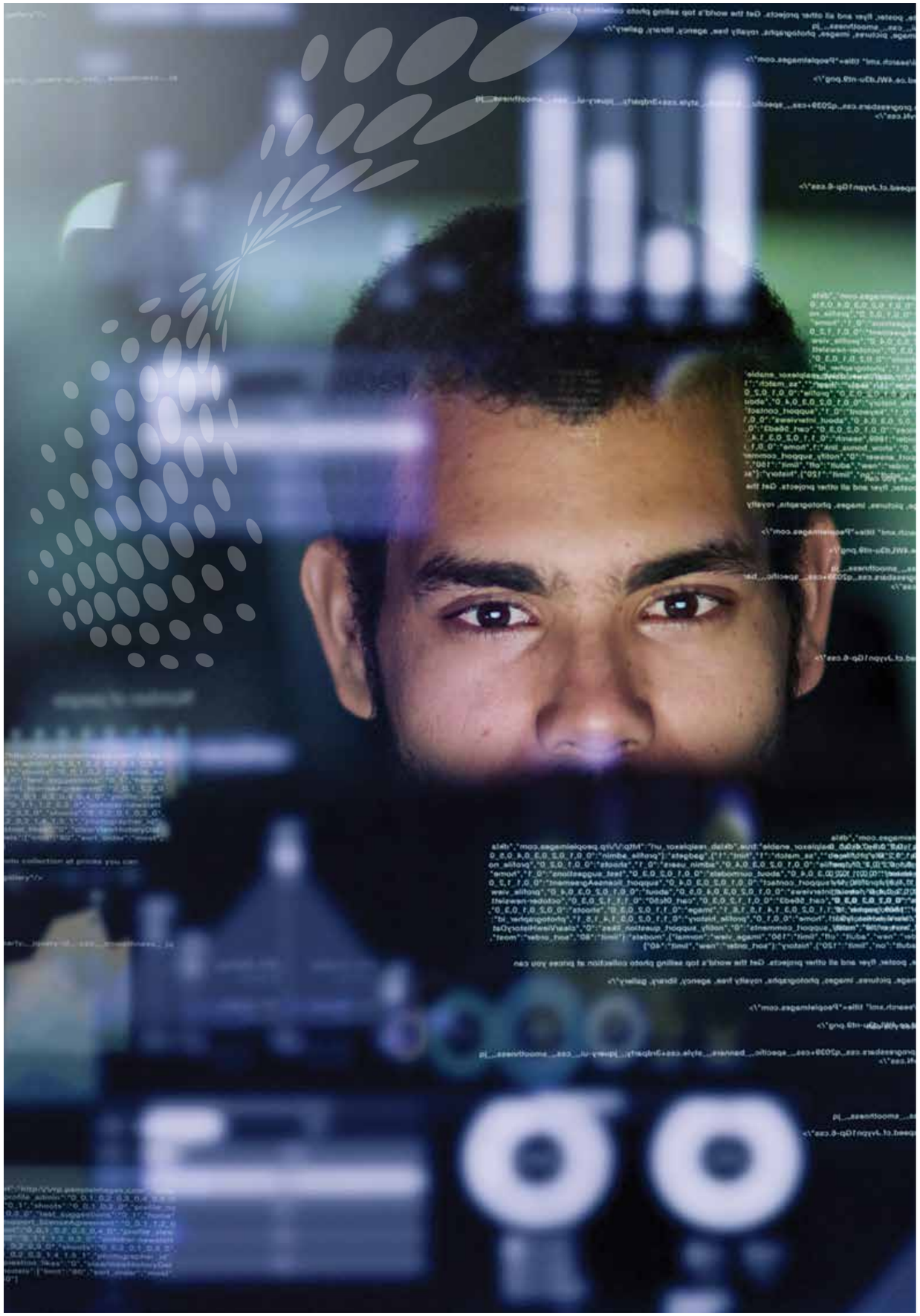
November 2016

Cybersecurity

Threats
Challenges
Opportunities



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

Clive James

Contents

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.

Foreword

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

01

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.

01

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**.

02

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!

And so it follows that in order to keep our way of life – and to continue to prosper through technology – we must ensure that it always operates and works for us as intended.

And for the most part it does, until it's hacked. In the hands of less than favourable individuals, organisations, and governments, technology and the data it depends on can be turned against us.

When you read yet another report of a multimillion-dollar bank theft, yet another million usernames and passwords leaked on the web, or yet another scam milking millions from vulnerable people – what you are reading about is the lack of cybersecurity: a failure to protect systems, processes, or data and thereby enabling exploitation. Sometimes the end result is just an embarrassment for a company or individual; at other times it can cause significant financial or operational harm. At its worst, loss of life can be a result.

Cybersecurity, then, is not optional. As our world transitions more products and services online, and we in turn depend on them, protecting this technological infrastructure has become a fundamental building block for information systems globally. It must underpin every technology, every gadget, every application, and anywhere data is stored.

To help understand the risks, this document will explore the threats Australia faces in this digital age: to our economy, our sovereignty, and ultimately, our way of life.

It will also cover the opportunities as a burgeoning industry – one that is projected to be worth $US639 billion[1] globally in the next seven years alone – and the possibility for Australia to establish itself as a leader, pioneering new technologies and exporting cybersecurity products to the rest of the world.

We are more than just the lucky country. We are early adopters. We are tenacious innovators. We are a nation with the skills and talent to lead the world in cybersecurity – and with the right mix of leadership and commitment from government, industry, and academia, we can make it happen.

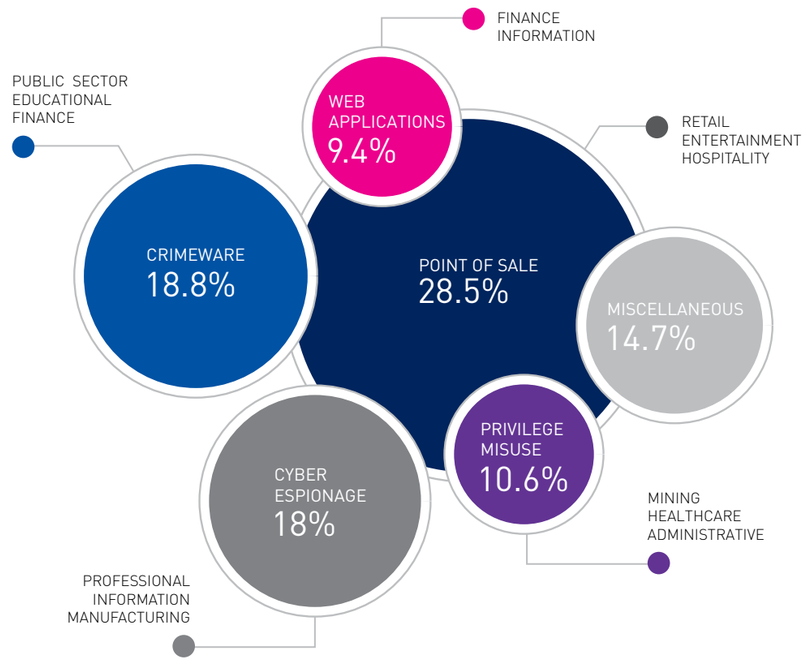
What part will you play?

46%

OF THE WORLD'S POPULATION IS CONNECTED TO THE INTERNET

THREAT VECTORS BY INDUSTRY

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



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.

Despite the threat of viruses and malware almost since the dawn of computing, awareness of the security and sanctity of data with computer systems didn't gain traction until the explosive growth of the internet, whereby the exposure of so many machines on the web provided a veritable playground for hackers to test their skills – bringing down websites, stealing data, or committing fraud. It's something we now call **cybercrime**.

Since then, and with internet penetration globally at an estimated 3.4 billion users (approximately 46% of the world's population[2]), the opportunities for cybercrime have ballooned exponentially.

Combating this is a multi-disciplinary affair that spans hardware and software through to policy and people – all of it aimed at both preventing cybercrime occurring in the first place, or minimising its impact when it does. This is the practice of **cybersecurity**.

There is no silver bullet, however; cybersecurity is a constantly evolving, constantly active process just like the threats it aims to prevent.

What happens when security fails? While what frequently makes the news are breaches of user accounts and the publication of names and passwords – the type that the Ashley Madison hack publicly exemplified – it's often financial gain, or the theft of critical business or government intelligence, that drives the cyber underworld.

One fact remains clear: it's only going to increase. As we integrate technology further into our lives, the opportunities for abuse grow. So too, then, must the defences we employ to stop them through the education and practice of cybersecurity.

The increasing prevalence and severity of malicious cyber-enabled activities... constitute an unusual and extraordinary threat to the national security, foreign policy and economy of the United States. I hereby declare a national emergency to deal with this threat.

Barack Obama,
President of the United States[3]

02

LAST
TO KNOW

MORE THAN
90%
OF BREACHES ARE DISCOVERED BY EXTERNAL PARTIES

WHAT'S THE PASSWORD?

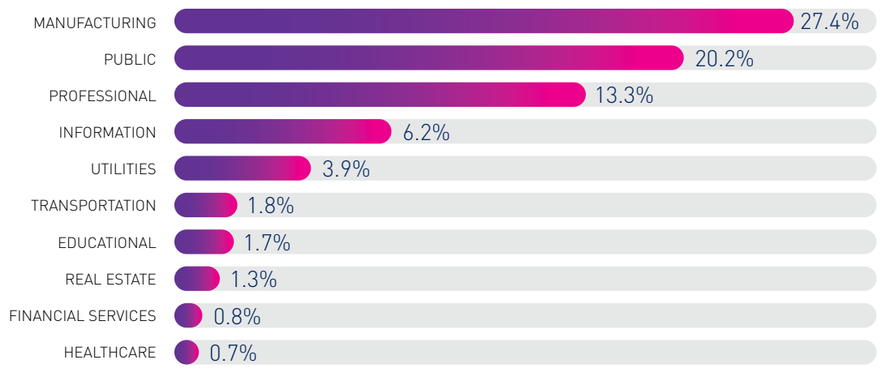
63%
OF BREACHES ARE CAUSED BY WEAK, DEFAULT, OR STOLEN PASSWORDS

EASY HACKS, EASY BREACHES

Source: Verizon 2016 Data Breach Investigations Report

TOP 10 ESPIONAGE TARGETED INDUSTRIES

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



02

AND THE WEAKEST LINK IS...

Humans are inherently complex and multi-faceted creatures with our own agendas, influences, faults, beliefs, and priorities.

Sometimes we're also simply just too trusting.

Even the most hardened system can be breached through **social engineering** – the 'hacking' of people. No amount of secure network topologies and firewalls or security software can withstand a user innocently clicking on an email link, or being convinced to give up login details over the phone by someone pretending to be from the IT department.

In fact a recent study by researchers at the Friedrich-Alexander University of Erlangen-Nuremberg, Germany, revealed that just over 50% of people click on links in emails from strangers, **even when they were aware of the risks**.[4]

And so, as a result, cybersecurity isn't just about technological defences: it's also about people. From the home user through to industry and government, everyone needs a basic understanding of cyberthreats and how to recognise them – something which comes under the umbrella of **digital literacy**.

A world without cybersecurity

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 FINACIALLY 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

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.

By way of example, and to draw from the emerging technology of driverless cars gaining popularity now, is the following example of what might happen if we continue to create products and services without cybersecurity in mind:

Thirty years from now our society runs on automated cars, buses and trains. Planes still require human authority – for now – and drones line the sky. On the one hand, this advance in technology has brought much greater efficiency: traffic jams eliminated, pollution lowered, cheaper cost of transport and more. It's a golden age.

Then a cyberattack compromises the central network. The systems that co-ordinate all transport shut down, bringing the city of Sydney – now 7 million people – to an abrupt halt.

No cars, no buses, no trains.

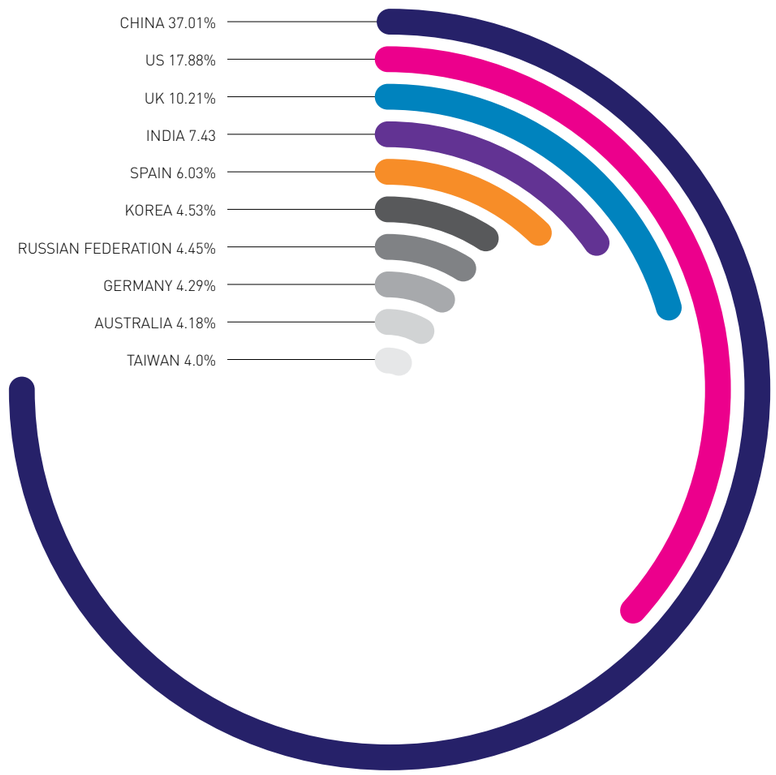
Workers can't get to and from work, and productivity stops. Life-saving medicine doesn't arrive and people die. Essential services begin to fail, and chaos ensues. The economic and social fallout is immense: a city held hostage by an external force – be it terrorist, criminal, or foreign power. Australia invaded without the invader ever stepping on our shores.

It's a stark example, but it demonstrates the Achilles heel the inter-connected society that we are heading for right now, and the reason cybersecurity must be part of all technology from the outset.

Consider this: the internet has enabled entirely new business models that have already shaped our planet. But the Googles and Facebooks and Amazons of this world are not the most profitable organisations that conduct business over the internet today – that crown belongs to cybercrime. It speaks volumes that the most lucrative business on the internet today is fraud.[9]

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

02

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]

03

500 Thousand

500,000 ATTACKS AGAINST FORTINET EVERY MINUTE

To understand just how technology becomes vulnerable to cybercrime, it helps to first understand the nature of threats and how they exploit technological systems.

You might first ask why technology is vulnerable at all, and the answer is simple: trust. From its inception, the protocols that drive Internet, by and large, were not designed for a future that involved exploitation – there was little expectation at its birth that we might need to one day mitigate against attacks such as a **distributed denial of service** (DDoS), or that a webcam you buy off the shelf might need security protocols to prevent it being hacked and used to spy on you.

There is much greater awareness today, but even so you can still buy devices that connect to the internet that have poor security measures or no security at all built-in, because up until recently this simply wasn't part of the design scope. In many cases, the idea that a device might be used for nefarious purposes isn't even considered.

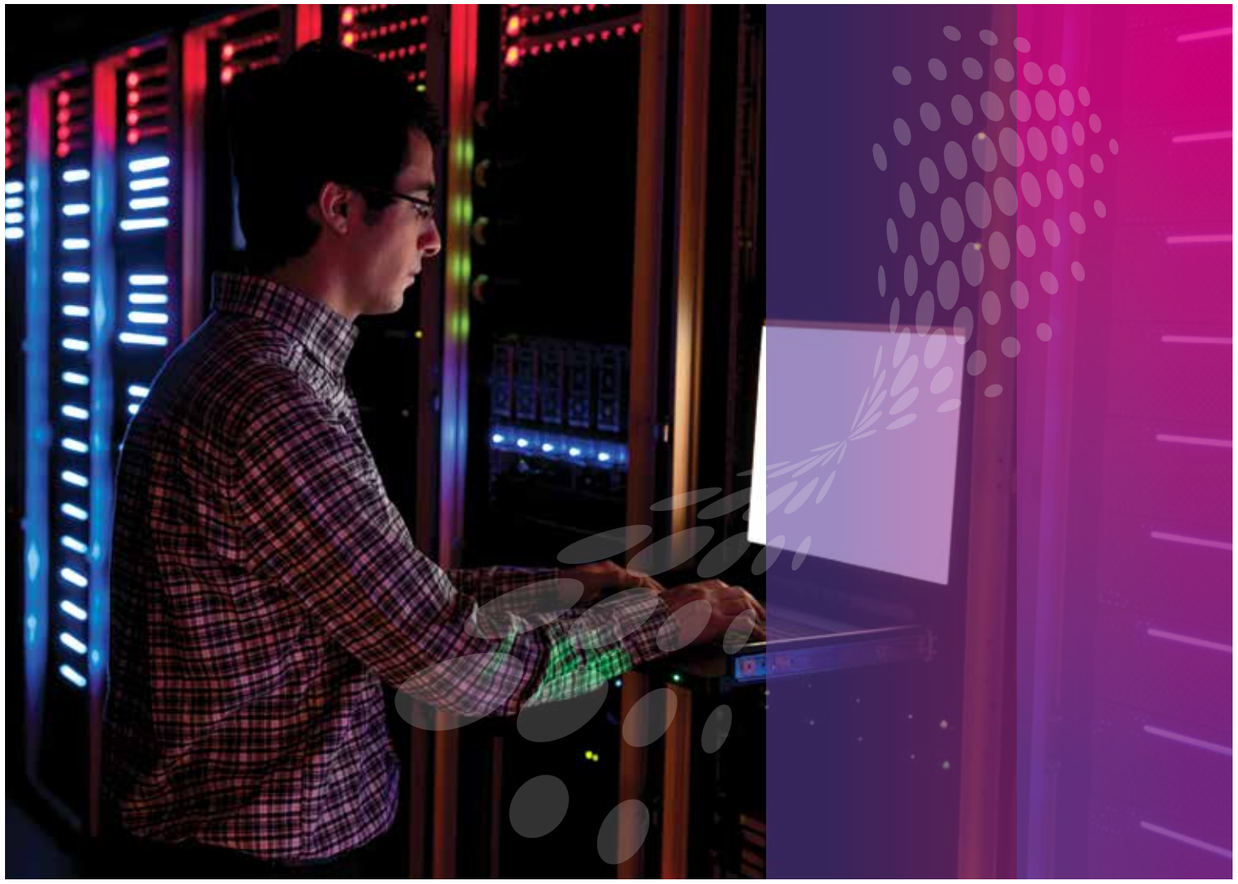
And the result is that today cybercrime almost exclusively leverages the lack of security-focused design in everything from your smartphone and web browser through to your credit card and even the electronic systems in your car.

The nature of threats

Cybercrime comes in a variety of forms ranging from denial of service attacks on websites through to theft, blackmail, extortion, manipulation, and destruction. The tools are many and varied, and can include malware, ransomware, spyware, social engineering, and even alterations to physical devices (for example, ATM skimmers).

It's no surprise then that the sheer scope of possible attacks is vast, a problem compounded by what's known as the **attack surface**: the size of the vulnerability presented by hardware and software. That is, if a hacking exploit works on Apple iPhones for example, and everyone in your organisation has one, then by definition the attack surface could range in the dozens to the thousands depending on the size of your company. Or, looking at it another way, if anyone with an iPhone is vulnerable, the attack surface worldwide totals in the hundreds of millions.

This is further compounded by the fact that hardware and software may provide multiple vectors for attacks, such that – and using the above example again – an iPhone might have multiple different vulnerabilities, each of them a possibility for exploitation. In some cases, multiple exploits can be used in tandem to hack a device, as the FBI recently demonstrated when it gained access to the San Bernardino shooter's iPhone (yes, the good guys can hack you, too...)



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.

Lucien Constantin, Network World, 2016[28]

03

And this is to say nothing of embedded systems the type that of which power our infrastructure including transport, electricity, and communications. Here, attacks are often more targeted – even down to specific to systems in a particular plant – but the repercussions are also considerably more dangerous. Shutting down an electrical grid, for example, can have life-threatening consequences.

What you also don't see – because it's hidden in the millions of fibre-optic networks and routers that form the internet – is that attacks are happening constantly all around the world, even as you read this. Your modem at home that gives you access to the internet is constantly fending off queries to see if your IP address has any open ports (the virtual addresses that allow software to communicate to and from your computers and network).

According to network security and services company Fortinet, 500,000 attacks occur against its networks every minute[5]. And that's just one service provider.

The bottom line is this: almost anything controllable by technology will have a weak spot. In the past year we've seen everything from cars ("Hackers remotely kill jeep on highway"[6]) to medical devices ("Hackers can send fatal dose to drug pumps"[7]) to toys ("Hackers hijack Hello Barbie Wi-Fi to spy on children"[8]) succumb to anyone with a little knowledge, time, and opportunity.

To appreciate the scope of the challenge that lies ahead – the new types of threats that we are starting to see emerge now – and thus the importance of cybersecurity for the government, industry, and the individual, the following section delves into our predictions of where cybercrime is heading, and the type of attacks we can expect to see.

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[18]

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 much touted internet-connected fridges. But IoT actually encompasses a broad range of products most of which you won't actually see – electronics, sensors, actuators and software soon to be built into everything from your car to your home: technology to unlock your door and turn on the lights when you arrive home; technology to allow cars to talk to other cars and traffic lights to prevent accidents; technology to let entire cities regulate air-quality, manage energy distribution, and regulate water supply all in real-time from thousands of buildings, each with thousands of sensors, all communicating through a city-wide network.

Sound like fantasy? There is already a development in the UK by River Clyde Homes and the Hypercat Consortium to build a Smart Neighbourhood in Scotland by installing hundreds of IoT devices to monitor everything from temperature and local weather through to carbon monoxide levels, potential gas leaks, lift maintenance, smoke detection and communal lighting to name a few. All of these talk to each other to provide an overall real-time knowledge base for the operating of neighbourhood services, and to minimise health and safety risks.

But this is just the beginning. IoT has the potential to encompass a lot more – heart monitoring implants, pathogen monitoring for food, transponders for animals on farms, environmental waste monitoring, field devices for police to detect threats, feedback sensors for firefighters in search and rescue and much, much more.

Perhaps the best way to imagine IoT is – and to borrow a phrase from a research paper at the Social Science Research Network – is to think of IoT as an "inextricable mixture of hardware, software, data and service"[11]. Which of course is to say that the potential is close to limitless.

According to the CEO of Cisco, Chuck Robbins, the IoT industry is expected to be worth $US19 trillion globally by 2020[12]. Closer to home, Frost & Sullivan is tipping the Australian market for IoT – just in terms of home devices, such as in security or energy management – to be worth $200M by 2020.[13]

Taken together, this means is that in the near future just about everything you use, and everywhere you go, devices will be hooked up to each other communicating, sharing data, and enabling a future that once was the realm of science-fiction. The potential boon for society is immense, but so too are the risks.

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

Considerably more devices will be connected to each other and the internet: Intel predicts there will be as many as 200 billion devices by 2020.[14]

And if you remember our primer at the start of this document, that is one very large, very vulnerable attack surface. It should go without saying that the threat potential from IoT is beyond vast, and therefore cybersecurity practices must form part of IoT development from the ground up. For example, car manufacturers need to build security protocols into the sensors in smart cars to ensure they can't be turned against the driver to cause injury or death. Something which, unfortunately, is currently not the case (see next section, **Autonomous systems**).

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[15]

Botnets armies

Somewhat related are botnets. A bot (sometimes called a 'zombie') is a remotely-controlled and compromised – unbeknownst to the owner – computing device that's connected to the internet. This could be a desktop computer or a laptop, but it can also be a webcam, a modem, or a Wi-Fi router, all of which almost everyone has in their home today. Unfortunately, again, poor security design sees devices like these come with only basic security that can be easily bypassed, allowing cybercriminals to install malware and control the device remotely.

Collect enough bots and you have a botnet, and with a botnet you can launch a distributed denial-of-service (DDoS) attack. In large enough numbers, such an attack can take down websites and knock services offline – something we saw first-hand earlier this year when the Australian Bureau of Statistics eCensus website was very publicly attacked.

This is to say nothing of what happens when IoT devices take part in a DDoS, which we know they already do. In fact, the world's largest DDoS occurred in August of this year knocking out French internet service provider OVH, suffering an attack that transmitted a record-breaking 1Tbps[17]. To put this into perspective, a 1Gbps attack is sufficient to knock most businesses anywhere in the world offline, and this attack was 1000 times stronger. It was only earlier in 2016 that the previous record came in at 579GBps. That is, we have already seen almost a doubling of capability in less than a year, and at a volume so high that very few very large players – the Googles and Akamais of this world – are able to withstand.

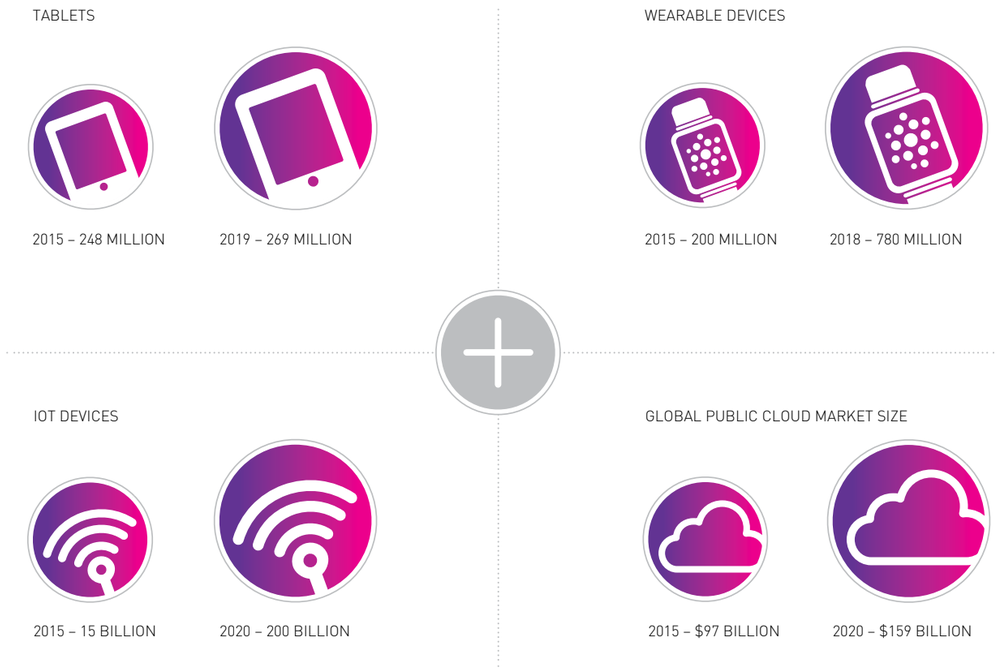
Analysis of the attack on OVH revealed it consisted of some 145,000 devices, the majority of which belonged to internet-connected CCTV cameras and DVRs (digital video recorders) typically used in business and home surveillance.

Such products make ideal bots because their limited functionality provides less scope for security software; they're often headless, meaning a user doesn't have a display or other means to interact with them to monitor activity. They almost always come with a default administrator password that nobody changes because it requires effort and a bit of technical know-how – allowing cybercriminals to walk through the front door and take it over.

This is a great example of how lack of security design enables cybercrime – who would think to hack a CCTV? But that's the line of thinking that engenders security flaws. And once a flaw is out there, it often can't be fixed: the cost of updating the devices could be ruinous for a company if they need to be recalled, as not every device supports the ability to be updated remotely.

Prevention, then, is better than cure.

Recently, cybercriminal botnet operators have moved to self-sustaining botnets that continually find new devices to infect and add to the flock, even while others may be taken offline[16]. This has led to cybercriminals to sub-lease access to their botnets on the cheap, meaning anyone with a grudge and $50 can bring down a website.



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.[19]

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[15]

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

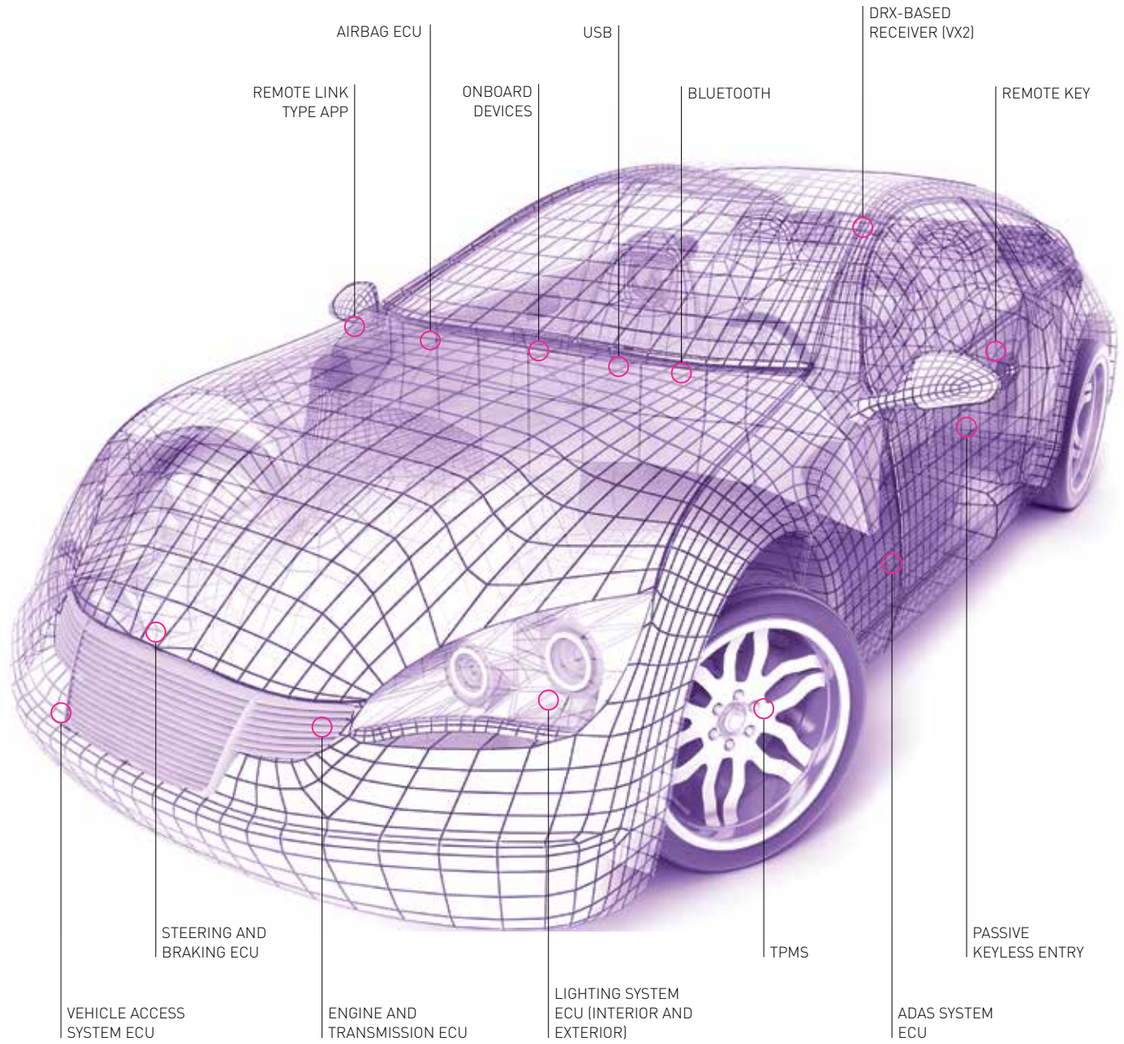
At the moment, driverless cars are stealing the limelight of autonomous systems. While so far there have been no documented cases of wilful misuse, it's already been demonstrated that autonomous cars can be remotely controlled.

In 2015, 1.4 million Jeep Cherokees were recalled after hackers demonstrated that the cars could be taken over remotely through the entertainment system.[6]

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]

McAfee's 2016 Threats Predictions Report notes that "poorly secured driverless cars and smart highways will further expose drivers and passengers in 2017 and beyond, likely resulting in lost lives...", and that "recent vehicle hacks are a great example... selectively modifying communications and commands so they can take control or affect what the vehicle does. This has a potentially terrifying result."[15]



THE ATTACK SURFACE OF A MODERN CAR
Many car systems have not been designed with security in mind, making it possible to hack into a car via smartphone or laptop.
Source: McAfee 2016 Threats Predictions

03

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[85]

ATMs and Point of Sale

Credit cards have long been the target of fraudsters, spurring the development of RFID chips and other protective technology in the banking ecosystem. However, security is an arms race and threats such as skimming is now a global phenomenon that allows data from cards to be read and transmitted wirelessly in real time from ATM machines and point of sale devices.

Indeed, point of sale systems as a whole are their own a sub-category of cybercrime infiltration, being the weakest point of the payment processing system, and so it's not uncommon to find malware specifically designed to pull data from embedded systems in POS terminals (see 'Birth and re-birth of a data breach' diagram, above.)

Now, of course, the technology has progressed further with contactless pay systems from the likes of Apple (Apple Pay) and Google (Android Pay), as well as players like Samsung (Samsung Pay, of course) that allow consumers to pay simply by waving their smartphone over a device – which presents yet another attack surface for cybercrime.

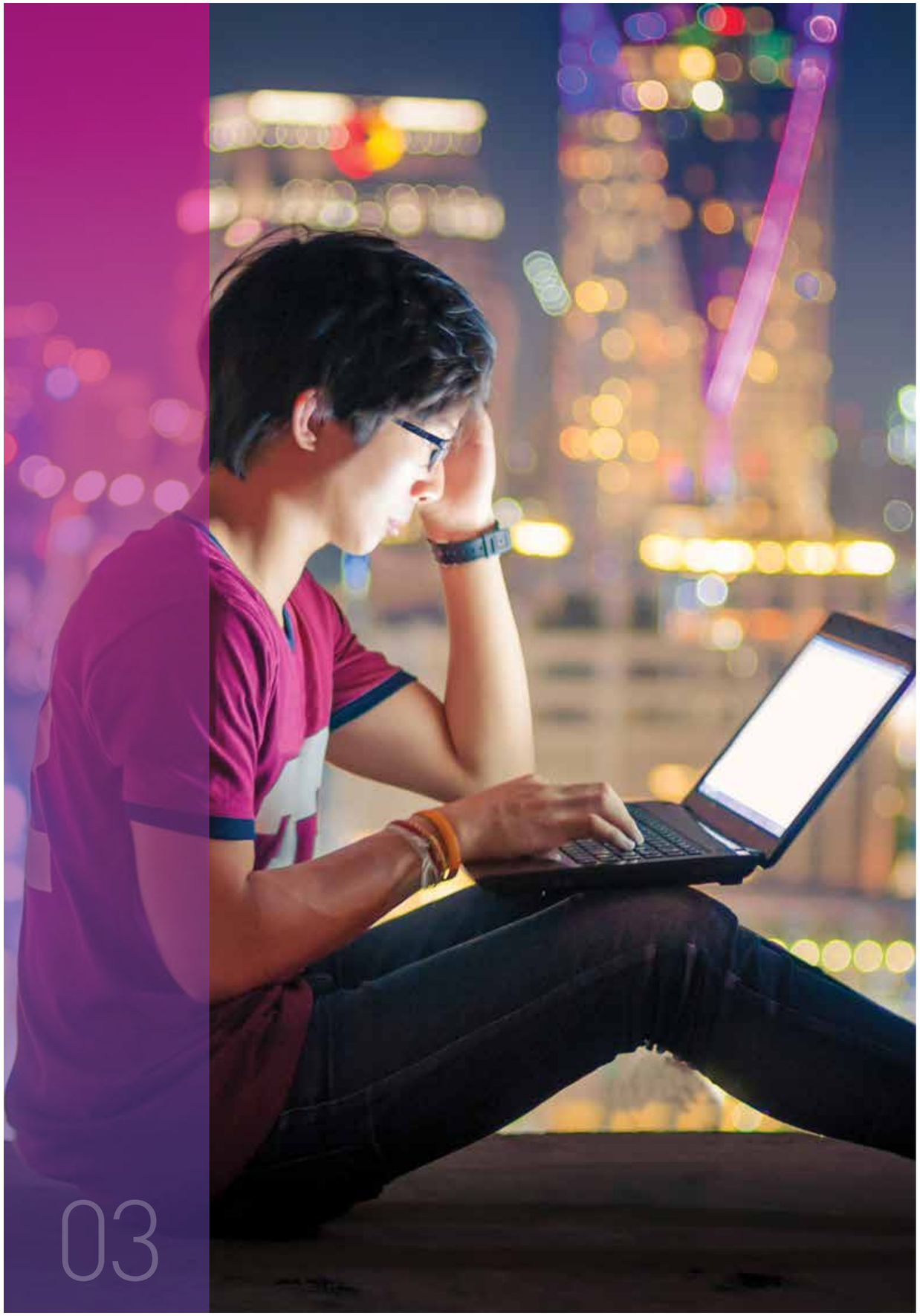
03

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.



03

Cyberwarfare

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

Dmitri Alperovitch, Cybersecurity industry executive[25]

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. The Prime Minister, Malcolm Turnbull, announced at the Australia-US Cyber Security Dialogue in September that Australia is well equipped to both defend against and carry out cyber-operations.

We now live in a world where warfare can be conducted entirely virtually – though the consequences will almost always have repercussions in the physical world.

Automated attacks

Much of what we talk about with regards to 'hacking' is a function of people at keyboards finding and abusing weak links in security. It is a skilled and time-consuming process.

However, in the ever-evolving arms race between subversive elements and cybersecurity, a move to automating such attacks would have clear benefits: whereas exfiltration may have taken days by skilled personnel, automated attacks can reduce this to hours – infiltrating, searching for a payload, gobbling it

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]

2

30,000

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

Almost half the security professionals surveyed think it is likely or extremely likely that a successful cyberattack will take down critical infrastructure and cause loss of human life within the next three years.

Critical Infrastructure Readiness Report, Aspen Institute and Intel Security, 2015[25]

up, encrypting it, and sending it out over the network before the host machine's security personnel even knows what's happened.

The defence to which, of course, is to automate security to combat automated attacks – computer software fighting computer software, all without human intervention. And while this sounds like a sci-fi movie, the reality is it's already here – in August this year the world's first automated cyber-hacking contest was held at DARPA (Defence Advanced Research Projects Agency), which saw supercomputers battle it out for a $2 million prize, the win going to a perhaps appropriately named machine called 'Mayhem'.[45]

Cyberattacks on infrastructure

As societies around the world depend ever more heavily on technology, the ability to shut down or destroy infrastructure, take control of machines and vehicles, and directly cause the loss of life has become a reality. To date, some of the more well-known examples of cyberattacks on infrastructure include:

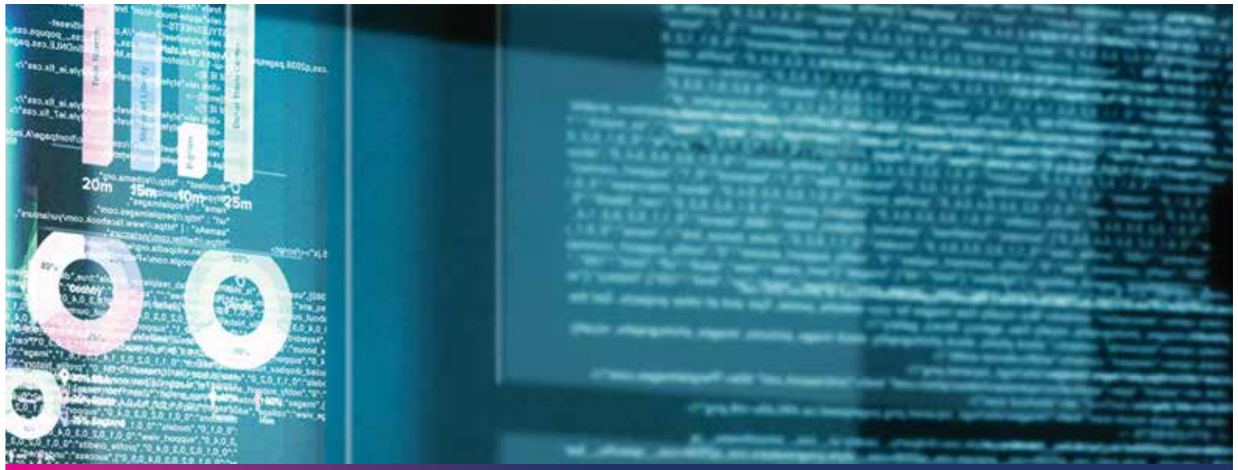
- In 2008 when Russia sent tanks into Georgia, the attack coincided with a cyberattack on Georgian government computing infrastructure. This is thought to be one of the first land and cyber coordinated attacks.[39]
- Also in 2008, Stuxnet – a computer worm purportedly jointly designed by the US and Israel – crippled Iran's nuclear-enrichment program by sabotaging centrifuges.[40]
- In 2014 a German steelworks was disabled and a furnace severely damaged when hackers infiltrated its networks and prevented the furnace from shutting down.[41]
- In 2015, with an attack strongly suspected to have originated from Russia, 230,000 people lost power when 30 sub-stations in Western Ukraine were shut down via a remote attack. Operators at the Prykarpattyaoblenergo control centre were even locked out of their systems during the attack and could only watch it unfold.[42]

In all of these, and as an indication of how the landscape of war is changing, the weapon of choice for these attacks wasn't guns or bombs – it was a keyboard.

French Coldwell, Chief Evangelist at governance, risk, and compliance apps company Metricstream, at a cybersecurity summit earlier this year noted that "this is the canary in the coalmine. Much more of this will come."[43]

We can expect governments around the world to strengthen their cyberattack and defence capabilities, spurring an arms race that will operate at a much faster pace than we saw in the Cold War. But here the results could be much more subtle – as noted in the McAfee 2016 Threats Predictions report, "they will improve their intelligence-gathering capabilities, they will grow their ability to surreptitiously manipulate markets, and they will continue to expand the definition of and rules of engagement for cyberwarfare."[15]

03



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

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]

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 data belonging to a business has been modified – with those who own the data none the wiser. As no destruction is caused such intrusions here can be harder to detect, if they're detected at all. Yet even the smallest alterations can have serious consequences and implications.

James Clapper, Director of US National Intelligence, said it succinctly when he stated, "Decision making by senior government officials (civilian and military), corporate executives, investors, or others will be impaired if they cannot trust the information they are receiving."[27]

Backdoors and espionage

Backdoors are particularly concerning because they can be both hard to discover and provide unfettered access to a system or entire network.

A compromised system can provide cybercriminals or a nation-state the ability to spy on data, or alter the data in place. And for as long as a system is compromised, abuse of privilege will be ongoing.

By way of example, in 2015 Juniper Networks announced it had discovered multiple backdoors in its firewall operating system code installed with its products – the same products used to protect corporate and government systems around the world. These backdoors had been active for at least three years.

One of the backdoors gave remote control of the firewall to an outside user, while another disturbingly allowed for the decryption of traffic running through a Juniper Networks firewall, allowing traffic to be eavesdropped. The sophistication and nature of this breach points to a nation-state as the culprit.[34]

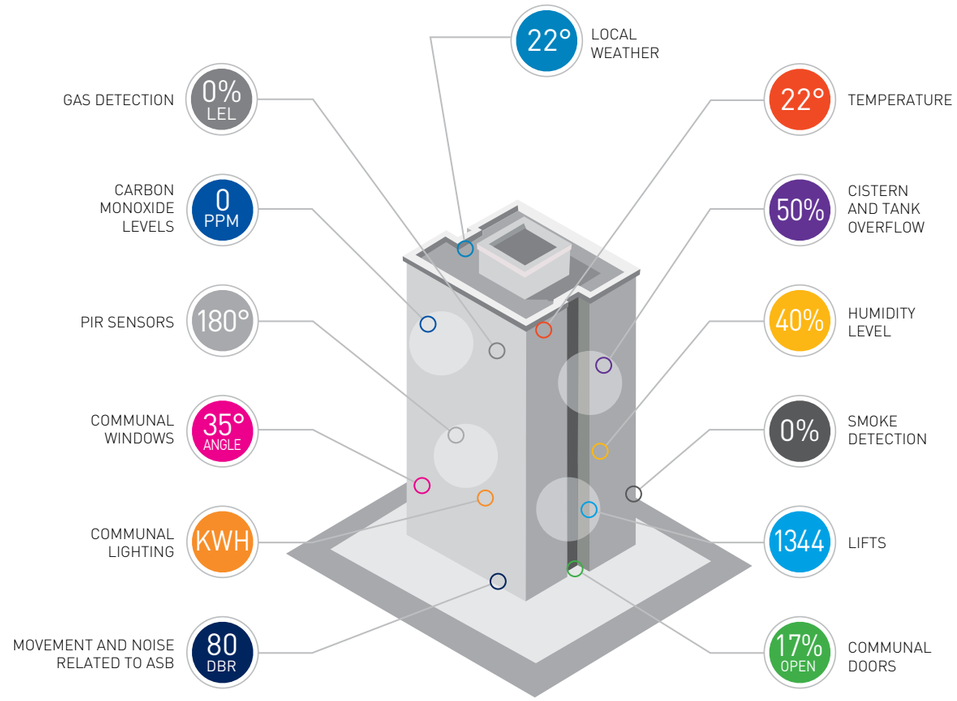
Cloud concerns

As with any successful technology, the more popular it becomes the larger a target it also becomes. Cloud is now well entrenched as a concept and a service offering, and indeed many businesses now rely on cloud services to operate.

On the one hand this can make security easier for companies outsourcing their data to lie on a cloud service where the cost of security is carried by the vendor, but on the other it centralises cloud services as highly viable targets for attack.

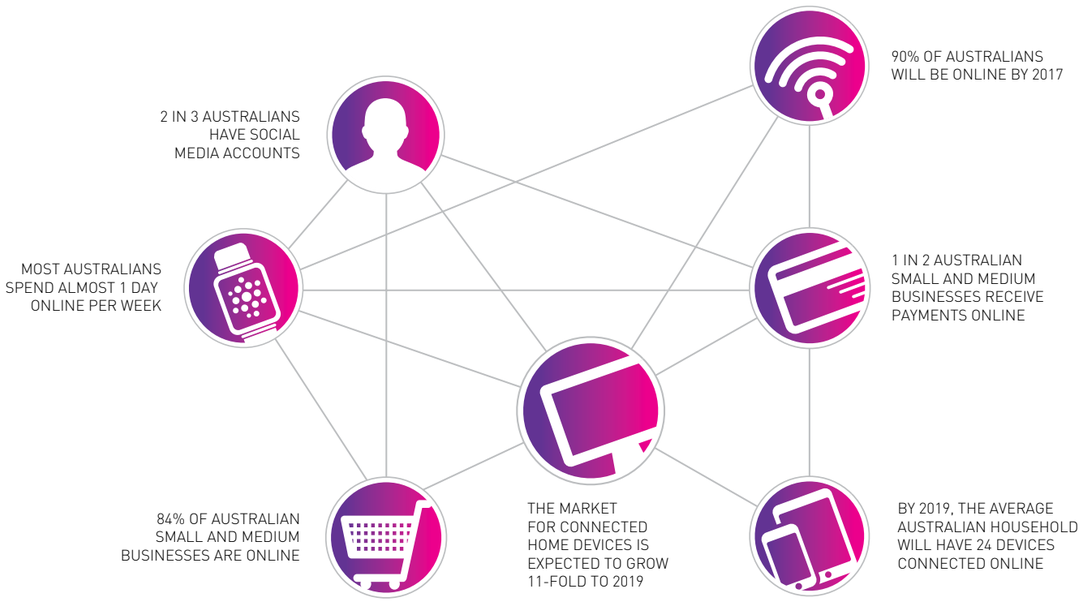
BLAST FROM THE PAST

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.



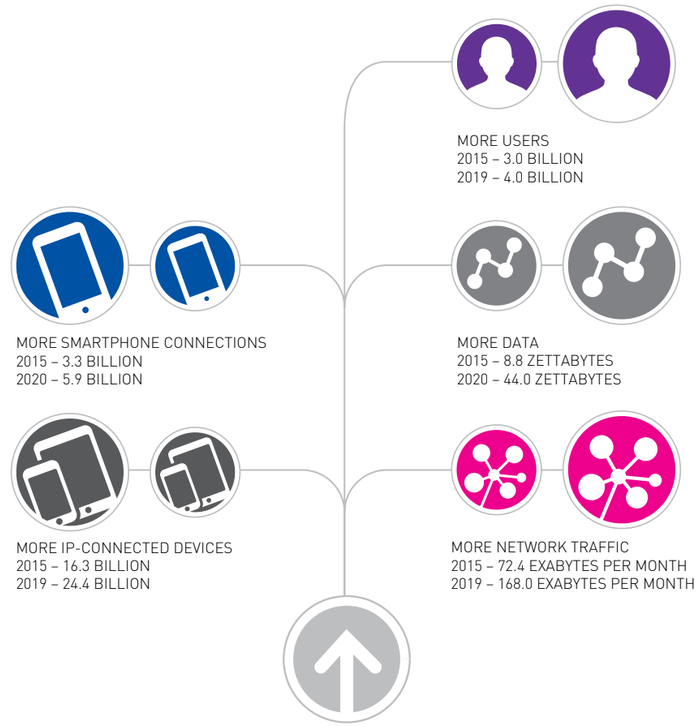
SMART CITIES – BRITAIN'S NEIGHBOURHOOD@BROOMHILL PROJECT
A small sample of the types of IoT sensors in a smart city apartment block.
Source: IoT Alliance Australia

03



AUSTRALIANS ARE BECOMING INCREASINGLY CONNECTED ONLINE

As Australia becomes ever more connected, cybersecurity becomes ever more important.
Source: Commonwealth of Australia, Department of the Prime Minister and Cabinet, Australia's Cyber Security Strategy.



THE GROWING CYBERATTACK SURFACE

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

Nation-state cyberwarfare will become an equaliser, shifting the balance of power in many international relationships just as nuclear weapons did starting in the 1950s.

McAfee Labs 2016 Threats Predictions[15]

But there's also a less obvious concern here: sovereignty.

Security of cloud data is not just about encryption, but also the sovereignty of access when data is physically located in an overseas jurisdiction. The internet may have no borders, but data itself still lies within traditional real-world boundaries and in turn may be bound by the laws of a foreign nation.[35]

Further, even if we trust in the laws of a foreign nation there's no guarantee they won't change, and data that was previously protected could be subpoenaed, accessed by government departments, or shared with third parties without consent.

A good example of how the landscape can change is the news earlier this year that in Russia, ISPs are now required to store both the metadata and content of communications, and hand over encryption keys for any encrypted data[36]. Any cloud data passing through an ISP can become readable by Russia's government and intelligence services. This had the immediate fallout of some popular VPNs closing their Russian nodes, and in at least one known case[37] servers were seized from the VPN provider under this law.

With cloud expected to grow by around 18% through 2016[38], concerns around the sanctity and sovereignty of cloud data are only going to increase.

Virtualised threats

As a result of the growth in cloud services, there has been an explosion in the use of virtual machines for business, making these prime targets for cybercrime.

Fortinet notes, "growing reliance on virtualisation and both private and hybrid clouds will make these kinds of attacks even more fruitful for cybercriminals."[5]

And, as the McAfee's 2016 Threats Predictions report notes, "how do you accurately track and attribute an attack, with all of the obfuscation possible with clouds and virtualisation?"[15] It goes on to state, "if we keep our stuff in the cloud and access it from a phone, tablet, kiosk, automobile, or watch (all of which run different operating systems and different applications), we have substantially broadened the attack surface."

Indeed, the use of apps that rely on the cloud will also allow mobile devices running compromised apps as a way for hackers to remotely attack and breach public and private corporate networks.[5]

Finally, there's one other consideration: cybercriminals can use cloud services themselves, providing powerful resources for processing power and storage, and the ability to appear and disappear at the click of a button.

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]

Industry and the individual

Malware is still very popular and growing, but the past year has marked the beginnings of a significant shift toward new threats that are more difficult to detect, including file-less attacks, exploits of remote shell and remote control protocols, encrypted infiltrations, and credential theft.

McAfee Labs 2016 Threats Predictions[15]

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.

And, it's also some of the hardest crime to combat – largely due to the sheer scope of attack surfaces which can range from desktop computers through to laptops, tablets and smartphones.

Sometimes, the vector is simply a phone: using social engineering through an employee to gain access to a network, or con an individual out of money – as in the classic **technical support scam**, of which the Government has a great summary at www.scamwatch.gov.au (also a great site to learn about other online scams).

Ransomware and Cryptoware

The ease with which amateur cybercriminals can get their hands on tools to extort money is increasing. So far in 2016 we've seen a prevalence of cryptoware targeting both enterprise and individuals, requiring the payment of a ransom to unlock encrypted files.

The most well-known of these was Cryptolocker, said to have earned its creators $US3 million before it was shut down by a consortium involving the US, the UK, and a number of security vendors and researchers.

While in an ideal world these ransoms would never be paid – and thus not encourage extortion as a business model – with victims opting to restore data from backups instead, the reality is that this isn't always practical. This is especially true for companies, where the downtime or lost productivity from denied access to the data can be higher than the price of the ransom.

Recently, however, the ante was upped with the appearance of ransomware that claims to have encrypted files and asks for payment for the decryption key, but in fact the files have simply been deleted unbeknownst to the owner.[46] Known as **Ranscam**, the one upside to this change in tactics is that if it becomes the prevalent form of ransomware, it will destroy the trust – or what little there is – between the criminal and the victim that the data will be recoverable. No honour among thieves, it seems.

Multi-vector attacks

Taking advantage of multiple concurrent attack mechanisms, a single attacker may try to penetrate an organisation on multiple levels in order to access different data, such as targeting the CFO with social engineering, with the aim to secure financial information while using spear-phishing targeted at office staff to get malware installed.

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?

One of the largest known (considering not all companies like to own up to having been scammed) scams to date resulted in the loss of €40 million from Leoni AG[84] in August of this year, facilitated by tricking a financial officer into transferring funds to the wrong account.

Importantly, success with one method can lead to exploitation of others, such as an employee clicking on a macro within an email which in turn downloads a program, which then automatically pulls down targeted malware to access network resources (this is sometimes known as 'weaponised email attachments').

The Aspen Institute's Critical Infrastructure Readiness Report notes "the analysis of this year's data led to an interesting new revelation – nearly 70% of attack victims are targeted for the purpose of advancing a different attack against another victim. For instance, an attacker may hack a website to serve malware to visitors with the intentions of infecting its true target."[25]

A common adage in cybersecurity is that while defence must consider every possible attack vector, attackers only need to find one weak point. An attack only needs to be successful once.

Identity theft

Identity theft is the crime no one thinks will happen to them until it does.

According to Javelin Strategy and Research, some $US16 billion was stolen from 12.7 million consumers in the US alone during 2014 due to identity theft.[26]

However, identity theft is more than just financial fraud, it's a central pillar for all manner of cybercrimes: once you can impersonate an individual, you can gain access to their accounts, commit multiple types of fraud in their name, steal information only they have access to, and much more.

As we share more of our lives online, we open ourselves to being exploited further. In McAfee's 2016 Threats Predictions report the authors note that "the growing value of personal data… is already more valuable than payment card information and will continue to climb."[15]

03

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]

04

$639 Billion

ESTIMATED WORTH OF THE CYBERSECURITY INDUSTRY BY 2023

It should be clear by now that we live in a world reliant on technology, and that this technology can also be vulnerable if it's not designed with security in mind. While some products and services are, many more are not, and to this end the development of cybersecurity tools, skills, and education is essential to protecting both our infrastructure and way of life.

Globally, the industry is worth $US106 billion with estimates projecting its value at $US639 billion by 2023[1]. As a nascent industry, there is a real opportunity for Australia to become a centre of cybersecurity excellence with the right leadership and investment.

Additionally, as cybersecurity must underpin the design of almost any technology product that comes to market, it goes without saying that if we don't develop our own cybersecurity products and services then we need to purchase them from overseas.

However, there is real value in producing cybersecurity products and services locally, not the least of which is control over the source code – ultimately, you must trust an overseas vendor that there are no backdoors or mechanisms in their software and firmware that would allow either exploitation by a foreign nation's government departments (such as intelligence agencies), or exploitation by cybercriminals discovering these vulnerabilities.

Particularly when it comes to national cyber defence, it would be preferable to utilise home-grown products. Not doing so is, in the words of Alex Scundurra, CEO of fintech hub Stone & Chalk, "like outsourcing our defence force to someone else."[56]

Achieving any kind of growth for a local cybersecurity industry will require support of the government, private sector, and academia. We know that as we depend more and more on technology the demand for qualified cybersecurity specialists, products, and services is only going to increase – so it's in our best interests to work towards developing and harnessing our own cybersecurity sector.

THE 100% SECURE COMPUTER

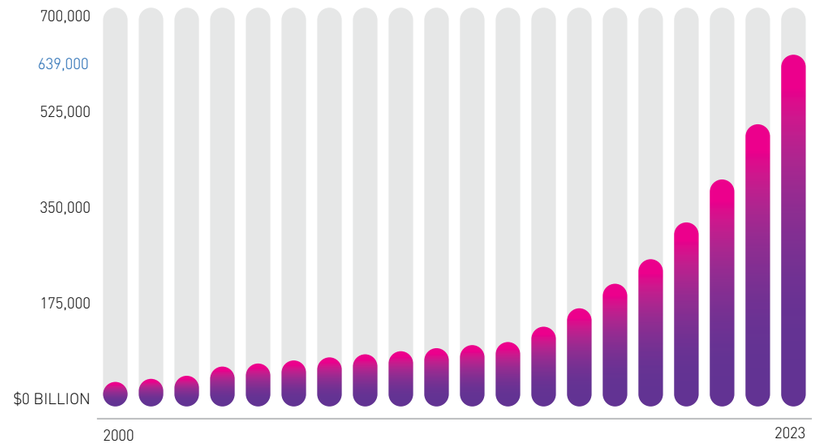
When it comes to security you can never completely eliminate risk, you can only minimise and mitigate it – there is no such thing as the 100% secure system.

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

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]

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: data will be king. From machine-learning AI to the Internet of Things, the accumulation and analysis of data from every aspect of our lives will drive entirely new insights and products.

We already have advanced local information system industries to support this, including the emerging FinTech sector (where already nine Australian FinTech businesses are listed in the world's top 100 FinTech companies[47]).

But the opportunities for products and services involving data are going to increase exponentially – already we are creating new ways to mine data and produce new services (right down to robot lawyers[86]). Combined with the Internet of Things, there is tremendous economic opportunity for Australian technology companies to innovate and produce products for the world stage.

But all of these will also require cybersecurity as a fundamental building block. Regardless of the level of investment or development in Australian technology businesses, we will need a vibrant cybersecurity sector to support innovation and guarantee the economic prosperity of technology initiatives.

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 sector, but for any of this to be possible, the gadgets and the networks they communicate on must be secure, and this means cybersecurity will need to form the basis of every new technology going forward.

The end result, as it happens, is that good cybersecurity is good for the bottom line. There is an inherent interest for companies to implement good cybersecurity strategies to ensure their profitability is protected, and this in turn will require cybersecurity products and skilled cybersecurity professionals in the workforce.

The economic opportunity for Australia then for a strong cybersecurity sector is clear.

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 of new technologies and products continues to grow.

There are lessons to be learned from Israel's high proportion of security vendors here: moving from a high proportion of agricultural exports some 50 years ago, one of Israel's primary exports is now software. Government support for a startup culture and the belief that technology is the backbone of a strong economy has seen Israel now lead the world in cybersecurity, second only to the US globally.

Currently there are some 228 cybersecurity vendors in Israel, and only 15 in Australia. Israel has one third the population of Australia.

Meanwhile in the UK, and since the British government published its cybersecurity strategy in 2011, the cybersecurity sector in the UK has almost doubled from £10 billion to £17 billion and is now responsible for employing 100 thousand people.[49]

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 the world's top universities, but as a previously resource-driven economy we currently lack a technology focus, the type of which Israel recognised as essential for a data-driven future.

Collaboration of government, industry and research organisations to incentivise new developments and monetise research to bring products and services to market will be key. This includes interacting with incubators and accelerators, sharing key learnings from innovation, and encouraging entrepreneurial thinking.

Diversity is also a critical component in order to meet demand for skilled ICT workers. This includes utilising a greater proportion of our aged workforce, and galvanising interest in ICT with women, who are currently underrepresented in the technology sector (just 28% of ICT roles are held by women[50]) and represent a large untapped resource.

04

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]

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 effort to both recognise and take action on what is clearly a vital function in today's technologically savvy world.

This is true across government, the private sector, education and academia – the rate at which technology adoption occurs in Australia far outstrips our ability to predict the implications of technology, particularly when it comes to the results of cybercrime.

The foundation of any society is trust, as well as the foundation for security itself. Security helps build trust between people and technology. If we cannot protect for example personal data, it will have negative consequences for technology adoption and the ICT industry as a whole.

As a result, leadership is required to tackle issues around cybersecurity, governance, private-sector support and education to ensure we can adequately protect the foundation of trust upon which we all depend.

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 years has revealed that cybercriminals work together exceptionally well: sharing knowledge of exploits, selling stolen data in an open market, and working together to develop new hacking techniques for infiltration.

By contrast, compare this with the other side of the coin – those of us who defend against cyberattacks: siloed security vendors with competing products, little co-operation between government and industry, and companies afraid to share that they've been hacked for fear of impacting share price.

The latter is particularly important: knowledge is power, as we know, and so keeping a breach secret only helps the attackers – if an exploit isn't made public, it can be used on the next company, and the next. In order to stop it, free sharing of information among business and enterprise, cybersecurity professionals, and security software vendors is essential. As Ron Moritz of TrueBit Cyber Partners notes, "while industry remains separate, the bad guys will always be ahead."[52]

Therefore, developing the knowledge and software to protect against cyberattacks cannot happen in a vacuum. No one company or security vendor is able to withstand the collective might of an opponent who collaborates. This is a key lesson many in the private sector will have to learn if we are to keep pace in the cyber arms race.

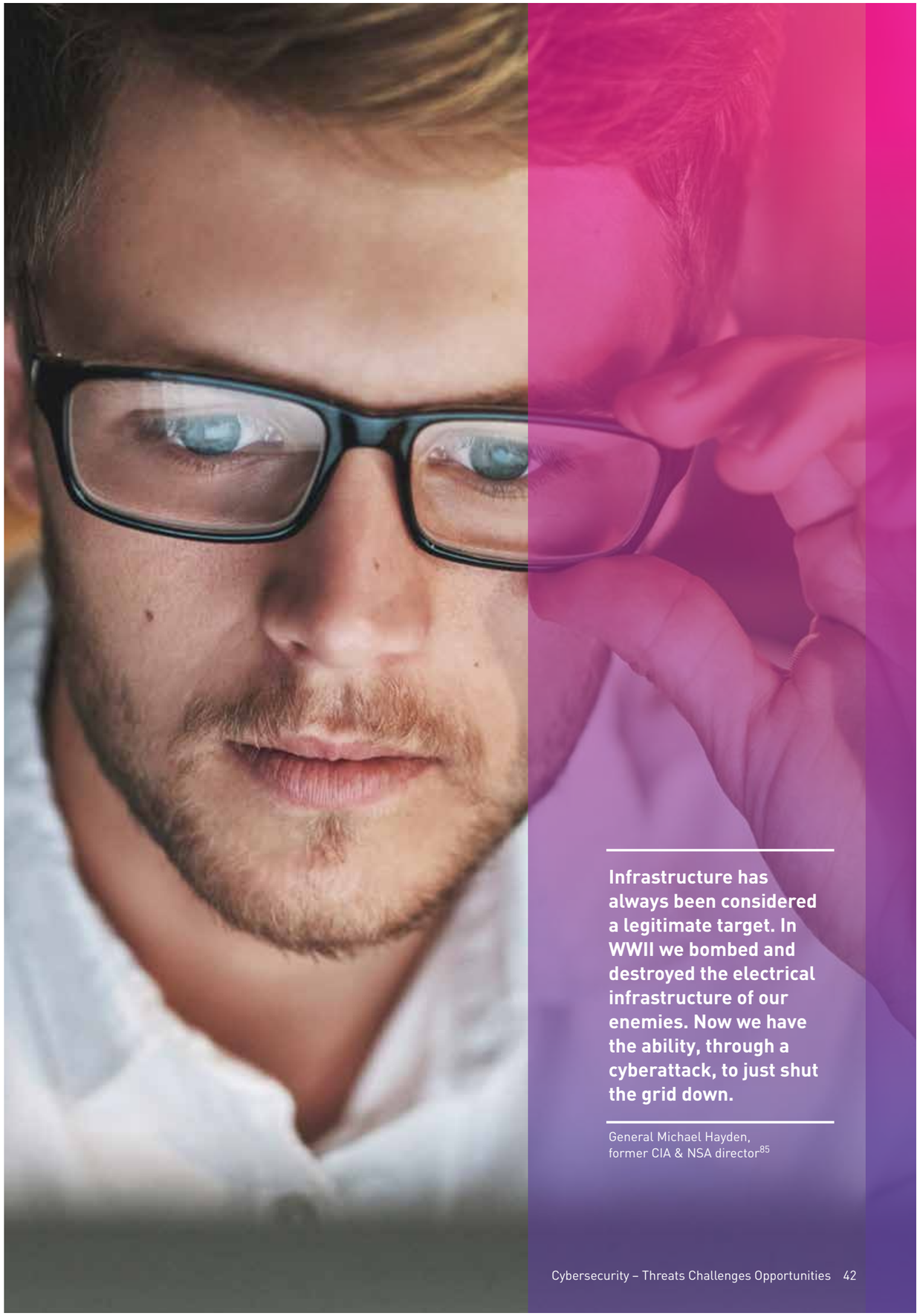
Education and awareness

According to **Australia's Digital Pulse**, a report commissioned by the ACS, the demand for skilled ICT workers will increase from 638K today to 695K by 2020, with ICT university graduates meeting only 1% of this demand.[50] Additionally, there has been a 35% drop in enrolment rates for ICT subjects at universities since 2001.[50]

As we move to a knowledge economy, we will need more scientists, mathematicians, engineers and programmers. Promotion and support of STEM subjects in schools, expanded degrees specific to cybersecurity disciplines at university, and an increased emphasis on entrepreneurial businesses skills will all help get Australians on track for roles in a cybersecurity industry as well as ICT at large.

It's interesting to note that professionals like lawyers and doctors are seen as prestigious, yet the skills and knowledge required to be a cybersecurity professional doesn't demand quite the same esteem. However, we are already at a stage where skilled cybersecurity professionals are essential to the operation of most industries in Australia. Can we generate a profession that garners a similar level of respect as other highly-skilled career paths?

Education also includes embedding cybersecurity in current workplace practice: as noted earlier, the weakest link is often people so good cybersecurity policies 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

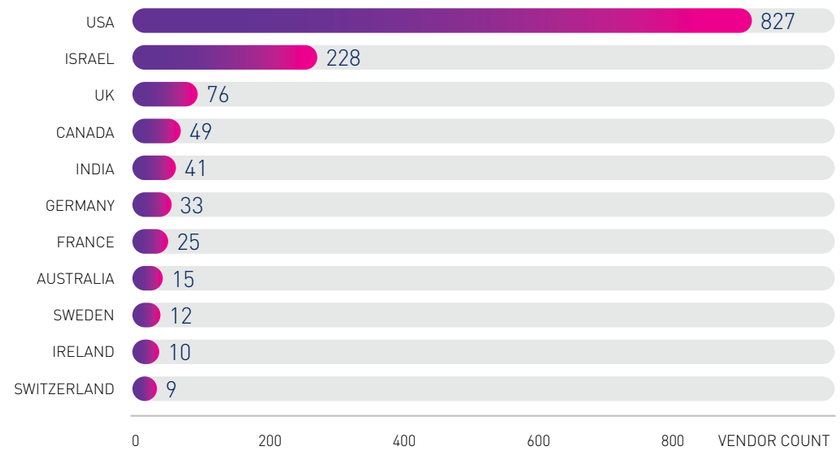
The famous adage 'you are what you eat' has an interesting parallel in the digital world – it's easy to forget that almost anything you do online involves data, and that this data tells a story about who you are and where you have been. From web browsing to smartphones, you and everyone you know is tracked,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



CYBERSECURITY VENDORS BY COUNTRY AS AT 2016
USA and Israel currently lead cybersecurity research and products.
Source: IT-Harvest

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 guys do have some hurdles the bad guys don't. For one, there may be legal or regulatory limitations, particularly where the sharing of 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 cases of identity theft, for example. The trend today for many companies is to capture as much personal information as possible, all the better to mine for advertising or other products, but as more breaches come to light this trade-off of personal data for services will come under increased scrutiny.

This has implications for mass surveillance and the storage of metadata. As Jill Slay, Director of 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 large database such as census data is a prime target for cybercriminals as it's a jackpot for identity theft. McAfee's Threats Predictions report for 2016 notes that "Government identity records such as birth/death, taxes, and national insurance IDs; and banking accounts and ATM transactions will also be targeted."[15]

Increasingly, as governments and corporations turn to big data, it will become paramount that this 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.

Pioneers like Atlassian and WiseTech Global demonstrate we have the capability to create highly successful companies and products that compete on the world stage.

Changing this perception will involve, in part, the promotion of the value of home-grown ICT and raising awareness of Australian technological solutions.

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.

05

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

Helping ensure a secure and successful environment ultimately comes down to every government, business, academic institution and individual around the world. All three are the targets of cybercrime and any government department, corporate network, or the smartphone in your pocket could be used as a vector for attack.

That's not to say we should all stop using technology because the risks are too high – it's all about process and procedure. Good government regulation, skilled and qualified IT staff in an organisation, and education about common scams and how to avoid them, can dramatically shrink the surface of exposure and minimise or prevent data breaches, cybercrime, and many of the threats covered here.

So what are other parts of the world doing, and what are we doing here in Australia?

State of the nation

Economies of scale aside, the US administration, under Obama and now Trump, allocated $US14 billion to cybersecurity spending in the 2016 budget[3], and has asked for $US19 billion for the 2017 fiscal year.[60]

In the UK the British Government has allocated £860 million over a five-year period from 2011-2016, and is increasing this to £1.9 billion to 2021.[51] The UK also conducts three exercises each month to test cyber resilience and response, and has a joint program with the US to prepare for a cyber-enabled terrorist attack on nuclear power stations. UK Chancellor George Osborne has called it "one of the greatest challenges of our lifetime".[54]

Elsewhere in Europe, the European Parliament in June imposed security and reporting obligations for industries such as "banking, energy, transport and health and on digital operators like search engines and online marketplaces."[87]

While in Japan the Japanese Government in August announced plans for a government institute, as part of Japan's Information Technology Promotion Agency (IPA), to train and educate employees to recognise and counter cyberattacks.[88]

So where are we now in Australia? In September this year Prime Minister Malcolm Turnbull addressed the Australia-US Cybersecurity Dialogue at the Center for Strategic and International Studies, in which he reiterated the importance of cybersecurity and noted "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."

On the 21st April, the Federal Government's Cyber Security Strategy[59] was launched and encompassed:

- A national cyber partnership between government, researchers and business including regular meetings to strengthen leadership and tackle emerging issues.

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 system and raising awareness of cybersecurity.

Additionally, initiatives like the Australian Centre for Cyber Security, (now in its second year), and an injection of $30 million to establish an industry-led Cyber Security Growth Centre – charged with creating business opportunities for Australia's cybersecurity sector – as part of the National Innovation and Science Agenda further establishes the government's commitment to cybersecurity development in Australia.

Meanwhile, the CyCSA national Cyber Security Challenge (www.cyberchallenge.com.au) encourages students to participate in a cybersecurity competition. It's now in its fourth year.

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 Australia-US Cyber Security Dialogue that leaders at government levels must know that "cyber is one of their essential functions" and to question what barriers can government "continue to remove, either through deregulation or positive action" to ensure the adoption of cybersecurity practices.

Regardless of your role in government, you can raise the conversation around cybersecurity and how it fits into your sector, and what the next steps are in bringing the government's cybersecurity strategy to fruition.

SHAKEN AND STIRRED

In security parlance a threat agent (not the 'James Bond' type) is an attack source combining motivation and capability. In general, threat agents can be categorised from benign to critical. To the right is a breakdown of common threat agent categories and their typical vectors:[25]

THREAT LEVEL	THREAT AGENT	THREAT VECTOR
CRITICAL	Nation state	Espionage, theft, sabotage, product alteration
	Competitor	Espionage, theft, product alteration
	Organised crime	Espionage, fraud, theft
	Terrorist	Sabotage, violence
HIGH	Activist/hacktivist	Espionage, data theft, sabotage
	Disgruntled employee	(All of the below)
	Reckless, untrained or distracted employees	Accidental breach or misuse of data
MEDIUM	Thief	Physical theft, espionage, fraud
	Irrational individual	Physical theft or sabotage
	Vendor or partner	Accidental leak, but also intentional fraud or theft
LOW	Outward sympathiser	Deliberate data leak or misuse of data

05

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 process, infrastructure investment, and regulatory and governance requirements.

Additionally, as people can themselves be an attack vector through social engineering, everyone within an organisation ultimately shares responsibility in ensuring best-practice cybersecurity processes are carried out. This requires staff education with regular updates to material as new threats arise. In fact, parallels have been drawn between cybersecurity and healthcare – everyone needs some form of cybersecurity education.

Finally, the employment of qualified cybersecurity professionals or certified training for key staff both in IT and management should form part of any cybersecurity readiness.

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.

Good cybersecurity readiness encompasses an understanding of risks and threats to assets and information relevant to the organisation and its people, monitoring and detecting cybersecurity threats regularly, protecting critical systems and information, ensuring the organisation meets all relevant standards compliance, has incident response plans in place in the event of a breach, and clear business continuity plans to minimize any loss.

Typically, many of the above responsibilities belong to the CISO (Chief Information Security Officer) or equivalent, though other stakeholders such as senior leadership, legal and communications staff, and public relations may also need to have preparations in the event of an incident.

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 identify and respond to the theft of data or the disabling of key services? How fast can affected servers or workstations be quarantined for forensic analysis? How quickly and easily can lost or corrupted data be restored? What is the incident response plan and who are the stakeholders that need to be notified immediately?

Importantly, the preservation and analysis of logs that can help identify how the breach happened, and thus how it can be closed, is part of the recovery process. It's not enough just to close the hole; an understanding of how the breach occurred can lead to preventing other, similar, breaches.

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.

The US government has increased its annual cybersecurity budget by 35%, going from $14 billion budgeted in 2016 to $19 billion in 2017. This is a sign of the times and there's no end in sight. Incremental increases in cybersecurity spending are not enough. We expect businesses of all sizes and types, and governments globally, to double down on cyber protection.

Cybersecurity Ventures[48]

'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[92]

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]

05

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 CYBER-SECURITY 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 CYBER-SECURITY 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.

05

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 data in an organisation (can include physical security).

Critical infrastructure: Physical and virtual assets that are vital to the operation of an organisation or nation, for example, the electrical grid.

Cyberattack: An offensive act against computer systems, networks, or infrastructure.

Cybercrime: Computer-facilitated crimes, though frequently can be used to refer to all forms of technology-enabled crimes.

Cyberespionage: The practice and theft of confidential information from an individual or organisation.

Cybersecurity: The discipline and practice of preventing and mitigating attacks on computer systems and networks.

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 'hacking at code', it's now become mainstream to represent individuals who maliciously breach ('hack into') computers and related systems.

ICT: Information and Communications Technology. Overarching term encompassing all forms of computing and telecommunications technology inclusive of hardware, software, and networks.

IoT: Internet of Things. An evolving definition of the wide-variety of internet-connected devices ranging from sensors to smartphones.

Internet security: A general term referring to the security of internet-related technologies, such as web browsers, but also that of the underlying operating system or networks.

Malware: Catch-all term to refer to any type of malicious software, typically used in reference to viruses, ransomware, spyware and similar.

Phishing: Deceptive attempt, usually over email, to trick users into handing over personally identifiable or critical information (such as passwords or credit card numbers). A form of social engineering.

Ransomware: Malware used to hold an individual or organisation to ransom, typically by encrypting files or an entire hard drive and demanding payment to 'unlock' the data. Also known as Cryptoware.

Social engineering: The practice of manipulating human beings to gain access to data or computer systems.

Spear-phishing: Highly-targeted form of phishing towards an individual or business, often utilising social engineering techniques to appear to be from a trusted source.

Spyware: Covert software designed to steal data or monitor people and systems for cybercriminals, organisations, or nation states.

Threat actor: an individual or entity that has the potential to impact, or has already impacted, the security of an organisation.

White Hat: Programmers who 'hack' into systems to test their capabilities, and report vulnerabilities to authorities to be fixed.

References

05

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 ssrn.com/abstract=2725913

12 'Cisco CEO Pegs Internet of Things as $19 Trillion Market', Bloomberg Technology, January 2014 www.bloomberg.com/news/articles/2014-01-08/cisco-ceo-pegs-internet-of-things-as-19-trillion-market

13 'Aussie IoT in the home spend tipped to top $200m in 2020', IoT Australia, November 2015 www.iotaustralia.org.au/2015/11/06/iot-facts-and-forecasts/aussie-iot-in-the-home-spend-tipped-to-top-200m-in-2020

14 A guide to the Internet of Things Infographic, Intel www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html

15 2016 Threats Predictions, McAfee Labs, 2016 www.mcafee.com/au/resources/reports/rp-threats-predictions-2016.pdf

16 'Lax Security Opens the Door for Mass-Scale Abuse', Imperva Incapsula, May 2015 www.incapsula.com/blog/ddos-botnet-soho-router.html

References continued

17 'Hosting company OVH suffers world's largest 1 Tbps DDoS attack', TheTechPortal.com
thetechportal.com/2016/09/28/worlds-largest-ddos-attack-ovh-iot

18 Dissecting the Top Five Network Attack Methods: A Thief's Perspective,
McAfee & Intel Security, 2015
www.mcafee.com/us/resources/reports/rp-dissecting-top-5-network-methods-thiefs-perspective.pdf

19 'The Lizard Brain of Lizard Stresser', Arbor Networks, June 2016
www.arbornetworks.com/blog/asert/lizard-brain-lizardstresser

20 'BMW, Mercedes Vulnerable to Remote-Unlocking Hack', Car and Driver, August 2015
blog.caranddriver.com/researcher-bmw-mercedes-vulnerable-to-remote-unlocking-hack

21 'BMW, Audi and Toyota cars can be unlocked and started with hacked radios',
The Telegraph UK, April 2016.
www.telegraph.co.uk/technology/2016/03/23/hackers-can-unlock-and-start-dozens-of-high-end-cars-through-the

22 'Fiat Chrysler recalls 1.4 million cars after Jeep hack', BBC News, July 2015
www.bbc.com/news/technology-33650491

23 The Connected Car Report, Business Insider, March 2015
www.businessinsider.com.au/connected-car-forecasts-top-manufacturers-leading-car-makers-2015-3

24 'Mark Zuckerberg covers his laptop camera and you should too',
Australian Financial Review, June 2016.
www.afr.com/technology/web/security/mark-zuckerberg-covers-his-laptop-camera-and-you-should-too-20160623-gppvwy

25 Critical Infrastructure Readiness Report, The Aspen Institute & Intel Security, 2015
www.mcafee.com/us/resources/reports/rp-aspen-holding-line-cyberthreats.pdf

26 Identity Theft Prevention – ID Theft Facts and Figures 2016, Kaspersky Lab, May 2016
youtu.be/Fztuohj3Fck

27 'The Next Wave of Cyberattacks Won't Steal Data -- They'll Change It',
Defense One, September 2015
www.defenseone.com/threats/2015/09/next-wave-cyberattacks-wont-steal-data-theyll-change-it/120701

28 'Massive DDoS attacks reach record levels as botnets make them cheaper to launch',
Network World, June 2016
www.networkworld.com/article/3079987/massive-ddos-attacks-reach-record-levels-as-botnets-make-them-cheaper-tolaunch.html

29 Therac-25, Wikipedia, 2016
en.wikipedia.org/wiki/Therac-25

30 'The Patriot Missile Failure', Douglas Arnold, August 2000
ima.umn.edu/~arnold/disasters/patriot.html

31 'Toyota's killer firmware: bad design and its consequences', EDN Network, October 2013
www.edn.com/design/automotive/4423428/Toyota-s-killer-firmware--Bad-design-and-its-consequences

32 'Tesla Autopilot Enthusiast Killed In First Self-Driving Car Death', Forbes, June 2016
www.forbes.com/sites/briansolomon/2016/06/30/the-first-self-driving-car-death-launches-tesla-investigation/

33 'Chinese cyberattacks hit key US weapons systems. Are they still reliable?',
Christian Science Monitor, May 2013
www.csmonitor.com/USA/Military/2013/0528/Chinese-cyberattacks-hit-key-US-weapons-systems.-Are-they-still-reliable

34 'Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors',
Wired, December 2015
www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors

35 'The 10 Commandments of Data Sovereignty', CSO Online, July 2013
www.cso.com.au/article/466539/10_commandments_data_sovereignty

36 'Russia Imposes New Data Storage Requirements for Telecoms and ISPs',
Hogan Lovells Media, July 2016
www.hlmediacomms.com/2016/07/11/russia-imposes-new-data-storage-requirements-for-telecoms-and-isps

37 'We are removing our Russian presence', PrivateInternetAccess.com
www.privateinternetaccess.com/forum/discussion/21779/we-are-removing-our-russian-presence

38 Image, Cyber Security Trends 2016, Cybernetic Global Intelligence, November 2015
cgi-content-imagesandcode.cyberneticglobal.netdna-cdn.com/wp-contentuploads/2015/11/cyber-predictions-2016-v2.png

39 Russo-Georgian War, Wikipedia, 2016
en.wikipedia.org/wiki/Russo-Georgian_War

40 'An Unprecedented Look at Stuxnet, the World's First Digital Weapon', Wired, November 2014
www.wired.com/2014/11/countdown-to-zero-day-stuxnet

41 'A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever',
Wired, January 2015
www.wired.com/2015/01/german-steel-mill-hack-destruction

42 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid', Wired, March 2016.
www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid

43 French Coldwell, Chief Evangelist, Metricstream,
National Fintech Cybersecurity Summit 2016, Sydney

44 'Kaspersky report on Energetic Bear', Security Affairs, August 2014
securityaffairs.co/wordpress/27224/cyber-crime/kaspersky-report-energetic-bear.html

45 ''Mayhem' program wins grand hacking challenge', BBC News, August 2016
www.bbc.com/news/technology-36980307

46 'When Paying Out Doesn't Pay Off', Talos Intel, July 2016
blog.talosintel.com/2016/07/ranscam.html

47 Fintech 100: Nine Australian companies make the cut
www.home.kpmg.com/au/en/home/media/press-releases/2016/10/the-fintech-100-announcing-the-worlds-leading-fintech-innovators-for-2016.html

48 Cybersecurity Market Report, Cybersecurity Ventures, 2016
cybersecurityventures.com/cybersecurity-market-report

49 Chancellor's speech to GCHQ on cyber security
www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security

References continued

50 Australia's Digital Pulse 2016, ACS & Deloitte Access Economics
www.acs.org.au/content/dam/acs/acs-documents/PJ52569-Australias-Digital-Pulse-2016_LAYOUT_Final_Web.pdf

51 The UK Cyber Security Strategy 2011-2016, Annual Report, April 2016
www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf

52 Ron Moritz, TrueBit Cyber Partners, National Fintech Cybersecurity Summit 2016, Sydney

53 Email interview, Rodney Gedda Senior Analyst, Telsyte, July 2016

54 'The Australian government must take cyber security more seriously', The Conversation, June 2016
theconversation.com/the-australian-government-must-take-cyber-security-more-seriously-60231

55 The dark side of wearables: How they're secretly jeopardizing your security and privacy, Tech Republic, April 2016
www.techrepublic.com/article/the-dark-side-of-wearables-how-theyre-secretly-jeopardizing-your-security-and-privacy/

56 Alex Scundurra, CEO Stone & Chalk, National Fintech Cybersecurity Summit 2016, Sydney

57 National Defense Education Act, Wikipedia, 2016
en.wikipedia.org/wiki/National_Defense_Education_Act

58 'The cyber-chasm: How the disconnect between the C-suite and security endangers the enterprise'
www.vmware.com/radius/wp-content/uploads/2015/08/EIU-VMware-Data-Security-Briefing.pdf

59 Australia's Cybersecurity Strategy, Commonwealth of Australia, Department of the Prime Minister and Cabinet, 2016
cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf

60 'Concerned by cyber threat, Obama seeks big increase in funding', Reuters, February 2016
www.reuters.com/article/us-obama-budget-cyber-idUSKCN0VI0R1
516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf
theconversation.com/the-australian-government-must-take-cyber-security-more-seriously-60231

61 'LinkedIn user? Your data may be up for sale', ZDNet, May 2016
www.zdnet.com/article/linkedin-user-millions-of-users-data-is-up-for-sale

62 'Apple devices held for ransom', CSO Online, July 2016
www.csoonline.com/article/3093016/security/apple-devices-held-for-ransom-rumors-claim-40m-icloud-accounts-hacked.html

63 'EasyDoc malware adds Tor backdoor to Macs for botnet control', The Register, July 2016
www.theregister.co.uk/2016/07/05/easydoc_malware_adds_tor_backdoor_to_mac_systems_for_botnet_control/

64 'Researchers Discover Tor Nodes Designed to Spy on Hidden Services', Schneier on Security, July 2016
www.schneier.com/blog/archives/2016/07/researchers_dis.html

65 'LizardStresser botnets using webcams, IoT gadgets to launch DDoS attacks', SC Magazine, July 2016
www.scmagazineuk.com/lizardstresser-botnets-using-webcams-iot-gadgets-to-launch-ddos-attacks/article/506962

66 'Researchers Found a Hacking Tool that Targets Energy Grids on the Dark Web', Motherboard, July 2016
motherboard.vice.com/read/researchers-found-a-hacking-tool-that-targets-energy-grids-on-dark-web-forum

67 'DDoS Attack Takes Down US Congress Website for Three Days', Softpedia News, July 2016
news.softpedia.com/news/ddos-attack-takes-down-us-congress-website-for-three-days-506451.shtml

68 'Citing Attack, GoToMyPC Resets All Passwords', Krebs On Security, June 2016
krebsonsecurity.com/2016/06/citing-attack-gotomypc-resets-all-passwords

69 'Hackers Find Security Gaps in Pentagon Websites', ABC News, June 2016
abcnews.go.com/Technology/wireStory/hackers-find-security-gaps-pentagon-websites-39945560

70 'Political Party's Videoconference System Hacked, Allowed Spying On Demand', Slashdot, June 2016
news.slashdot.org/story/16/06/18/1831235/political-partys-videoconference-system-hacked-allowed-spying-on-demand

71 'Hacker steals 45 million accounts from hundreds of car, tech, sports forums', ZDNet, June 2016
www.zdnet.com/article/hacker-steals-45-million-accounts-from-hundreds-of-verticalscope-car-tech-sports-forums/

72 'Online Backup Firm Carbonite Tells Users To Change Their Passwords Now', Slashdot, June 2016
it.slashdot.org/story/16/06/21/2032209/online-backup-firm-carbonite-tells-users-to-change-their-passwords-now

73 '10 million Android devices reportedly infected with Chinese malware', CNet, July 2016
www.cnet.com/news/malware-from-china-infects-over-10-million-android-users-report-says

74 'FLocker Mobile Ransomware Crosses to Smart TV', Trend Micro, June 2016
yro.slashdot.org/story/16/06/13/1845221/android-ransomware-hits-smart-tvs

75 'Thieves Go High-Tech to Steal Cars', The Wall Street Journal, July 2016
www.wsj.com/articles/thieves-go-high-tech-to-steal-cars-1467744606

76 'Hackers Can Use Smart Watch Movements To Reveal A Wearer's ATM PIN', Slashdot, July 2016
news.slashdot.org/story/16/07/06/2132206/hackers-can-use-smart-watch-movements-to-reveal-a-wearers-atm-pin

77 'Crooks are winning the 'cyber arms race' admit cops', ZDNet, July 2016
www.zdnet.com/article/crooks-are-winning-the-cyber-arms-race-admit-cops

78 'Identity fraud up by 57% as thieves 'hunt' on social media', BBC News, July 2016
www.bbc.com/news/uk-36701297

79 'A hack will kill someone within 10 years and it may have already happened', Yahoo News, June 2016
uk.news.yahoo.com/hack-kill-someone-within-10-091800465.html

References continued

80 'Why you should delete the online accounts you don't use anymore - right now', Sydney Morning Herald, June 2016.
www.smh.com.au/technology/technology-news/why-you-should-delete-the-online-accounts-you-dont-use-anymore--right-now-20160602-gp9n18.html

81 'China Hacked US Banking Regulator From 2010 Until 2013', Slashdot, July 2016
yro.slashdot.org/story/16/07/13/1923215/china-hacked-us-banking-regulator-from-2010-until-2013---and-us-officials-covered-itup-report

82 2015 Threat Report, Australian Cyber Security Centre, 2015
www.acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf

83 'Internet Of Things On Pace To Replace Mobile Phones As Most Connected Device In 2018', Forbes, July 2016
www.forbes.com/sites/louiscolumbus/2016/07/09/internet-of-things-on-pace-to-replace-mobile- phones-as-most-connecteddevice-in-2018/#468e81846aef

84 'One of Europe's Biggest Companies Loses €40 Million in Online Scam', Softpedia
news.softpedia.com/news/one-of-europe-s-biggest-companies-loses-40-million-in-online-scam-507818.shtml

85 Cyber War, ABC, 4 Corners, August 2015
www.abc.net.au/4corners/stories/2016/08/29/4526527.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.

ACS
Level 11
50 Carrington Street
Sydney NSW 2000

P: 02 9299 3666
F: 02 9299 3997
E: info@acs.org.au
W: www.acs.org.au