 routers, such as those used by Internet service providers (ISPs).

Akamai, State of the Internet Q2 2015 Report[10]



TOP 10 SOURCE COUNTRIES FOR DDOS ATTACKS, Q2 2015

Top sources of mitigated DDoS attacks on Akamai's network.
Source: Akamai State of the Internet Report, Q2 2015

Threats in the information age

> Every minute, we are seeing about half a million attack attempts that are happening in cyberspace.

Derek Manky,
Fortinet Global Security Strategist[5]

There were 19 distributed denial-of-service (DDoS) attacks that exceeded 100 Gbps during the first three months of the year, almost four times more than in the previous quarter. In some cases attackers don't even have to deliver on their threats. Researchers from CloudFlare reported that an extortion group earned $100,000 without ever launching a single DDoS attack.

Lucian Constantin,
Network World, 2016[28]

> **For $6 in Bitcoin, I can rent time on a DDoS tool and bring down most websites. Better yet, if I send just the right type of packet to their web servers, I can crash the site for free.**

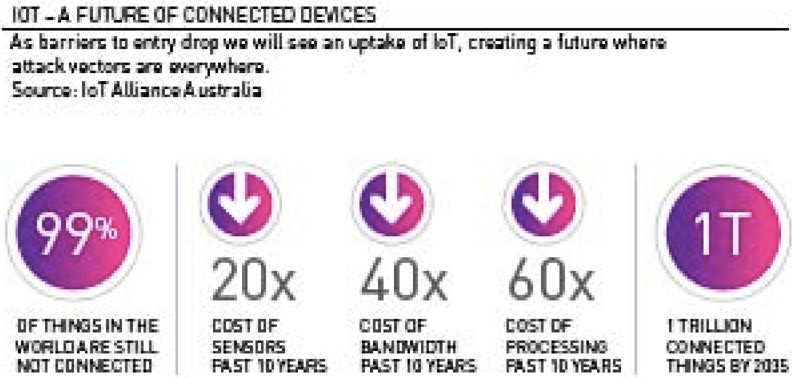
A Thief's Perspective (interview), Intel Security, 2015[14]

The Internet of Things (IoT)

Perhaps the most recognised buzzword of the moment, the Internet of Things (IoT) encompasses the many and varied devices currently on the market, or soon to be on the market, that will connect to and stay connected to the internet 24/7.

Typically this includes products like webcams, smart TVs, and even the

But this is just the beginning. IoT has the potential to encompass a lot



IOT – A FUTURE OF CONNECTED DEVICES

As barriers to entry drop we will see an uptake of IoT, creating a future where attack vectors are everywhere.

Source: IoT Alliance Australia

99%

OF THINGS IN THE WORLD ARE STILL NOT CONNECTED

20x

COST OF SENSORS PAST 10 YEARS

40x

COST OF BANDWIDTH PAST 10 YEARS

60x

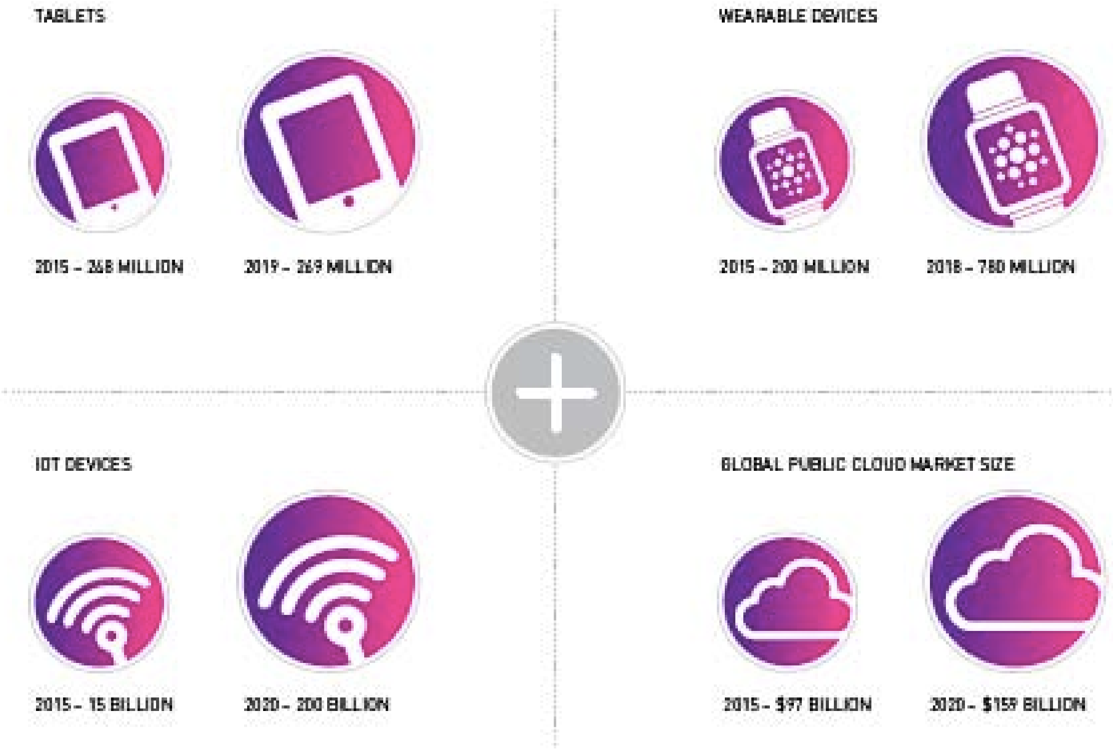
COST OF PROCESSING PAST 10 YEARS

1T

1 TRILLION CONNECTED THINGS BY 2035

Although a successful attack on industrial IoT devices with an installed base of hundreds of millions would likely cause havoc, one device at a key point in a critical infrastructure control system could be far more devastating.

McAfee Labs 2016
Threats Predictions[18]



MORE DEVICES, MORE THREATS

The growth in user-centric mobile and IoT devices will see greater exploitation of personal data.
Source: McAfee 2016 Threats Predictions

WHEN SECURITY IS AN AFTERTHOUGHT

One of the most potent botnets to date is **Lizardstresser**, by the infamous Lizard Squad DDoS group. In 2015 the group released the source code, allowing others to make their own. This has resulted in copy-cat groups and a stark increase in botnets-for-hire.

Lizardstresser relies on cheap IoT hardware to build large botnet armies, using shell scripts (simple text-based scripted programs) to scan IP ranges and to attempt access using hardcoded usernames and passwords (usually all related to administrator logins).

It's so successful because many IoT devices are manufactured with the same default login credentials. Additionally, these same devices are also often simply plugged in and turned on, and have unfettered access to the internet through whatever corporate or home networks they are connected to. This makes them easy targets to enslave into botnets.[18]

Attacks on automobile systems will increase rapidly in 2016 due to the rapid increase in connected automobile hardware built without foundational security principles.

McAfee Labs 2016
Threats Predictions[18]

Autonomous systems

As technology continues to permeate our lives, we move from operating technology to integrating with it. This is especially true of autonomous systems that are by definition designed to blend in with our society, becoming second nature.

By the same token however, reliance on such systems makes the outcome of their abuse potentially more damaging. Typically, these technologies also integrate into critical infrastructure, such as payment systems and – in the case of autonomous cars – the transport network, making protecting them from a cybercrime a pivotal focus for cybersecurity.

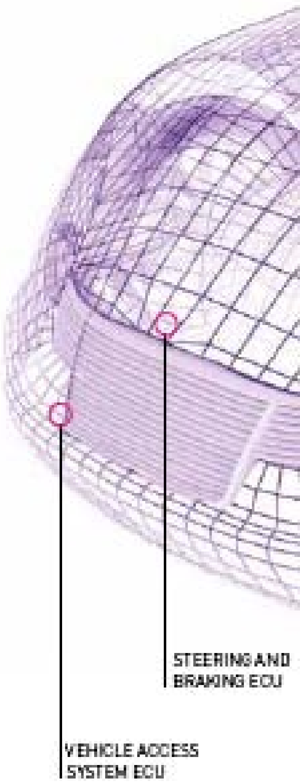
Driverless cars and transport

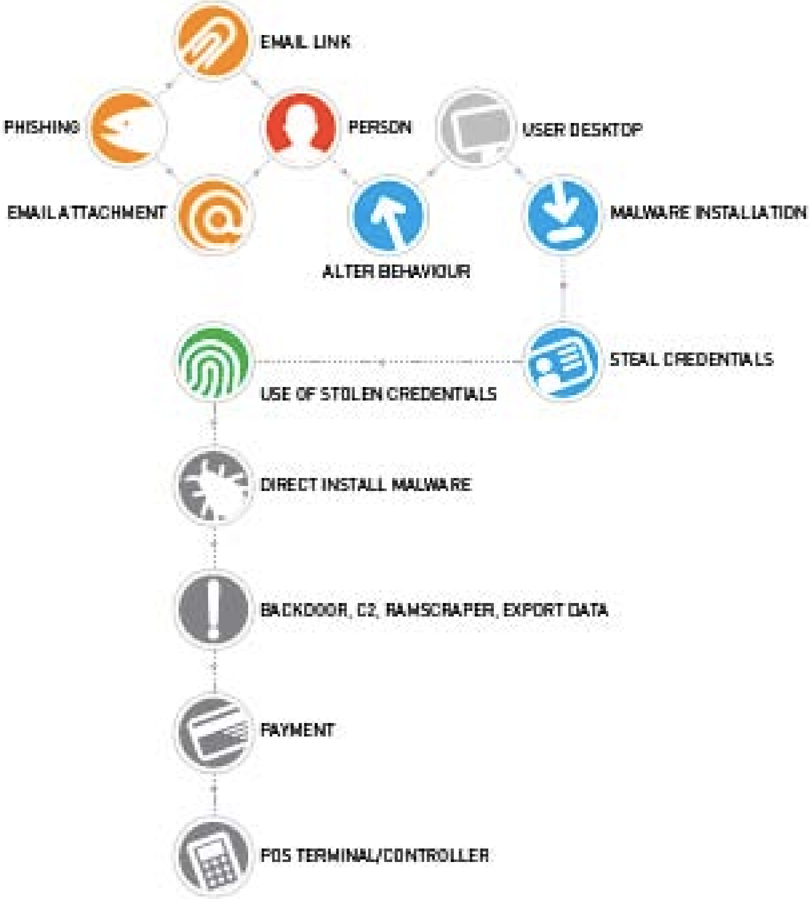
At the moment, driverless cars are stealing the limelight of autonomous

Similar abuse of access has also been demonstrated with cars from Mercedes, BMW, Toyota, Audi and Fiat – all due to poor security in the design process.[20 21 22]

It's not hard to see that in the wrong hands such abuse could result in cars being used as weapons to maim or kill pedestrians – or even the occupants themselves – on the road. According to Business Insider in its Connected-Car Report, there will be 220 million autonomous cars on the road by 2020.[23]

[illegible] 2016 Threats Predictions





BIRTH AND REBIRTH OF A DATA BREACH

An example of how one breach can lead to another (in this case, harvesting payment data of consumers after first breaching a POS vendor).
Source: Verizon 2016 Data Breach Investigations Report

They'd been inside our network for a long period, about two years. And the way it was described to us was they're so deep inside our network it's like we had someone sitting over our shoulder for anything we did.

Daryl Peter, IT Manager,
NewSat 2012-2014[60]

WHAT ABOUT WEARABLES?

Wearables are rapidly gaining popularity with smartwatches such as the Apple Watch and Samsung Gear, as well as exercise wearables like those from FitBit and Jawbone. According to ABI Research, an estimated 780 million wearable devices will be in circulation by 2019.

Now you might be wondering just what would be so bad about hacking a fitness wearable? This is exactly the line of thinking that allows cybercrime to occur.

Wearables are tracking all sorts of personal information including GPS location, blood pressure, heart rate, and anything else you feed them such as weight or diet. Such personally identifiable information could be used as a base to target you for spear-phishing, or aid in identity theft. But the real opportunity is these devices linking to your smartphone, where phone numbers, more personally identifiable information, emails, web logins etc. could theoretically be compromised.

Cyberwarfare

Most modern countries now are treating cyberspace as another military domain, in addition to land, air and sea.

Dmitri Alperovitch, Cybersecurity industry executive[23]

Once the domain of science fiction, cyberwarfare is now very real, with most superpowers now having dedicated cyberwarfare divisions of the military. And while there have been few known, co-ordinated cyberattacks on physical targets, we don't need a crystal ball to predict the future: they will only increase.

It's telling that we are now in an age where governments, political groups, criminals and corporations can engage in cyberespionage, cyberwarfare, and cyberterrorism

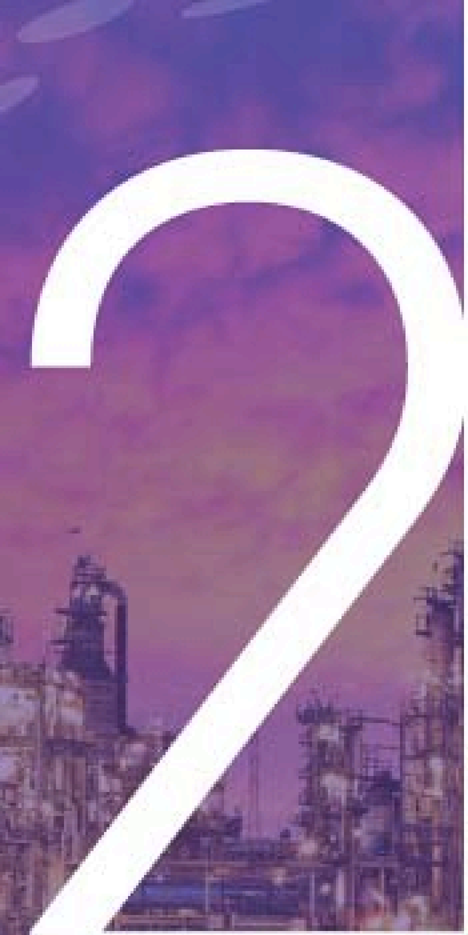
Automated attacks

Much of what we talk about with regards to 'hacking' is a function of people at keyboards finding and

ENERGETIC BEAR

One of the more well-known nation-state sponsored tools of cyberwarfare currently active is Energetic Bear. First uncovered in 2012, and believed to be sponsored by Russia, Energetic Bear used the Havex Trojan to gain access to company networks, particularly those in the energy sector, though it has also been found in manufacturing, construction, health care and defence companies.

Primarily designed for cyberespionage, when the threat was first mapped in 2014 by security firm Kaspersky Labs, it identified nearly 2,800 victims worldwide, affecting countries including the US, Spain, Japan and Germany.[44]



230,000

PEOPLE LOST POWER WHEN 30 SUB-STATIONS IN WESTERN UKRAINE WERE SHUT DOWN VIA A REMOTE ATTACK

America's top spies say the attacks that worry them don't involve the theft of data, but the direct manipulation of it, changing perceptions of what is real and what is not.

Patrick Tucker, Defense One[27]

WHEN SOFTWARE KILLS

It's easy to forget that computers can have life-threatening consequences. Here are some well-known examples of what happens when technology fails due to small mistakes in computer code.

Therac 25

This is so well known that it's now taught in computer science curriculums. Therac 25 was a Canadian medical machine designed to help save lives by administering targeted doses of radiation to kill cancer. Instead, a rare software glitch saw patients receiving 100 times the necessary dose. In a period from 1985-1987 five patients died, while many others were

Toyota

Toyota
worldw
faults w
Control
death o

Tesla'

In July
relying
his Tes
detect

These
softwa
ulation
result i
undete
Military

America's top spies say the attacks that worry them don't involve the theft of data, but the direct manipulation of it, changing perceptions of what is real and what is not.

Patrick Tucker, Defense One[27]

WHEN SOFTWARE KILLS

It's easy to forget that computers can have life-threatening consequences. Here are some well-known examples of what happens when technology fails due to small mistakes in computer code.

Therac 25

This is so well known that it's now taught in computer science curriculums. Therac 25 was a Canadian medical machine designed to help save lives by administering targeted doses of radiation to kill cancer. Instead, a rare software glitch saw patients receiving 100 times the necessary dose. In a period from 1985-1987 five patients died, while many others were seriously injured.[29]

Patriot missile

During the Gulf War in 1991 a Patriot missile failed to intercept a Scud missile due to a software fault, resulting in the death of 28 US soldiers and injuring 100 others.[30]

Toyota's ETCS

Toyota recalled 8 million vehicles worldwide starting in 2009 after faults with the Electronic Throttle Control System resulted in the death of 89 people.[31]

Tesla's autopilot

In July 2016 a man died while relying on the autopilot function of his Tesla Model S when it failed to detect a trailer, crashing into it.[32]

These are examples of unintended software faults, but subtle manipulation of data could intentionally result in loss of life, and remain undetected until this occurs. Military officials in the US have even raised concerns that Chinese hackers known to have infiltrated defence contractors over the last decade could have already altered code for weapon systems, sitting dormant until the next major conflict.[33]

Data manipulation

Not all attacks are about theft or destruction. A more sinister cause is the manipulation of data in place – such that machines can be controlled – or the wrong information reported to human operators without their knowledge.

It's clear if a cybercriminal releases stolen usernames and passwords on the web. It's much less clear if

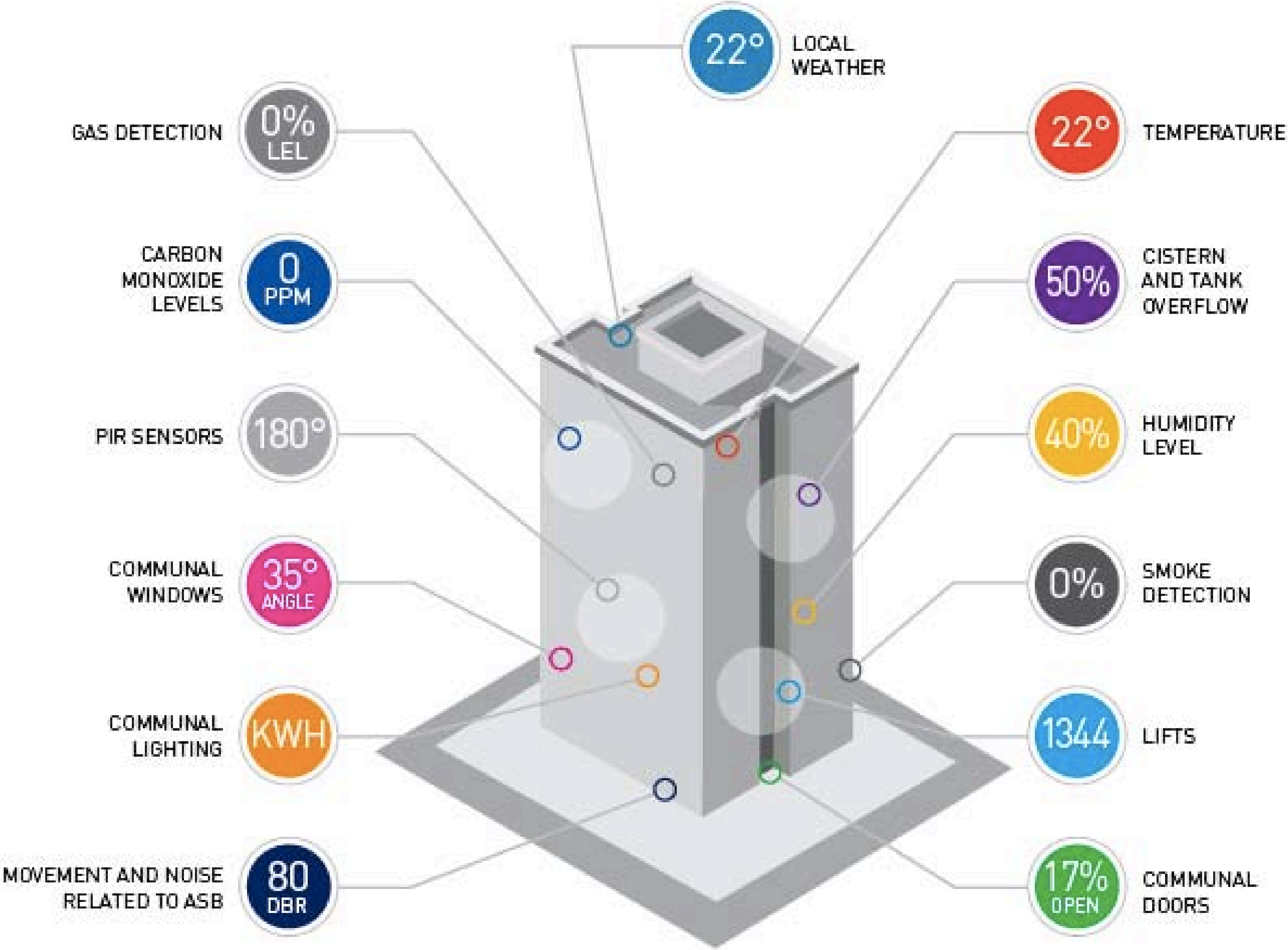
By way of example, in 2015 Juniper Networks announced it had discovered multiple backdoors in

The biggest threats in cybersecurity today are around the large scale proliferation of targeted attacks – from breach and email distribution of socially engineered ransomware to potentially harmful attacks on critical infrastructure like energy networks.

Rodney Gedda,
Senior Analyst, Telsyte[53]

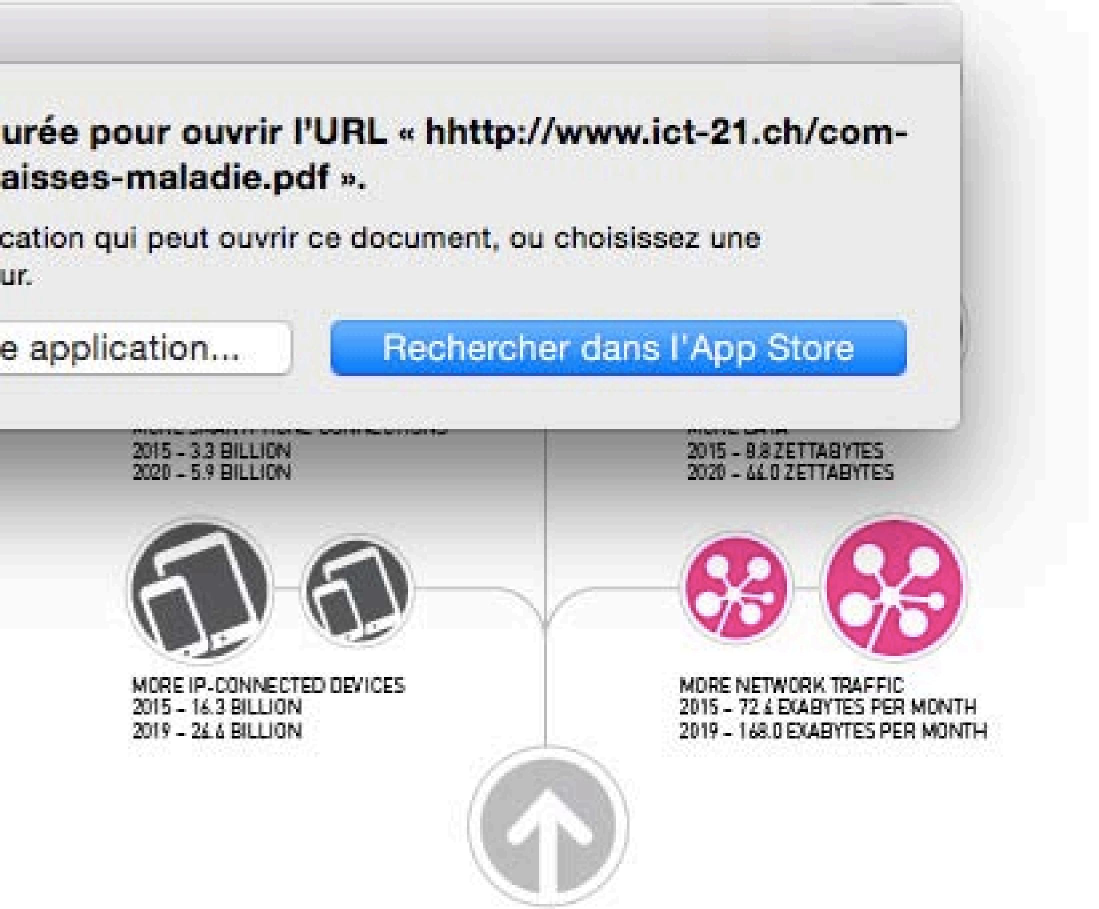
BLAST FROM THE PAST

Perhaps one of the more prominent examples of cyberwarfare – even before the internet became ubiquitous – comes from the cold war in 1982 when a Siberian oil pipeline exploded, creating at the time one of the largest non-nuclear explosions in history, so large it was visible from space. Later the cause was revealed to be a Trojan horse implanted by the US in pipeline equipment sold from a Canadian company on to Russia. End result: economic sabotage facilitated by computer software.



SMART CITIES – BRITAIN'S NEIGHBOURHOOD@BROOMHILL PROJECT

A small sample of the types of IoT sensors in a smart city apartment block.
Source: IoT Alliance Australia



urée pour ouvrir l'URL « hhttp://www.ict-21.ch/com-
aisses-maladie.pdf ».

cation qui peut ouvrir ce document, ou choisissez une
ur.

THE GROWING CYBERATTACK SURFACE

More devices, more users, more data – every year.
Source: McAfee 2016 Threats Predictions

Industry and the individual

While large security breaches make the news, the majority of cybercrime involves fraud targeting businesses and individuals. Here, a mixture of malware and social engineering can see financial fraud resulting in the loss of thousands, all the way up to millions, of dollars.

> Utilising the cumulative bandwidth available to these IOT devices, one group of threat actors has been able to launch attacks as large as 400Gbps.

Arbor Networks on LizardStresser[19]

THE WORLD WE LIVE IN

Facebook CEO, Mark Zuckerberg, has been observed in a promotional photo for Instagram with his laptop in the background sporting tape covering both the camera and the microphone – the implication being he doesn't trust his own machine is secure from cyberespionage.[24]

If the CEO of one of the world's technology innovators can't necessarily trust his own computer, what does that mean for the rest of us?

The future in our hands

Asia-Pacific is rapidly emerging as a potential market for cybersecurity solution providers, driven by emerging economies such as China, India and South-East Asian countries.

Cybersecurity Ventures[48]

$639 Billion

ESTIMATED WORTH OF
THE CYBERSECURITY
INDUSTRY BY 2023

THE 100% SECURE COMPUTER

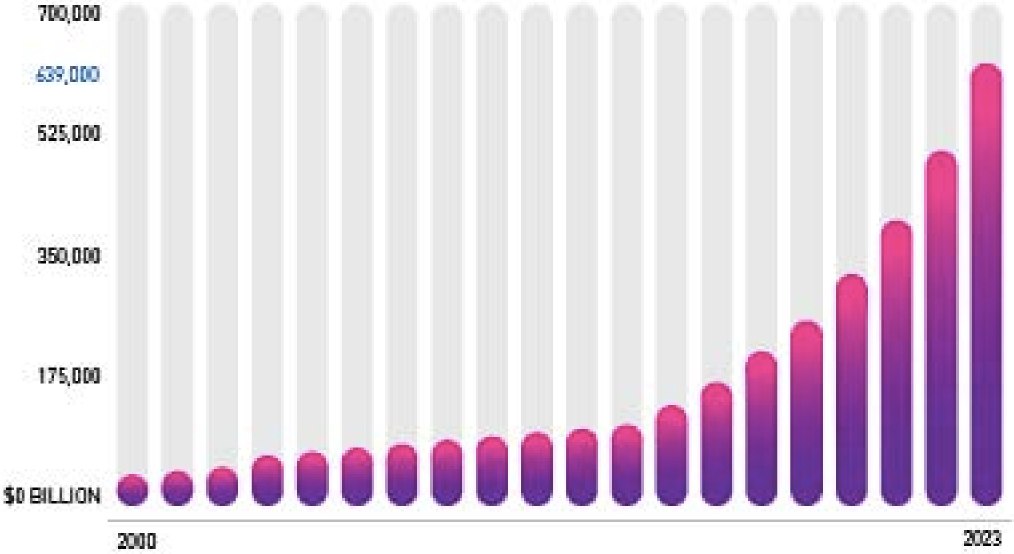
When it comes to security you can never completely eliminate risk, you can only minimise and mitigate it – there is no such thing as the 100% secure system.

The adage goes that the only **truly** secure computer is locked in a lead box, buried fifty feet underground, sealed with concrete, with no wired or wireless connections in or out.

And turned off.

Which is to say, not a very useful computer.

Ultimately, for the majority of cases, security is about making the cost of entry higher than the value of the assets being protected.



ESTIMATED GLOBAL CYBERSECURITY SPENDING TO 2023

An estimated ten-fold increase in spending as cybercrime becomes a pivotal focus.
Source: IT-Harvest

Opportunities

The threats are many and varied, but so are the opportunities – technology constantly teases us with new ideas, new products, and new ways of living our lives. It also presents new economic opportunities, new ways of doing business, and new ways to make a difference.

The data-driven economy

If there's one prediction we can make about the next decade it is this:

to increase exponentially – already we are creating new ways to mine data and produce new services (right

Cyberattacks are costing global businesses as much as $500 billion per year... The banking and financial sectors have led the way as top targets for cyberattacks in the last five years, with IT and telecom, defence, and the oil and gas sectors following behind.

Cybersecurity Ventures[48]

> **Security is as much about software as it is about awareness. It takes sophisticated coding to develop ransomware, but only one click to activate it.**
>
> Rodney Gedda,
> Senior Analyst, Telsyte[53]

Technology as wealth creation

The benefits of technology have created tremendous wealth over the last decade – you only need to look at household names like Google, Apple, or Facebook for examples.

As we move to a world populated by internet-connected devices – from your car to your fridge, your children's toys and even the clothes you wear – there are still Googles and Apples and Facebooks to be discovered.

This alone represents tremendous opportunities for Australia's ICT

Cybersecurity as job growth

According to SEEK, cybersecurity roles are already in demand, having grown 57% in the last year.[50] This includes jobs like Security Analyst, Security Architect, Security Engineer, and Chief Information Security Officer, all of which represent the new type of opportunities that are developing in the workforce.

We have the skills and talent in Australia to support and capitalise on this growth, which will only see more demand as the importance of cybersecurity in the development

Australia can galvanise its own cybersecurity industry with government and private-sector support – but part of this involves addressing the need for more trained scientists, mathematicians, engineers, and ICT workers. As a nation we need a scientifically literate community capable of engaging in a national conversation on vital technology issues like cybersecurity.

Leveraging technology talent

Which leads us to the talent we already have – Australia has some of

Challenges

While the opportunities are clear for ICT in Australia and the nation as a whole, there are a number of challenges we need to address. Ideally, all sectors from government and industry, to enterprise and academia, need to play a part in the development and promotion of cyber education, skills and products.

Leadership

Lack of leadership is a key challenge, if only because it takes a concerted

The foundation of any society is trust, as well as the foundation for security itself. Security helps build

Many of these devices are always on, always listening, and always communicating... raising concerns about transparency and privacy. With homeowners unprepared and ill-equipped to detect and remediate most security threats, some highly successful attacks will collect personal info on an ongoing basis.

McAfee Labs 2016
Threats Predictions[15]

LEARNING FROM HISTORY

In 1958 when the National Defense Education Act was signed into law in the US, the goal was to provide funding to education institutions at all levels. The impetus was Russia beating the Americans to space, and a national feeling that America was falling behind. Over a period of four years $USD1 billion was spent on science education.[57]

Today we face a similar situation where we are already in a skills shortage for ICT in Australia, and if we are to create a blossoming cybersecurity ecosystem we will first need a strong emphasis on and promotion of STEM-based skillsets for Australians throughout the educational pathway.

695k

THE DEMAND FOR SKILLED ICT WORKERS WILL INCREASE FROM 638K TODAY TO 695K BY 2020

Collaboration

If there's one lesson to learn from cybercriminals it is this: collaboration is king. Analysis of attacks over the

on the next company, and the next. In order to stop it, free sharing of information among business and enterprise, cybersecurity professionals,

As we move to a knowledge economy, we will need more scientists, mathematicians, engineers and programmers. Promotion and

Infrastructure has always been considered a legitimate target. In WWII we bombed and destroyed the electrical infrastructure of our enemies. Now we have the ability, through a cyberattack, to just shut the grid down.

General Michael Hayden,
former CIA & NSA director[85]

YOU ARE WHAT YOU DO

The famous adage 'you are what you eat' has an interesting parallel in the digital world – it's easy to forget that almost anything you do online involves data, and that this data tells a story about who you are and where you have been. From web browsing to smartphones, you and everyone you know is tracked, logged, and the data shared among a variety of services.

Whether it's a connection from your IP address in a application's log, or cookies about a website stored on your computer, every day you leave a trail – often called your **digital exhaust** or **data exhaust**.

While much is for analytics, once it's out there you have no control over it, let alone ownership (most applications and programs will prompt you to sign over your permission on first use). Even Microsoft's latest Windows 10 comes with 'mandatory' data collection about your use of the operating system.

McAfee's 2016 Threats Predictions report notes that "within the next five years, the volume and types of personal information gathered and stored will grow from a person's name, address, phone number, email address, and some purchasing history to include frequently visited locations, 'normal' behaviours, what we eat, watch, and listen to, our weight, blood pressure, prescriptions, sleeping habits, daily schedule, and exercise routine."[15]

The more information that is out there about you, the greater the risk there is for it to be abused. Not just by cybercriminals seeking to develop correlations that can be used in fraud such as identity theft, but also intentional or unintentional misuse by companies or government services.

> **We're entering this world where everything is catalogued and everything is documented and companies and governments will be making decisions about you as an individual based on your data trail. If you want to be considered an individual and not just a data point, then it's in your interest to protect your privacy.**
>
> Josh Lifton, CEO of Crowd Supply[55]

procedures are as essential to the operation of any business. If you are in an organisation that currently does not have policies and procedures in place to both prevent and mitigate cybercrime, now is a good time to start.

Finally, perhaps the biggest hurdle here is educating the sector, particularly among CEOs and Boards. There is a dearth of knowledge among decision makers on cybersecurity risks and the investment required to manage them.

According to a survey by The Economist Intelligence Unit, IT and security leaders in Australia think cybersecurity is the #1 issue at present – but less than 6% of C-Suite executives agree. There is a large disconnect between the reality of threats and awareness of them at the executive level.[58]

Legal and regulatory

While collaboration is key, the good

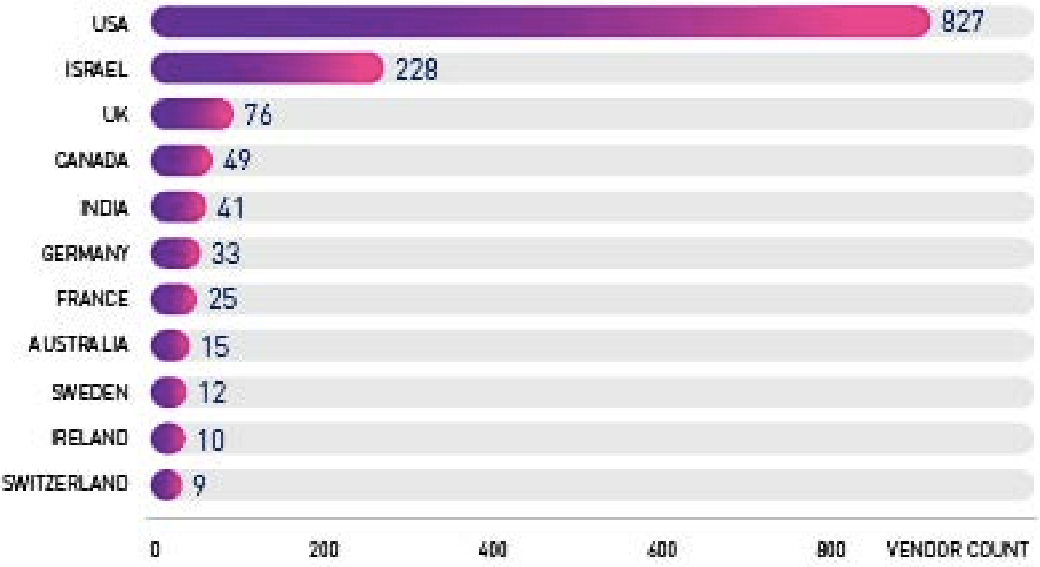
information could breach privacy laws. Where necessary, reviewing laws and regulations to facilitate better communication and collaboration for the purposes of cybersecurity may be required.

Services and privacy

Increasingly in our digital world services come at the cost of privacy. There is an inherent trade-off, and while we accept some encroachment of privacy over data we share, it nonetheless remains a fundamental building block of our society and must factor into any solutions.

We now know there is no such thing as a 100% secure system, any personal data stored on any server be it government, enterprise, or otherwise has the possibility of being breached and personal information being made public.

It's also important to note how the type and volume of data stored also acts as a target for cybercrime, in



CYBERSECURITY VENDORS BY COUNTRY AS AT 2016

USA and Israel currently lead cybersecurity research and products.

Source: IT-Harvest

the Australian Centre for Cyber Security, and Greg Austin, Professor Australian Centre for Cyber Security, succinctly noted, "you cannot demand mass surveillance and metadata retention without there being costs that make us much less safe. Metadata retention is retrospective – it won't predict or stop crimes, but it will open up breaches that bad actors can waltz through."[54]

The DDoS against the Australian Bureau of Statistics eCensus servers in August this year demonstrated just how easily a service can be knocked offline and, typically, DDoS attacks can often hide secondary attacks aimed at breaching a system. Any

data be de-identified when possible to limit the damage from data breaches as well as preserve privacy of individuals.

Perception and practicality

Finally, there is a perception that Australia is not currently a technology leader – not just in cybersecurity, but as a whole. The current view with technological products is that it's better if it comes from overseas.[56]

This is a perception that needs to change. We have all the ingredients to create world-class products and services in Australia, particularly in relation to ICT and cybersecurity

Practically, it also helps for the private sector and the ICT industry as a whole to seek Australian products when canvassing for solutions.

It's a market economy... the price of a compromised system of $5 shows you exactly how far down the road we are of the cybersecurity story.

Tim Wellsmore, Former Manager, Fusion Special Intelligence 2013-16[85]

Looking to the road ahead

It's clear cybersecurity is pivotal to both the economic future of Australia and indeed the fabric of our society. As we develop and embrace more and more technology, this will become ever more important.

> For all my enthusiasm for government's responsibilities in cyberspace, good cyber policy requires the cooperation and creativity of academia and industry. Indeed, government needs to be challenged by academia and industry.

Malcolm Turnbull,
Prime Minister of Australia.
September 2016

At the end of the day this really is about stewardship for us as a country. It's really about them, about the next generation. Bear in mind that they are only entrusting us with their future for a little while longer, because they're coming, and they're coming with or without us.

Adrian Turner, CEO, Data 61[93]

- Strong cyber defences to better detect, deter and respond to threats and anticipate risks.
- Working with international partners through the new Cyber Ambassador and other channels to champion a secure, open and free internet while building regional cyber capacity to crack down on cyber criminals and shut safe havens for cybercrime.
- Help Australian cybersecurity businesses to grow and prosper, nurturing our home-grown expertise to generate jobs and growth, and support new business models, markets and investment.
- Create more Australian cybersecurity professionals by establishing Academic Centres of Cyber Security Excellence in universities, fostering skills throughout the education

What role can you play?

We know cybersecurity isn't just about technological defences; it's also about people and the way we handle data in the workplace, the emails we click or the sites we browse, and how good we are at identifying social engineering and other scams and tricks.

Good cybersecurity needs both good technological solutions and good people solutions. And, it requires all of us to participate.

In which case – whatever your responsibilities – what role can you play to make a difference?

Government

If you work in government, Prime Minister Malcolm Turnbull has already laid out in his address at the

Education and research

If you work in academia, university, research or other educational institutions you have a great opportunity to see how cybersecurity principles can either be applied to your work, or considered in the application and delivery of your work.

Educational institutions from pre-school through to university all play a vital part in the promotion of STEM-based skills upon which disciplines such as cybersecurity are based. And, as we've noted in this guide, we are already in a shortage of skilled cybersecurity professionals. What you can do to promote this challenging and rewarding career pathway is of benefit not just to your students but Australia as a whole.

Within research and academic institutions the results of your work may be critical in any number of ways, and so if not already the access to and handling of data needs to be guided by solid cybersecurity principles in order to minimise or prevent any loss through a cyberattack.

Business and industry

In your workplace, the single most important step you can take is to draw attention to cybersecurity – or the lack of it – within your company. If you are able, write a cyber security strategy focusing policies, security culture, education training and awareness programs, risk management processes and technical controls.

Every business plays its part just as every one of us plays a part. The smartphone in your pocket could act as a vector for the theft of your own personal data, or as a vector of attack in the company you work for. It's in everyone's best interests to be informed, prepared, and responsible. Remember, cybersecurity is not just a safety risk, it's a business risk.

If you are an executive, it is incumbent on management to be well-versed in cybersecurity language and the realities of cybersecurity threats to your business. If not already, appoint a CISO (Chief Information Security Officer) or CSO (Chief Security Officer) and ensure they have a place in board-level decision making. Also ensure clear and easy lines of communication between security, IT staff and upper management – these employees are your front line of defence.

Remember that just as your business does not operate in a vacuum, the same is true for cybersecurity. You may have all the best policies and procedures in the world but be vulnerable through a third party such as suppliers or distributors with which you do business. It is important to ensure they, too, have adequate cybersecurity preparations and resources to protect themselves and the businesses they work with – and you can help them.

Finally, it's important to ensure your IT staff and security specialists are trained with up-to-date qualifications, as well as ensuring the have the necessary skills and expertise, and are certified to a recognised standard.

You, the individual

Because we all use a variety of devices every day, cybersecurity isn't just about protecting corporate networks or organisational assets.

Each of us has plenty of data – personal information – that should remain personal and not be used against us for extortion, identity theft, or as part of a scam.

It's telling that we lock our doors when leave home, or lock our cars when we arrive at work, and yet don't consider the safety of the data on our computers when we browse the web or install an application.

And there's actually a lot you can do to help ensure your data remains yours. There are plenty of guides online, but a good summary includes:

- Use complex passwords over simple ones, and don't re-use passwords between sites and services. If you find passwords hard to remember, use a password manager.
- When on offer, use two-factor authentication. This is becoming more common now with various services to ensure others can't log in as you, even if they manage to attain your passwords.
- Learn to recognise phishing emails – listen to that nagging voice in your head: if it sounds suspicious, it is. Banks, government services, and reputable companies won't ask for your login details over email.
- Don't open files from someone you don't know, and don't download or install any files delivered through pop-ups or pop-unders during web browsing.
- Keep your operating system and your applications up-to-date with the latest patches.

There's plenty more to learn. See the Online Resources on page 52 for a good place to start.

The five pillars of cybersecurity readiness

As the peak body for ICT professionals in Australia, the ACS considers the following to be the five core pillars of cybersecurity readiness.

1

Education and Awareness

First and foremost, it's essential that cybersecurity forms part of the conversation in every organisation, from the lunch room to the boardroom. Only through keeping cybersecurity front of mind can it form part of the decision-making

2

Planning and Preparation

A cybersecurity incident isn't an 'if' but a 'when', and to that end, preparation is essential. This can include management systems, best practice policies, IT auditing, and dedicated staff responsible for cybersecurity operations.

3

Detection and Recovery

When a breach happens, the quicker it is detected and responded to, the greater the chance of minimising loss – be it financial, reputational, or otherwise.

How quickly can your organisation

4

Sharing and Collaboration

As we've covered in this guide, collaboration is essential to mitigating current and future risks.

Sharing the results of your breach analysis with government and industry can help stop a known attack vector hitting other organisations. In turn, your company may be able to prevent an exploit by learning from a breach that another organisation shared.

Also consider joining or providing information to an ISAC (Information Sharing and Analysis Centers, www.nationalisacs.org) if there is an equivalent for your industry.

In some cases, your organisation may be bound by legislative requirements to report an incident. At a minimum, a breach should be reported to government or organisations such as AusCERT (www.auscert.org.au) and the Australian Centre for Cyber Security (www.acsc.gov.au).

5

Ethics and Certification

It may initially seem a less practical pillar, but the difference between a 'white hat' hacker and 'black hat' hacker is mindset.

In any company or organisation, ethics plays a role and should be of particular concern when it comes to cybersecurity. While some organisations, such as defence, will have their own means to vet credentials, for an industry as diverse and skilled as ICT it helps if professionals can demonstrate adherence to a code of ethics through membership of a professional institution.

Many professional organisations hold their members to standards that ensure the reputation and respectability of a profession is preserved. ACS, for example, has a code of ethics all Certified Professionals must abide by, in addition to other requirements such as demonstrating continued education and personal development in their chosen professional field of expertise.

ONLINE RESOURCES

For further reading and more information, visit the following websites:

- Australia's Cybersecurity Strategy
  cybersecuritystrategy.dpmc.gov.au
- Australian Center for Cyber Security
  www.acsc.gov.au
- Australian Computer Emergency Response Team (AusCERT)
  www.auscert.org.au
- Australian Cybercrime Online Reporting Network (ACORN)
  www.acorn.gov.au
- Australian Internet Security Initiative
  www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative
- Australian Signals Directorate – Top 4 Mitigation Strategies
  www.asd.gov.au/infosec/mitigationstrategies.htm
- Australian Signals Directorate – CyberSense Videos
  www.asd.gov.au/videos/cybersense.htm
- Australian Government – Stay Smart Online
  www.staysmartonline.gov.au
- ACCC – Scam Watch
  www.scamwatch.gov.au
- Australian Computer Society (ACS)
  www.acs.org.au

Through the looking glass

The following is a snapshot – just a sample – of the stories that made the news during the production of this guide. These headlines give you an insight to the ongoing, every day, occurrences of what happens in the absence of cybersecurity.

'LINKEDIN USER? YOUR DATA MAY BE UP FOR SALE'[61]

'EASYDOC MALWARE ADDS TOR BACKDOOR TO MACS FOR BOTNET CONTROL'[63]

'LIZARDSTRESSER BOTNETS USING WEBCAMS, IOT GADGETS TO LAUNCH DDOS ATTACKS'[65]

'DDOS ATTACK TAKES DOWN US CONGRESS WEBSITE FOR THREE DAYS'[67]

'HACKERS FIND 138 SECURITY GAPS IN PENTAGON WEBSITES'[69]

'HACKER STEALS 45 MILLION ACCOUNTS FROM HUNDREDS OF CAR, TECH, SPORTS FORUMS'[71]

'10 MILLION ANDROID DEVICES REPORTEDLY INFECTED WITH CHINESE MALWARE'[73]

'THIEVES GO HIGH-TECH TO STEAL CARS'[75]

'CROOKS ARE WINNING THE 'CYBER ARMS RACE', ADMIT COPS'[77]

'A HACK WILL KILL SOMEONE WITHIN 10 YEARS AND IT MAY HAVE ALREADY HAPPENED'[79]

'CHINA HACKED US BANKING REGULATOR'[81]

'APPLE DEVICES HELD FOR RANSOM, RUMOURS CLAIM 40M ICLOUD ACCOUNTS HACKED'[62]

'RESEARCHERS DISCOVER TOR NODES DESIGNED TO SPY ON HIDDEN SERVICES'[64]

'RESEARCHERS FOUND A HACKING TOOL THAT TARGETS ENERGY GRIDS ON THE DARK WEB'[66]

'CITING ATTACK, GOTOMYPC RESETS ALL PASSWORDS'[68]

'POLITICAL PARTY'S VIDEO CONFERENCE SYSTEM HACKED, ALLOWED SPYING ON DEMAND'[70]

'ONLINE BACKUP FIRM CARBONITE TELLS USERS TO CHANGE THEIR PASSWORDS NOW'[72]

'ANDROID RANSOMWARE HITS SMART TVS'[74]

'HACKERS CAN USE SMART WATCH MOVEMENTS TO REVEAL A WEARER'S ATM PIN'[76]

'IDENTITY FRAUD UP BY 57% AS THIEVES 'HUNT' ON SOCIAL MEDIA'[78]

'WHY YOU SHOULD DELETE THE ONLINE ACCOUNTS YOU DON'T USE ANYMORE – RIGHT NOW'[80]

'MASSIVE DDOS ATTACKS REACH RECORD LEVELS'[28]

'HACKER DEMONSTRATES HOW VOTING MACHINES CAN BE COMPROMISED'[89]

'FTC WARNS CONSUMERS OF RENTAL CAR DATA THEFT RISK'[90]

'YAHOO CONFIRMS MASSIVE DATA BREACH, 500 MILLION USERS IMPACTED'[91]

Fast facts

It's hard to choose just a handful of facts that highlight the threats and opportunities facing Australia, but here is a sample.

THREATS

IN 2014-15 CERT (COMPUTER EMERGENCY RESPONSE TEAM) AUSTRALIA RESPONDED TO

11,733

INCIDENTS, 218 OF WHICH INVOLVED SYSTEMS OF NATIONAL INTEREST OR CRITICAL INFRASTRUCTURE. OF THESE, ENERGY, BANKING AND FINANCE, AND COMMUNICATIONS WERE THE TOP THREE TARGETS.[82]

THE AUSTRALIAN GOVERNMENT DEPARTMENT OF COMMUNICATIONS HAS REPORTED THAT THE AVERAGE COST OF A CYBERCRIME ATTACK TO A BUSINESS IS AROUND

$276,000[82]

65

THE WORLD ECONOMIC FORUM'S GLOBAL RISKS 2015 REPORT HIGHLIGHTED CYBERATTACKS AND THREATS AS ONE OF THE MOST LIKELY HIGH-IMPACT RISKS. IN THE UNITED STATES, FOR EXAMPLE, CYBER CRIME ALREADY COSTS AN ESTIMATED

$US100

BILLION A YEAR.[50]

IOT SENSORS AND DEVICES ARE EXPECTED TO EXCEED MOBILE PHONES AS THE LARGEST CATEGORY OF CONNECTED DEVICES IN 2018, GROWING AT A

23%

COMPOUND ANNUAL GROWTH RATE (CAGR) FROM 2015 TO 2021.[83] SOLID CYBERSECURITY POLICY MUST BE IN PLACE FOR THIS FUTURE.

CYBERSECURITY IS A BUSINESS ISSUE, NOT JUST A TECHNOLOGY ONE. IN A SURVEY OF CLOSE TO

4,000

COMPANY DIRECTORS IN AUSTRALIA, ROUGHLY ONLY HALF REPORTED TO BE CYBER LITERATE, AND OF CO-DIRECTORS ONLY

FIFTEEN

PERCENT CLASSED AS CYBER LITERATE. THERE IS A LACK OF KNOWLEDGE ABOUT CYBERSECURITY AT THE EXECUTIVE LEVEL IN MANY BUSINESSES IN AUSTRALIA.[1]

OPPORTUNITIES

IN 2003 THE CYBERSECURITY INDUSTRY WAS TAGGED AT **$US2.5** BILLION TODAY THE GLOBAL CYBERSECURITY MARKET TOTALS MORE THAN $US106 BILLION. SOME ESTIMATES PEG THE SECTOR WILL BE WORTH $US639 BILLION BY 2023.[1]

BY 2030 IT'S ESTIMATED DATA ANALYTICS, MOBILE INTERNET, CLOUD AND IOT COULD GENERATE $US625 **BILLION** IN SALES PER YEAR IN APAC.[1]

THE UK PUBLISHED ITS CYBERSECURITY STRATEGY IN 2011 – SINCE THEN THE SECTOR ALMOST DOUBLED FROM TEN BILLION POUNDS TO **SEVENTEEN** BILLION POUNDS AND IS NOW RESPONSIBLE FOR EMPLOYING 100K PEOPLE.[51]

THERE ARE **1,404** CYBERSECURITY VENDORS IN THE WORLD TODAY. AUSTRALIA SPORTS ONLY FIFTEEN. VENDORS BY COUNTRY:
USA 827, ISRAEL 228, UK 76, INDIA 41, AUSTRALIA 15.[1]

JOB ADVERTISEMENTS FOR CYBERSECURITY ALONE HAVE GROWN **57%** IN THE LAST 12 MONTHS ACCORDING TO JOBS WEBSITE SEEK. NETWORK SECURITY CONSULTANTS WERE THE **SIXTH** MOST ADVERTISED ICT OCCUPATION ON LINKEDIN IN 2015.[50]

Glossary

A collection of some common words and phrases you will see used for discussions in and around cybersecurity.

Administrator: Person who administers a computer system or network and has access to the Administrator account.

Black Hat: Programmers who 'hack' into systems to test their capabilities, and exploit vulnerabilities for personal or financial gain. See Cybercrime.

Advanced Persistent Threat: Usually refers to long-term stealth attacks on or infiltration of a system, but can also be used to describe a group, such as a foreign government, with advanced cyberattack capabilities.

CIO/CISO: Chief Information Officer/ Chief Information Security Officer. Executive position responsible for ensuring the security of systems and

Cyberthreat: A potential threat targeting computer systems and technology, typically from the internet.

Cyberwarfare: Internet-based conflict to attack computer systems to disrupt or destroy. Usually in reference to nation states but can also refer to companies, terrorist or political groups, or activists.

DoS/DDoS: Denial of Service/ Distributed Denial of Service. A common attack involving thousands of devices accessing a site simultaneously and continually to overload its ability to serve web pages.

Hacker/Hacking: While originally in reference to a programmer

Malware: Catch-all to any type of malici typically used in refe ransomware, spywa

Phishing: Deceptive over email, to trick u handing over persor or critical informatio passwords or credit A form of social eng

Ransomware: Malw hold an individual or to ransom, typically files or an entire har demanding paymen data. Also known as

Social engineering: manipulating huma

References

1 Richard Stiennon, Chief Research Analyst, IT-Harvest,
National Fintech Cybersecurity Summit 2016

2 Internet Users by Country 2016, Internet Life Stats, July 2016
www.internetlivestats.com/internet-users-by-country

3 'Cybersecurity Market... Expected To Reach $170 Billion By 2020', Forbes, Dec 2015
www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020

4 'One in two users click on links from unknown senders', Fau.eu, August 2016
www.fau.eu/2016/08/25/news/research/one-in-two-users-click-on-links-from-unknown-senders

5 'Biggest cybersecurity threats in 2016', CNBC, Dec 2015
www.cnbc.com/2015/12/28/biggest-cybersecurity-threats-in-2016.html

6 'Hackers remotely kill a jeep on the highway', Wired, July 2015
www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

7 'Hackers can send fatal dose to hospital drug pumps', Wired, June 2015
www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps

8 'Hackers can hijack Wi-Fi Hello Barbie to spy on your children', The Guardian, November 2015
www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children

9 Simi Bajaj, 'Cyber Fraud: A Digital Crime',
www.academia.edu/8353884/cyber_fraud_a_digital_crime

10 Akamai's State of the Internet Security Report Q2 2015
media.scmagazine.com/documents/144/q2_2015_soti_security_report_-_35820.pdf

11 Contracting for the Internet of Things: Looking into the Nest,
Social Science Research Network, February 2016

in-online-scam-507818.shtml

85 Cyber War, ABC, 4 Corners, August 2015
www.abc.net.au/4corners/stories/2014/08/29/4526527.htm

86 'Robot Lawyers Could Make Time-Consuming, Expensive Court Conflict Thing Of The Past', ABC, July 2016
www.abc.net.au/news/2016-07-06/robot-lawyers-dutch-conflict-resolution-technology-on-its-way/7572488

87 'European Union's First Cybersecurity Law Gets Green Light', Bloomberg Technology, July 6
www.bloomberg.com/news/articles/2016-07-06/european-union-s-first-cybersecurity-law-gets-green-light

88 'Japanese Government Plans Cyber Attack Institute', The Stack, August 2016
thestack.com/security/2016/08/24/japanese-government-plans-cyber-attack-institute

89 'Hacker Demonstrates How Voting Machines Can Be Compromised', CBS News, August 2016
www.cbsnews.com/news/rigged-presidential-elections-hackers-demonstrate-voting-threat-old-machines

90 'FTC Warns Consumers: Don't Sync To Your Rental Car!', Slashdot, September 2016
tech.slashdot.org/story/16/09/04/0912201/ftc-warns-consumers-dont-sync-to-your-rental-car

91 'Yahoo Confirms Massive Data Breach, 500 Million Users Impacted', Slashdot, September 2016
it.slashdot.org/story/16/09/22/095255/yahoo-confirms-massive-data-breach-500-million-users-impacted-updated

92 Image, StaySmartOnline.gov.au, October 2015
www.staysmartonline.gov.au/sites/g/files/net301/f/Cost%20of%20cybercrime_INFOGRAPHIC_WEB_published_08102015.pdf

93 Adrian Turner, CEO, Data 61, National Fintech Cybersecurity Summit 2016, Sydney

ABOUT THE ACS

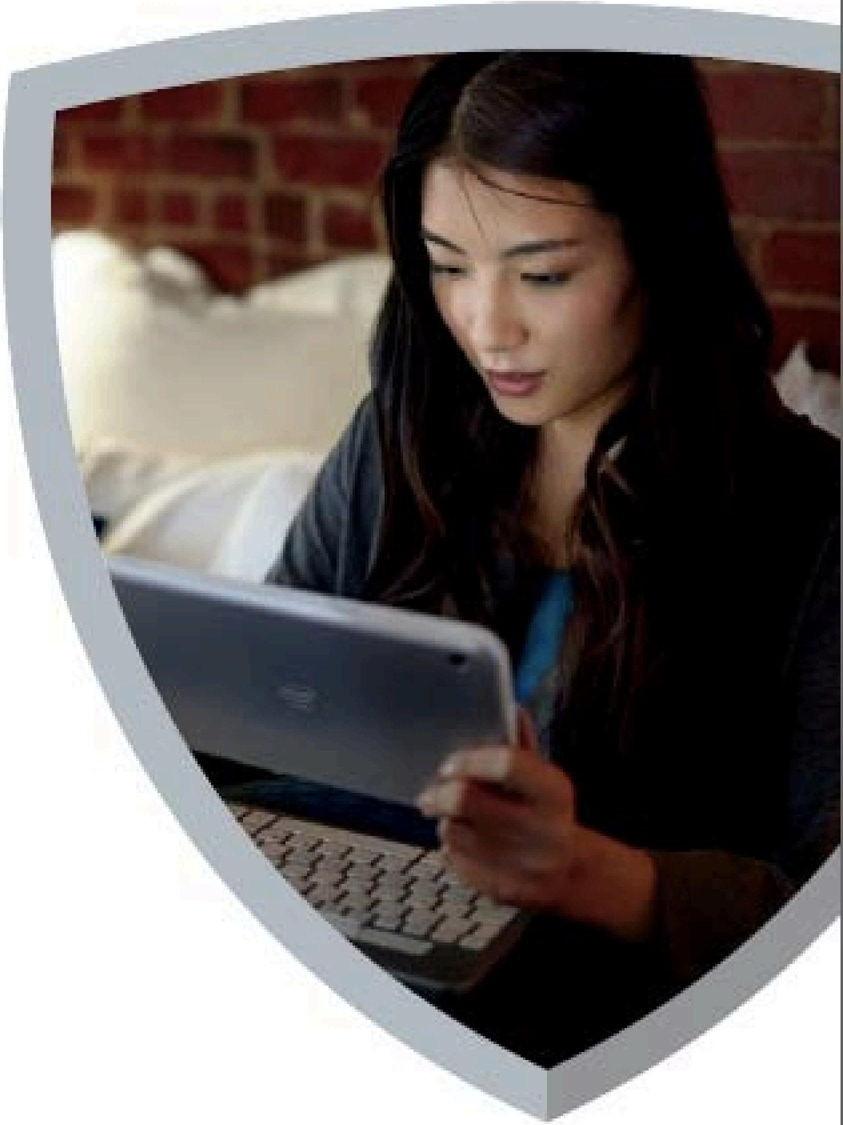
The Australian Computer Society is the professional association for Australia's Information and Communications Technology sector.

We are passionate about recognising and developing ICT skills and provide more than 60 products and services to our members. We are also the voice of Australian ICT, representing all practitioners in business, government and education.

In everything we do, our goal is to advance ICT in Australia and help our members be the best they can be.

COPYRIGHT NOTICE

Report



McAfee Labs
2016 Threats Predictions