DIGITAL PRODUCTIVITY AND SERVICES
www.csiro.au

# Enabling Australia's Digital Future:

## cyber security trends and implications

## ACKNOWLEDGEMENTS

CSIRO would like to acknowledge Defence Science and Technology Organisation (DSTO) for the original concept and broad approach of describing the future cyber landscape in terms of cyber dependency, threat and vulnerability within a context of "increasing dependence on an increasingly vulnerable cyber domain". We also acknowledge DSTO for contributing their cyber security expertise and methodology, as well as for their input into developing the technology-use framework used to analyse sectoral technology dependence.

CSIRO engaged with both Commonwealth and State Departments and Industry stakeholders particularly relevant to the Government and Commercial Services sector, Health Services and Energy Sector whilst preparing this report and we would like to thank each of them for their valuable input. Some of those Departments and Organisations included:

- NSW Department of Finance and Services
- Australia Post
- National E-Health Transition Authority (NEHTA)
- Jemena

Lastly, CSIRO would also like to acknowledge the support of the Digital Productivity and Services Flagship members Ian Oppermann, Jay Guo, Sarah Dods, Geof Heydon and Helen Sargent, as well as assistance and insights provided by CSIRO's Computational Informatics staff John Colton, John Zic, Surya Nepal, Dimitrios Georgakopoulos, David Hansen, and Mark Paterson (Energy Flagship).



## AUTHORS

Sandra Arico (CSIRO Futures)
Vivek Srinivasan (CSIRO Futures)

# Contents


**Executive Summary** 3

**Introduction** 4
Objectives and scope 4
Approach 4
The Australian context 5

**A changing landscape** 6
Healthcare 7
Energy (Electricity) 7
Government 8

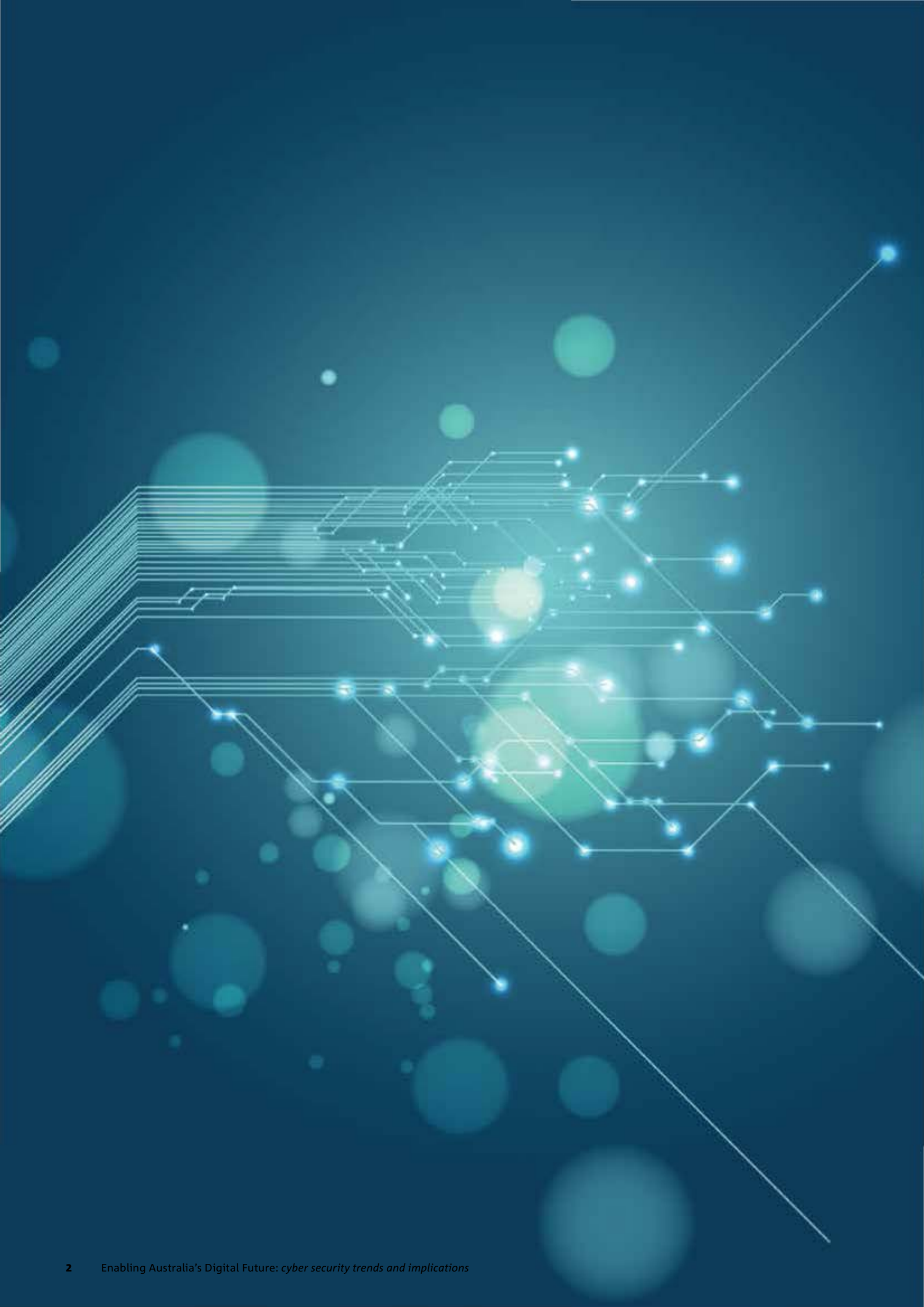
**Increased technology dependence: our digital future** 9
Customer technology-use trends 12
Provider technology-use trends 15
Customer-Provider technology-use trends 19
Implications for ICT support infrastructure 21
A complex digital future 22

**Cyber security threats: a familiar yet evolving landscape** 23
Understanding cyber threats 24
Threat actors 24
Evolving threat landscape 26
Implications going forward 27

**An increasingly vulnerable environment** 28
A changing paradigm 29
Implications of a breach 29
Scenario analysis 30

**Enabling Australia's digital future: key considerations** 35
People 36
Process 37
Technology 38
Conclusion 38

**References** 39



# Executive Summary

Australia's digital future is set to transform the nation. Our transition towards a more digital economy will drive economic progress, improve social wellbeing, and open up new opportunities for innovation and increased competitiveness on the global stage.

Continued technological advancement and rapid adoption are central to our progress, as new developments spur more innovative business models, products and services, which are crucial in responding to key national and sectoral challenges - such as rising healthcare costs, increasing household electricity prices and Government pressures to do more with less. As technology and digital solutions continue to play a key role in driving the economy and society forward, they become increasingly embedded into business operations, across key service offerings and into our personal lives.

Australia's future is digital, hyper-connected and critically dependent on technology, making strong cyber security capability crucial to navigating the associated risks and opportunities ahead. Our increased dependence on technology, combined with the evolving complexity and sophistication of cyber security threats, together increase our level of vulnerability – at a national, organisational and individual level.

Advancements in technology may be contributing to these evolving security challenges, but they are also a key part of the solution. Developments in data analytics and machine learning are allowing us to better understand network anomalies and harness big data. Progress in cryptography techniques are helping to better secure information. And sophisticated risk management modelling tools are allowing leaders to make more informed cyber decisions.

Whilst progress has been made towards improving and advancing cyber security solutions, we are at risk of becoming complacent. Amidst an environment of continuous, rapid change, with increasing levels of complexity and uncertainty, we cannot afford to rely solely on past and present solutions. Ensuring Australia's digital success into the future will require bold cyber security leadership and further investment now. It will require ongoing science and technology research that can identify emerging cyber security challenges and develop practical solutions. And it will require a cultural shift, extending cyber security responsibility out to every organisation, every government, and every individual.

Taking this direction requires a change in perspective, recognising that cyber security is not solely a technology challenge. It is also a cultural challenge, and one that extends beyond traditional information security practices. Alongside investment in new cyber security tools and technologies that can keep pace with evolving threat challenges, our nation's future strategies require a commitment to improving cyber security skills, awareness and education, as well as an imperative to evolve cyber security perceptions to understand the central role this capability has in enabling our digital future.

Successfully navigating the road ahead will require a whole-of-nation effort, harnessing the full range of resources available across our economy. Alongside existing national and defence-related strategies, the research community in partnership with industry and Government have a vital role to play, through applying innovation and cutting-edge technology to the people, process and technology solutions needed going forward. Through the integration of knowledge, ideas and resources, we can ensure strong cyber security capability is at the core of a digitally-enabled Australia.

**Dr Ian Oppermann**

*Director, Digital Productivity and Services Flagship, CSIRO*

# Introduction

Australia's transition to a digital economy is opening up new and exciting opportunities for innovation and global competitiveness. It is driving change across key sectors such as healthcare, energy and government and facilitating greater levels of social and economic prosperity. However, these new opportunities are also driving a greater dependence on technology – which is constantly evolving, increasing in complexity and continuously exposed to a sophisticated landscape of cyber threats. This challenge is compounded when you consider the blurring lines between people, organisations, processes, services and technologies that require seamless interaction and trust across the cyber ecosystem.

As a result, our national progress is directly tied to our ability to minimise risk exposure without limiting progress – making cyber security a capability of crucial importance.

## Objectives and scope

The objectives of this report are to:

- increase general awareness and understanding of digital trends and implications for cyber security in Australia;
- provide a broad overview of the current and future cyber security needs and challenges on a national level;
- present key considerations and strategic questions to serve as input for forward planning and investment considerations into the future.

A time frame of approximately ten years (to 2025) has been considered in analysing trends and presenting future scenarios.

Key considerations and strategic questions for cyber security have been posed in the broad areas of people, process and technology. Specific recommendations have not been included in this report, as they will be the subject of further collaborative effort in partnership with industry, government and the research community. The questions posed are intended as input into these further discussions and strategic planning activities.

## Approach

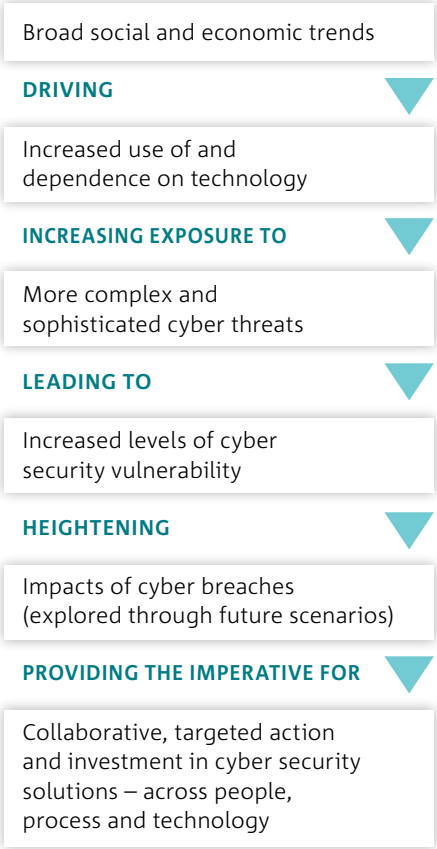
Like any complex system, cyber space is made up of many interrelated parts, which can be examined to help us better understand the overall system – and in this case, to help us gain a clearer understanding of our cyber security needs and challenges going forward. Figure 1.0 highlights this approach, reflected in the report structure as follows:

- **A changing landscape.** Focusing on three key representative sectors – healthcare, energy and government – this section provides an overview of broad economic and social trends, which are driving change and leading to increased digitisation and technology use nationally;
- **Increased technology dependence: our digital future.** Looking at emerging technology trends, this section analyses how technology usage and dependence is changing across each of the sectors. A technology-use framework is adopted, which considers various usage trends across sectoral providers (organisations) and customers (consumers), and broader technology trends related to underlying ICT support infrastructure;
- **Cyber security threats: a familiar yet evolving landscape.** Considering the cyber security threats landscape, this section explores various types of threats, different threat actors and their motivations, as well as how the landscape overall is evolving in complexity and sophistication;
- **An increasingly vulnerable environment.** Combining increased technology dependence and connectivity, alongside a more sophisticated and complex threat landscape, this section examines the implications on our level of cyber security vulnerability.* Considered from a broad, national perspective, potential exploitation of vulnerabilities is explored using three future scenarios across each of the key sectors;

*This methodology of technology dependency overlaid with threats to understand vulnerabilities has been adapted from collaborations with DSTO, as well as from other cyber security methodologies.[1],[2],[3] Traditionally, vulnerability assessments are conducted at a very technical level within organisations. For this paper we have adopted the methodology to look broadly at vulnerabilities across national sectors.

- **Enabling Australia's digital future: key considerations.** Bringing together the dependency, threat and vulnerability analyses, this section looks at the broad implications for Australia's current and future cyber security, outlining key strategic questions for consideration in enabling Australia's digital future.

**FIGURE 1.0 – APPROACH SUMMARY**




## The Australian context

A common question raised in response to cyber security is whether threats and breaches are happening here in Australia. Much of the cyber security data and cases reported point to other countries around the world, which can lead to a misconception that this is not an issue to be taken seriously on our own soil. It is not possible to present a complete picture of cyber security threats and breaches due to many cases going unreported or being of a classified nature and therefore unable to be publicly shared. However, publicly available information provides enough data to illustrate the reality of the challenge we are facing here in Australia:

- Whilst many instances of cybercrime go unreported, non-government estimates put the cost of cybercrime in Australia as high as $2 billion annually.[4] Defence estimates that in 2012, 5.4 million Australians were victims of cyber crime.[5]
- According to antivirus vendor Trend Micro, Australian computers experienced 17,692,567 malware infections in 2008. Australia reported the fifth highest level of infections worldwide.[6]
- CERT Australia, the national computer emergency response team and the single point of contact for cyber security issues affecting major Australian businesses, reported close to 7,300 incidents in 2012. The following year, incidents increased, with approximately 8,500 reported by mid-August.[7]
- The Australian Bureau of Statistics Personal Fraud Survey indicated that over the 12 month period from 2010-11[8]:
  - An estimated 1.2 million Australians aged 15 years and over were victim to at least one incident of personal fraud
  - Australians lost $1.4 billion as a result of personal fraud
  - An estimated 44,700 Australians were victims of identity theft
  - Approximately 6.4 million Australians were exposed to a scam

### ASIO building plans stolen

It has been reported the Australian Security Intelligence Organisation (ASIO) building security and communication systems blueprints were stolen in a major cyber attack in 2013.[9]

### Assuming deceased identities

An unlawful foreign national falsely assumed the identity of four deceased individuals, with almost $76,000 of false benefit claims made.[10]

This is just a snapshot of data highlighting the reality that cyber security challenges are not confined to a just handful of nations – every country is affected and every country has a role to play in enabling better national and global cyber security.

# A changing landscape

Understanding Australia's cyber security needs and challenges is a complex task, considering technology use and digital connectivity cut across all sectors, organisations and individuals, in multiple ways and to varying degrees.

In considering this complex system, we have focused on a subset of sectors to help us understand the broader national picture and the common trends and patterns evolving across all dimensions. The three sectors are healthcare (focussing on health services), energy (focussing on electricity) and government (focussing on government services), all of which are considered critical to Australia's sustained economic prosperity and social wellbeing, and whose services impact the wider population.

The following section presents an overview of the broad economic and social trends across these sectors, which are driving change and leading to increased digitisation and use of technology. These trends serve as a backdrop to the detailed technology dependency analysis that follows.

## Healthcare

### SECTOR SUMMARY

The healthcare sector is in the midst of a turbulent transformation. As the population ages and lifestyle-related illness continues to rise, increasing pressure will be placed on the healthcare system, with costs expected to grow to unsustainable proportions. This creates an increasingly challenging environment in which healthcare providers will need to operate, with several implications for the health services industry. Demand for health services will continue to grow, as will expenditure, driving changes in the nature and delivery of care, as well as creating new models for care outside of existing traditional institutions.

### Key trends:

- **Australia's population is ageing.** Between 2012 and 2060 the number of people aged over 75 years will grow by approximately four million people, an increase roughly equivalent to the current population of Sydney.[11] This is in part due to advancements in science, technology and healthcare, which are enabling people to live longer. In 1901, the average life expectancy in Australia was just 47 years;[12] by 2025, it will increase to over 80 years.[13]
- **Lifestyle-related illness and chronic disease are on the rise.** Non-communicable diseases such as cardiovascular disease, cancer, respiratory disease and diabetes, will account for almost 69% of total deaths in 2030 (up from 59% in 2002).[14] The World Health Organisation is calling this an 'invisible epidemic'.[15] The Australian Institute of Health and Welfare note that from 2003-2033, treatment costs for diabetes alone will increase by as much as 436% to $8.6 billion.[16]
- **More people are using health services, driving healthcare costs up exponentially.** More Australians (young and old) are increasingly visiting doctors, having a higher number of tests and operations and taking more prescription medication.[17] These conditions are resulting in higher healthcare costs per person and increased health expenditure across the system, with government health spending in Australia estimated to grow from 4% of GDP in 2009-10 to 7.1% in 2049-50.[14] Unchecked, healthcare expenditure could consume as much as 40% of Australian taxes by 2043.[18]
- **Demands on health services workers are changing.** By 2050, the demand for aged care staff will quadruple due to an ageing population.[19] An increased number of aged and chronically ill patients will also likely increase the need for longer-term care, requiring a greater breadth of skills to allow workers to be more effective with these patients.[20] The result will be greater competition for healthcare workers.
- **Delivery of care is changing, from institutions to independence.** There will be an increased drive away from institutional care and towards alternative community and independent care options, with advances in technology enabling this transition.[21] Additionally, in comparison to previous generations, Australia's elders will be better educated and more tech-savvy, with improved financial resources, more purchasing power, and higher expectations.[13]

## Energy (Electricity)

### SECTOR SUMMARY

The electricity grid is modernising towards a smart grid, improving visibility, reliability, monitoring and control of the electricity network. In addition to enabling a greater use of emerging technologies (such as renewables), modernisation will help to reduce operating costs, particularly those related to servicing peak demands, which account for a large portion of Australia's electricity expenditure. This will in turn help to control electricity price rises and consumer bill 'price shocks'.

### Key trends:

- **Household electricity prices are increasing.** Household electricity prices increased by 70% between 2007 and 2012,[22] resulting in a 'price shock' to Australian consumers. Whilst there are a number of reasons for this increase, a large portion was as a result of network costs (such as major electricity network upgrades),[23] which are forecast to increase. The current five year cycle for transmission and distribution networks, for example, will see an increase in investment of 16% and 60% (real terms) respectively.[24]
- **Servicing peak demand is expected to remain a key cost driver.** To ensure reliability of services and electricity generation, network capacity is designed to accommodate the highest amount of electricity consumption (peak demand) at any point in time. This peak demand is often driven by extremes in weather, such as a heat wave or cold snap. By its nature, peak demand occurs infrequently, yet still requires a large proportion of investment. For example, in New South Wales, peak demand events occurring for less than 40 hours per year (or less than 1% of the time) account for around 25% of retail electricity bills.[22] Whilst future rates of peak demand are uncertain, limiting its growth is

projected to save 2 c/kWh each year on the costs of electricity distribution between 2020 and 2050.[23]

- **The use of renewable power generation is growing.** There is growing societal pressure to reduce the electricity sector's greenhouse gas emissions, which in Australia is the single largest source of emissions.[23] This is resulting in a significant push for renewable energy sources such as wind, solar, hydro and geothermal. By 2049-50, it is expected that approximately 51% of Australia's electricity generation will be from renewable sources (up from 13% in 2012-13) with a large percentage coming from wind [21%] and solar (16%).[25]
- **The grid is moving towards two-way management and control.** Australia's electricity grid largely operates with systems, processes and technologies that are designed to manage energy flow in a single direction – from large generators to customers. However, improvements in technology (including renewable technology) supported by changes in policy, are enabling electricity to be generated at or close to the point of consumption. This allows surplus power to be fed back into the distribution network.[22] This concept, known as distributed (or on-site) generation, creates two-way energy flows, which must be carefully monitored to ensure reliability.
- **New developments are leading to a smarter grid.** Requirements to manage peak demand, decrease carbon emissions and facilitate on-site generation are driving a modernised, 'smarter' electricity grid, allowing greater visibility, reliability, monitoring and control of the network. This modernisation (which includes the roll-out of smart meters) is not unique to Australia. USA, Canada, Europe, Great Britain, Ireland, Japan and Korea for example, all have regions with smart grid and smart meter projects deployed or underway.[26]

## Government

### SECTOR SUMMARY

Government departments and agencies are digitising processes, systems and services in the face of greater consumer expectations, tightening budgets and increasingly complex operating environments. This transition to a more connected, digital government or 'e-government', is occurring at both state and federal levels and includes an increase in online services, coordinated whole-of-government strategies (such as consolidated ICT infrastructure), as well as improved collaboration and information sharing across government and with businesses and citizens.

### Key trends:

- **Consumer preferences are changing.** Consumers are increasingly choosing to interact via online channels and will expect that governments are agile and keep pace with private sector digital maturity. In 2012, Australians showed a strong preference for the use of e-government service channels over other means of interaction, with two thirds of people using e-government for their most recent contact.[27] By 2020, four out of five Australians will choose to engage with Government through the internet or other types of online service.[28] However, in order to satisfy consumer expectations into the future, governments will need to recognise the importance of convenience in interactions and the need to meet or exceed private sector service standards.[27]
- **Governments face increasing pressure to do more with less.** As demand for government services increases and budgets tighten, pressure will continue to be placed on governments to 'do more with less'. Virtually all governments are reducing staff levels, often without any real reduction in service levels.[29] Governments that can adapt and move to shared models of services, labour and resources through increasingly networked and digitised approaches, will have the ability to remain lean but still deliver on their mission.[29] In line with this, the Department of Finance estimates that their co-ordinated, whole-of government approach to data centres will avoid $1 billion in costs over the next 10-15 years.[30]
- **Digitised services can help to cut costs and increase productivity.** Globally, successful e-government projects have reduced transaction costs and processing times, and increased government revenues.[29] In Australia, the introduction of the Department of Immigration and Citizenship's 'SkillSelect' system in 2012 has seen a 200% increase in online skilled migrant applications and a 20-30% reduction in referrals to exception processing at Sydney Airport through the Border Risk Identification System.[28] Digitised services can also assist governments to contribute to productivity gains across the economy, through unlocking value in shared data.[31]
- **Governments are operating in an increasingly complex environment.** The issues faced by the public sector are increasingly multi-dimensional in nature and require more collaborative effort between governments, departments, agencies and public and private communities to innovate and develop more sophisticated solutions.[29] A key theme from the 2012 OECD E-Leaders meeting[32] acknowledged this, stating that governments need to take steps to defragment as they are historically structured to solve domain-specific problems. ICT and better information flow across boundaries were seen as key enablers of improved collaboration and co-ordination.

# Increased technology dependence: our digital future

The world is undergoing a digital transformation, driven by rapid technological innovation and uptake. Technology is becoming increasingly embedded into our personal lives, the way we do business and the way we govern our nation. This is transforming Australia into a truly digital and highly competitive economy, with cyber security capability central to our success.

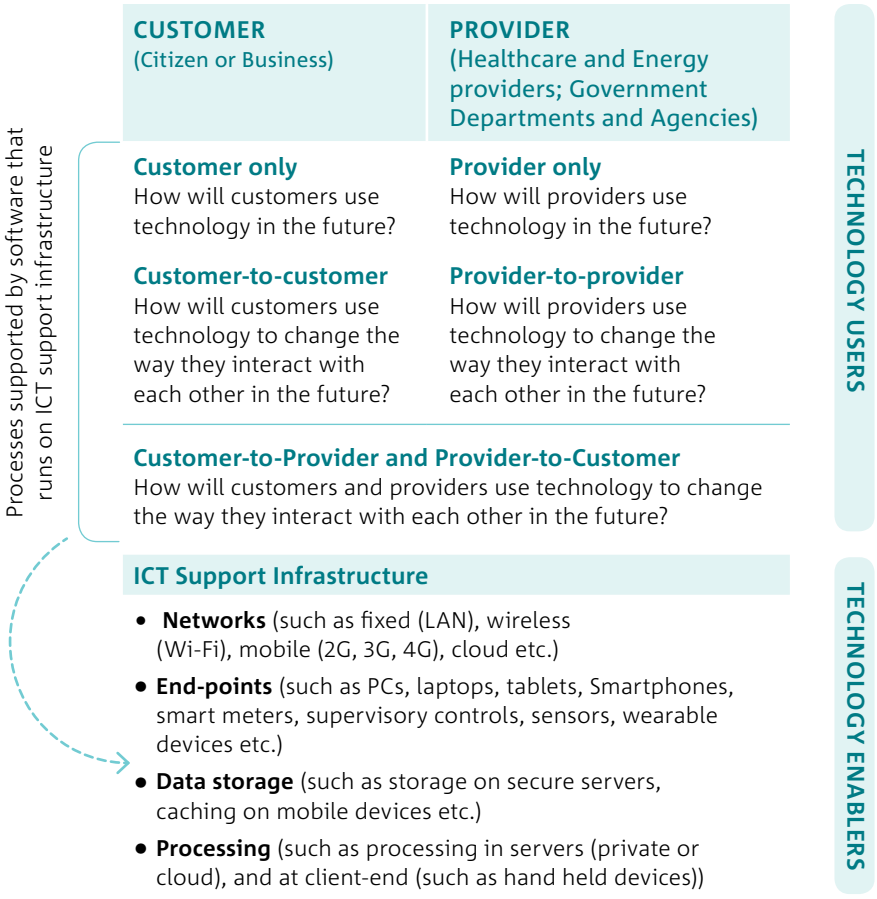
To understand our future cyber security needs, it is important to gain an appreciation of our future technology dependence. Given the pace of technology change, it is impossible to predict exactly how technology usage will evolve over the next decade. However, signs of our digital future are already here. Pockets of our economy that are more progressive, as well as specific technologies that are highly advanced and ahead of the curve, give us insight into how the nation could be transformed if adoption was widespread.

In exploring some of these developments, this section focuses on emerging technology usage trends across the key sectors of healthcare, energy (electricity) and government, providing a snapshot of our digital future.

Adopting a technology-use framework (Figure 2.0), we consider emerging technology usage trends across sectoral providers (organisations) and customers (consumers), and how these and broader technology trends are impacting underlying ICT support infrastructure. Customers and providers are considered to be the primary technology *users*, with underlying ICT support infrastructure components presented as the *enablers* to that usage (i.e. the systems, networks, processes and devices that allow us to use and interface with technology).

The technology-use framework presents a simplified picture of what is in reality a complex ecosystem of non-linear, dynamic processes, platforms and interactions. It is not intended as a comprehensive model, acknowledging that the lines between all dimensions of users and technology enablers are becoming increasingly blurred and interconnected. The trends explored are also not intended to be exhaustive, but provide an evidence-based indication of how the sectors and our nation are digitally evolving. Figure 3.0 provides a high level summary of these trends, which are explored in detail in the next section. This provides us with the foundation to explore cyber security implications going forward.

**FIGURE 2.0 – TECHNOLOGY-USE FRAMEWORK**




Across each of the sectors, providers and customers are considered to be:

| | CUSTOMERS | PROVIDERS |
|---|---|---|
| **Healthcare** | Citizens and recipients of health services | Public and private hospitals, GPs, allied health, etc |
| **Energy** (Electricity) | Citizens and businesses that are recipients of electricity services | Electricity generators, distributors and retailers |
| **Government** | All citizens and businesses | All government departments and agencies |

**FIGURE 3.0 – TECHNOLOGY DEPENDENCY TREND SUMMARY**

| | CUSTOMER TECHNOLOGY-USE TRENDS | PROVIDER TECHNOLOGY-USE TRENDS | CUSTOMER-PROVIDER TECHNOLOGY-USETRENDS |
|---|---|---|---|
| | **SUMMARY:** *The future customer will be increasingly empowered, with greater choice, a louder voice and a stronger connection to local and global communities.* | **SUMMARY:** *The future provider will be data driven, breaking down existing barriers to share information, skills, knowledge and infrastructure, within and outside of their organisation.* | **SUMMARY:** *The future customer-provider relationship will open up unprecedented levels of communication, personalisation and collaborative engagement, improving service delivery and creating new opportunities for growth.* |
| HEALTH | **Customer only**<br>• Shifting from provider-centric to patient-centric<br>• Customers more actively involved in own care<br>• Enabled by personal health records, personal monitoring devices and mobile applications<br>**Customer-to-Customer**<br>• Relationship expanding to encompass patient, family and the community<br>• Increasingly empowered and connected patients<br>• Enabled largely by social media and community websites | **Provider only**<br>• Rapidly evolving service delivery by transitioning to a more digital environment<br>• Enabled by electronic health records, cloud computing and mobility, and a new generation of diagnostic technologies<br>**Provider-to-Provider**<br>• Shifting from silos to a connected health services ecosystem<br>• Integrating of data, knowledge and expertise<br>• Enabling improved diagnosis, treatment, patient mobility, access to care and scientific research opportunities | **Customer-to-Provider/ Provider-to-Customer**<br>• Relationship between customers and healthcare providers will continue to evolve and deepen<br>• Greater personalisation and more frequent interactions<br>• Increased opportunity for preventative care and outreach through new remote care and consultation models |
| ENERGY | **Customer only**<br>• Shifting from reactive and consumption-based to more engaged and proactive customers<br>• Generating own energy and monitoring consumption<br>• Enabled by real-time data from smart meters and apps connected to appliances, buildings and homes<br>**Customer-to-Customer**<br>• Interacting in new ways and influencing electricity developments e.g. new consumer electricity sharing models<br>• Enabled by social media and energy technology advances | **Provider only**<br>• Step change in decision-making and load forecasting by combining real-time smart meter data and advanced analytics and modelling<br>• Greater application of advancements in remote monitoring, distributed generation and storage technologies<br>**Provider-to-Provider**<br>• Provider-to-provider relationship transforming, integrating data and information through use of smart meters<br>• Enabling smarter electricity grid, increased grid efficiencies and greater control and reliability of electricity | **Customer-to-Provider/ Provider-to-Customer**<br>• Evolving relationship between customers and providers as smart meters improve communication and real-time monitoring<br>• Greater information sharing, improved demand management and personalised energy pricing schemes<br>• Incorporation of personal electricity generation back into the grid |
| GOVERNMENT | **Customer-to-Customer**<br>• Rise of 'e-democracy' leading to more policy debate and discussion<br>• Faster, larger scale conversations happening outside of government channels – presents opportunities and challenges<br>• Enabled by social media and online collaboration | **Provider only**<br>• Digitising operations to reduce costs and increase flexibility e.g. leveraging cloud services, analytics, etc<br>• Improving processes and employee flexibility through teleworking and mobility technologies<br>**Provider-to-Provider**<br>• Greater sharing of data and services, infrastructure consolidation and whole-of-gov. technology roadmaps<br>• Greater integration, process efficiencies, reduced duplication, improved decision-making and a better view of operations and national needs | **Customer-to-Provider/ Provider-to-Customer**<br>• Interactions increasingly moving online<br>• Enabling improved communication, greater control (self-management), increased information accessibility, more efficient transactions and lower cost to serve<br>• Leading to improved experience, especially when dealing with multiple departments and/or agencies |

## Customer technology-use trends

The future customer will be increasingly empowered, with greater choice, a louder voice and a stronger connection to local and global communities.

### Healthcare

#### CUSTOMER ONLY

The focus in health services is shifting from being provider-centric to patient-centric, with customers taking a more active role in their own care through the use of personal health records, personal monitoring devices and mobile applications. This shift is expected to play a pivotal role in creating a proactive and preventative health culture in Australia.

#### Early indicators:

- **Australian Government's personally controlled electronic health record (PCEHR)** is enabling individuals to own and control their own personal health record, as well as share it. PCEHR provides significant value to those with chronic illness and disabilities, caregivers for the elderly and parents with small children.[33] By 2013/14, PCEHRs are expected to reach 1.5 million registrations.[34]
- The market for **wearable health and fitness devices** (such as wrist watches, chest and arm bands) is growing rapidly and estimated to reach 170 million devices in 2017, up from 21 million in 2011.[35] This new generation of wearable devices have the ability to monitor and wirelessly transmit health data on blood pressure, heart sounds and electrical activity, body and skin temperature, respiration, oxygen saturation and blood glucose.[36] Advancements will continue, evidenced by radical new innovations, such as the smart contact lens for Glaucoma detection.[37]
- **Growth in the use and sophistication of smart phones and mobile applications** (apps) is empowering individuals with unprecedented control of their personal health. In 2012, one in five US smart phone owners had at least one health app and 31% used their phones to look up medical information.[38] By 2016, as many as 142 million downloads of mobile health and fitness apps is anticipated.[39]

#### CUSTOMER-TO-CUSTOMER

Through the use of social media, the healthcare relationship is expanding beyond the traditional patient-doctor relationship to include a new customer-to-customer relationship, encompassing the patient, their family and the community. These relationships will result in increasingly empowered and connected individuals, moving care away from being a solitary experience.

#### Early indicators:

- One third of Americans have **gone online to better understand theirs or another's medical condition,** with 26% in 2012 having read about or watched someone else's experience with health or medical issues, and 16% having tried to find others who share similar health concerns.[40]
- **Health content and community websites are continuing to spring up**, offering up-to-date, often expert-checked information and advice to consumers on medical conditions. Medical website WebMD has grown in popularity exponentially, with an estimated 80 million unique visitors per month (as of March 2014),[41] providing knowledge, as well as hundreds of discussion communities, where members and experts can share and respond to health questions.
- Online health platforms are using **innovative approaches to connect consumers to one another in a more personalised way**, as well as improving the information on offer. Online patient community PatientsLikeMe engages with and empowers individuals through knowledge and peer support, connecting those with similar medical conditions and allowing for tracking and sharing of personal experiences. Launched in 2004, PatientsLikeMe now has over 200,000 patients on the platform and tracks 1,800 diseases.[42]
- **Consumers are increasingly being given more power and a stronger voice** through social media. Independent site Patient Opinion[43] allows patients to share feedback on experiences with health service providers, helping others to make decisions about their own care, as well as driving improvements within the healthcare system. Significantly, high volumes of feedback have been experienced from hard-to-reach groups such as the elderly, disabled and homeless, which Patient Opinion CEO attributes to people wanting "their voice to count for something, especially vulnerable people... this is because they normally don't know how to get their voice heard."[44]

# Energy

### CUSTOMER ONLY

The focus is shifting from a reactive, consumption-based model, to one where customers (citizens and businesses) are more engaged and proactively monitoring their energy consumption, through real-time data from smart meters and applications connected to appliances, as well as through the generation of their own energy (such as the use of renewable energy sources).

## Early indicators:

- **Energy monitoring, automation and control for non-residential buildings are expected to increase.** This will be particularly important for heating, ventilation and air-conditioning (HVAC), which are estimated to consume 9% of Australia's electricity and create over 55% of peak demand in CBD buildings.[45] The value of smart meter data to monitor and control electricity consumption will grow as building energy efficiency standards rise to include six, seven and eight star ratings.[46]
- Increasing sensitivity to electricity price rises is leading to a **greater adoption of in-home energy management devices and applications,** wirelessly connected to data from smart meters. The sophistication of energy management will increase as homes become connected with smart devices (machine-to-machine), such as the smart fridge, television and thermostat.[47] This will allow consumers to monitor, control and optimise consumption across their entire household.[48] In future, this may lead to 'set and forget' home monitoring approaches, allowing consumers to completely automate electricity consumption-monitoring based on their personalised needs.[49]
- **At-home (on-site) electricity generation** is expected to increase as technology costs fall and electricity bills continue to rise. Between 2008 and 2012, the total estimated install capacity of rooftop solar systems increased from 23MW to 1,450MW; based on a moderate growth scenario, the Australian Energy Market Operator (AEMO) estimate that capacity will hit approximately 12,000MW by 2031.[50] New business models may increase uptake (such as solar leasing schemes found in the US[51]). However, the growth rate of solar rooftop systems (or similar on-site generation methods) will be highly dependent on Government policy.

### CUSTOMER-TO-CUSTOMER

Advances in technology are enabling customers (citizens and businesses) to interact in new ways, with the potential to influence developments in the electricity sector. The growth in use of electric vehicles for example, is opening the door to new consumer electricity sharing models; whilst increasing use of social media is enabling communities to form around common issues of concern with a louder voice.

## Early indicators:

- Although currently a minor segment of the car market, electric vehicles are attracting the attention of state governments, due to growing consumer awareness, goals to improve air quality, economic benefits and energy infrastructure needs (such as re-fuelling stations).[52],[53] Unlike traditional combustion engine vehicles, which require refuelling at specialised, infrastructure-intensive locations (i.e. petrol stations), **electric refuelling can occur almost anywhere, opening the door to new customer-to-customer electricity sharing models.** This is already happening amongst citizens and businesses, such as the US City of San Francisco, which operates electric vehicle charging stations in city-owned parking facilities, including the San Francisco International Airport.[54] In 2013, the major retailer Kroger also announced plans to offer charging stations at a number of locations.[42] With the electric vehicle market expected to grow to 5-7% market share of total car sales by 2020[55], electricity sharing in the consumer market could also increase, which has the potential to cause significant shifts in the electricity sector (for example, through changes in electricity load requirements[56]).

- **Web-based platforms have the potential to strengthen the voice of communities** and mobilise change around common issues of concern and importance. An example in the energy sector is the debate about smart meter safety. Whilst energy providers and state government departments have provided assurances that smart metering devices are being installed safely and meet health and safety standards,[57],[58] online platforms have been used to enable anti-smart meter campaigns. A number of community websites have sprung up to influence the banning of smart meters(59) and cases of physical meter damage have also been investigated by police.[60] Whilst smart meter rollout is still continuing in Australia and around the world, such groups have the potential to stall progress, as a strong community voice demands a response. **As social media and online channels grow in use and influence, customers will continue to demand greater transparency, access to information and a voice in decision-making,** requiring electricity sector businesses to engage more closely with the community, as well as consider cultural change elements in the rollout of any new large-scale technologies.

## Government

### CUSTOMER-TO-CUSTOMER

Social media and online collaboration are enabling a new form of 'e-democracy', leading to unprecedented levels of citizen-to-citizen policy debate and discussion. As a result, public opinion and discourse is occurring at a faster rate and on a larger scale outside of government channels, posing both challenges and opportunities for the sector.

### Early indicators:

- **Web-based communication is fast evolving to create new opportunities and challenges.** The widespread use of the internet as a communication channel has changed the way we disseminate, access and process information, presenting significant opportunities for greater openness, transparency and accountability.[61] Online communication is not new, but with an increasing number of people connected to the web and collaborative platforms constantly evolving, citizens from all corners of the world are being empowered to discuss key issues, share ideas and effect real change on unprecedented levels (such as GetUp![57] and WikiLeaks[58]). However, the anonymity and reach that the web enables can pose new risks, particularly if information is inaccurate, falsified or misleading.[62] This will require the continued adaptation of policy and regulatory frameworks to reflect and respond to online developments. Despite challenges and risks, citizen-led online communication, including via social media platforms, will continue to play a key role outside of formal government communication channels.

- **Online collaboration to enable large-scale change is extending beyond the citizen, to include businesses with some serious power.** A large-scale example of this was the 2012 co-ordinated online protests against two proposed laws in the US Congress – the Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA). Protests were based on concerns that measures in these acts would harm the free distribution of information and lead to censorship if abused.[63] Several influential websites, such as the English Wikipedia, considered temporarily closing their content in protest; other sites such as Google, Mozilla and Flickr featured protests against the acts; and some shut down completely. It is estimated that 115,000 websites joined the internet protest,[64] which then extended offline and was reported globally. The impact of these collaborative protests was the shelving of the piracy bills and ceasing of further voting and progress.[65] The New York Times called this a "political coming of age from the tech industry".[66]

## Provider technology-use trends

The future provider will be data driven, breaking down existing barriers to share information, skills, knowledge and infrastructure, within and outside of their organisation.

### Healthcare

**PROVIDER ONLY**

Providers are rapidly evolving service delivery through transitioning to a more digital environment, enhanced by electronic health records, cloud computing and mobility, and a new generation of diagnostic technologies.

#### Early indicators:

- **Digitisation of providers extends beyond adoption of electronic health records and paperless environments.** Most providers have begun investing in the re-architecture of technology systems, applications and processes. For example, a number of Australian hospitals have increased investment in wireless technologies to enable care from ambulances to rooms,[67] as well as integration of biomedical and environmental machine-to-machine sensors and mobility investments allowing data to be displayed, stored and transferred between central nursing stations to a physician's tablet or handheld device[68].

- **Investment in cloud computing will increase over the next decade** in order to drive provider efficiencies across IT operations. By 2018, as many as 19,000 hospitals across Asia Pacific will adopt cloud solutions.[69] By 2023, pay-as-you-go clinical software is also expected to be used via the cloud across a number of providers, allowing compatibility and interoperability of systems from finance to clinical departments.[69]
- **Adoption of new and emerging diagnostic technologies will reduce testing costs, improve patient experience and deliver greater outcomes.** The high growth point-of-care-testing market, expected to reach over $9 billion by 2019,[70] is creating a new generation of portable, non-invasive, bedside diagnostic devices, which provide accurate monitoring and results within minutes and allow faster physician decision and action times. Phillips and Google are also demonstrating innovative progress through their "Google Glass" technology, which will in future allow clinicians to gain hands-free, voice-controlled access to critical information while operating or mobile through the hospital – enabling faster analysis, diagnosis and response.[71]

**PROVIDER-TO-PROVIDER**

Integration of data, knowledge and expertise across providers (underpinned by the rise of electronic health records) is transforming healthcare from siloed operations to a truly connected ecosystem of health services. This will enable improved diagnosis and treatment, greater patient mobility, increased access to care and greater scientific research opportunities.

#### Early indicators:

- **At a provider level, Australia's PCEHRs have experienced positive traction,** growing from 3,039 organisations registered to 4,502 between May and July 2013. While an estimate of 53% of General Practices (GPs) are currently registered in Australia,[34] greater opportunities are possible if adoption increases across all providers (such as pharmacies, aged care facilities and hospitals), such as in countries like New Zealand, Denmark and Sweden, who are further along in provider adoption rates[72]. Australia can look to these international experiences for lessons; however progress will be highly dependent on sector and government policy decisions.
- **Video conferencing, analytics and cloud-based services are enabling providers to integrate and leverage services from specialist providers.** For example, through telemonitoring technologies,[73] an experienced professional can supervise, train and assist a fellow practitioner on medical procedures remotely. In future, this may extend to telesurgery, where surgical procedures are conducted remotely via a robotic surgical system; such as the pioneering laparoscopic cholecystectomy successfully conducted on a patient in 2001 in France.[74] Although feasible, there are still challenges present, such as network latency and equipment cost.

- **In combination with real-time analytics, health providers will have the ability to make new scientific discoveries.** Hood and Flores predict the discovery and advancement of health research will shift from being communicated primarily through articles and journals to being "integrated through digital networks and heterogeneous databases that capture data from every clinical encounter".[75] This may improve the efficiency and success of drug development and research processes, which have been estimated to cost over $1 billion and take between 10-15 years on average to eventuate.[37] A pioneering example of this is the 2013 White House sponsored initiative on open science, "Champions of Change". Open scientific data and publications from thirteen leading people and organisations is being used to "accelerate progress and improve our world",[76] including an initiative publishing 400 trillion data points on disease in partnership with a children's hospital.

## Energy

**PROVIDER ONLY**

Energy providers have used technology for decades to improve operations, such as using control systems to drive greater efficiencies in energy management. However, new technology advancements, combined with access to real-time data via smart meters and data analytics, are enabling a step change in operational efficiencies, decision making and load forecasting.

### Early indicators:

- In addition to improving back-office functions via applying new IT service models (such as cloud computing), providers are increasingly **adopting and applying emerging technologies to significantly improve operational efficiencies.** This ranges from improvements in maintenance and remote monitoring, to the use of distributed generation and micro grids (small, self-contained electricity networks), which ease the burden of transmission and distribution to remote Australian communities.[77] With the expectation that energy storage costs will decline by 50% by 2030,[23] providers will also be able to ensure higher levels of network reliability, whilst at the same time reducing costs through deferred or decreased infrastructure investment.[78]
- Providers are facing an **explosion of data generated by smart meters,** which are measuring electricity usage in 30 minute intervals (compared to the historic monthly meter readings). Across Victoria, this equates to over 17,000 meter reads per year for each of the 2.5 million smart meters installed across the state.[79] As the smart grid expands to include smart devices in homes, businesses and operations, the amount of data collected will grow exponentially, making new developments in big data analytics of crucial importance to the efficiency and effectiveness of the grid going forward.
- Smart meter data combined with **analytics will increasingly enable invaluable insight into provider operations and customer usage and behaviour.** Frost and Sullivan present the journey of data-driven utilities in Europe evolving from simple reporting tools in 2013-15 towards advanced analytics and forecasting by 2020-25.[80] This journey will enable opportunities in areas such as cost and process optimisation, load forecasting, customer insight, new pricing models and data-driven decision making. As an example, the US utility company Oklahoma Gas and Electric (OG&E), which services nearly 800,000 customers, is leveraging analytics and high performance database technology to forecast energy demand and understand an individual customer's consumption data in hours instead of days – processing over 30,000 records per customer per year (up from 12 records per customer per year).[81] OG&E has also experimented with using its data to offer variable peak pricing programs and time-of-use programs that help customers understand energy saving opportunities.

### PROVIDER-TO-PROVIDER

Integration of data and information through the use of smart meters is set to transform the provider-to-provider relationship and enable a smarter electricity grid. This will help to increase efficiencies across the grid and allow for greater control and reliability of electricity (particularly in the management of electricity generated by renewable energy sources).

## Early indicators:

- **Australia is heading towards a more integrated, efficient, smarter electricity grid,** made up of smart meters, automated energy control and management systems, and process and policy change. This will help to transform siloed generation, distribution and retail activities into a truly integrated system that is digital, two-way, self-monitoring and self-healing, adaptive and, among other things, facilitates distributed generation and greater customer choice.[82] In the long term, this smart grid may expand to become Australia-wide, encompassing all current state energy grids.[22] However, integration will require greater smart meter penetration, which today is highly dependent on state-based policy and direction.

- **The integration of renewable energy sources will drive increased data sharing among providers, enabling improved monitoring, forecasting and reliability.** Operations can be significantly impacted by variability in wind and solar energy output, which is highly dependent on local weather conditions.[83] With Australian wind generation expected to rise from over 2,500MW in 2013 to approximately 11,500MW in 2020,[84] providers (particularly distributors and generators) will need to share a significant amount of data and information to closely monitor and control any fluctuations in generation. This will include using forecasting algorithms to combine current and historic load, with weather and geographic data to create new forecasts.[85] If not managed adequately, power issues could result, such as voltage spikes, which can impact reliability and safety.[56]
- The combination of smart meter infrastructure and renewable energy sources across the grid will result in **unprecedented levels of data communication across the grid and a significant reliance on data communication networks.** Using the Victorian smart meter example from earlier, the state would be conducting over 42.5 billion meter reads per year (17,000 reads per year x 2.5 million smart meters).[79] In the US, the Massachusetts Institute of Technology (MIT), predicted that "over the next 20 years, the growth in percentage terms of data flowing through grid communications networks will far exceed the growth of electricity flowing through the grid".[86] They went on to highlight that future advances such as the use of renewables and the requirement for real-time control would depend on both the data collection and communications network.

# Government

### PROVIDER ONLY

In addition to improving processes and allowing greater mobility of employees, individual government departments and agencies are digitising operations – eliminating paper processes, leveraging cloud services and developing analytics capabilities – to reduce costs and increase flexibility.

## Early indicators:

- **The use of cloud computing in Government is on the rise.** The US Federal Government cloud computing market alone is expected to reach $10 billion in annual value by 2018.[87] This is reflective of the implementation of the US Government's "Cloud First" policy, adopted in 2011, with improved efficiency, agility and innovation as the major drivers.[88] European Governments are also moving to cloud solutions to boost business and achieve cost savings and efficiency improvements.[89] Australia has set its own goals for transitioning to the cloud, releasing the Australian Government Cloud Computing Policy in 2013, stating: The Australian Government will be a leader in the use of cloud services to achieve greater efficiency, generate greater value from ICT investment, deliver better services and support a more flexible workforce.[90]

- Australia's Big Data Strategy anticipates that government will realise **substantial productivity and innovation gains from the use of big data.**[91] An example illustrating this potential is the Department of Immigration and Citizenship's risk tiering system, the Border Risk Identification System (BRIS), which is being used in Australia's international airports. A 2011 prototype of the analytics system, in conjunction with existing border risk data and systems, halved the number of travellers undergoing additional checks at immigration points, detected an increasing number of suspicious travellers and saved on average $60,000 per refusal of entry into Australia.[91] With over 42,000 travellers entering Australia every day and upward of 50 million movements, arrivals and departures across Australia's borders by 2020, big data analytics will become increasingly critical to border management.[92]
- A large number of Government departments and agencies are developing strategies to support **enterprise mobility (including bring your own device (BYOD) policies) and telework capabilities.** Further to improving productivity and efficiency, enterprise mobility can help reduce hardware and office costs and provide job satisfaction for employees, particularly those that travel frequently.(93) Adoption and maturity of enterprise mobility will in turn enable more flexible workplace models such as teleworking,[94] which could double in uptake with at least 12% of employees having telework arrangements by 2020.[95]

### PROVIDER-TO-PROVIDER

Whole-of-government technology roadmaps and infrastructure consolidation strategies are allowing a significant reduction in operating costs. This, combined with greater sharing of data and services, is enabling more effective inter-organisational linkages and process efficiencies, reduced duplication, improved decision-making, and a more comprehensive view of operations and national needs.

## Early indicators:

- **A shift is taking place towards connected governance and 'e-government-as-a-whole'.** Government departments and agencies are increasingly looking outside of their own boundaries and moving towards the concept of "e-government-as-a-whole", a more holistic approach to public sector ICT-enablement, which focuses on streamlining front-end service provision and integrating back-end systems, data, infrastructure and processes.[96] This will enable co-ordinated service delivery, cost savings amidst tightening fiscal environments and enhanced efficiencies. The Department of Human Services in Australia is a key example of this, bringing together major social and health-related service delivery agencies – Centrelink, Medicare and Child Support – to provide a more convenient and streamlined front-end and simplify transactions. This integration is part of a broader service delivery reform program aimed at improving services and increasing efficiencies through integration activities such as physically co-locating offices, implementing a central customer relationship management system across all services and streamlining customer registration and proof of identity processes.[97]
- **Information is being transformed into a government and national asset through data analysis and sharing.** The amount and breadth of data generated across governments is growing exponentially. Australian Government agencies alone installed an extra 93,000 terabytes of storage over 2008-2012 to cope with the increasing production of data.(91) Globally, it is estimated that we create 2.5 quintillion bytes of data every day, with 90% of the data in the world generated in the last two years alone.[98] By 2020, data production is estimated to increase 4300% annually.(99) However, this growing pool of data is only as valuable as the ability to analyse and extract meaningful insights from it, as well as the ability to share and integrate that information with other rich data sets. An example of this is the Singapore Geospatial Collaborative Environment (SG-SPACE) Initiative, which links up spatial data from the Land Data Hub, with information on people and businesses from other national data hubs (previously developed and operated independently). Using centralised IT infrastructure, 33 agencies have been able to share over 300 layers of data (such as addresses, land ownership, transportation and utilities networks), enabling better decision-making, improved efficiency and better quality of data.[100]

## Customer-Provider technology-use trends

The future customer-provider relationship will open up unprecedented levels of communication, personalisation and collaborative engagement, improving service delivery and creating new opportunities for growth.

### Healthcare

**CUSTOMER-TO-PROVIDER/ PROVIDER-TO-CUSTOMER**

The relationship between customers and healthcare providers will continue to evolve and deepen, with greater personalisation, more frequent interactions, and increased opportunity for preventative care and outreach through the use of new remote care and consultation models.

#### Early indicators:

- **Ongoing advances in ICT will continue to make telehealth more important to the future of healthcare**[67] and an increasingly popular care option to consider. Telehealth has been successfully adopted in North Queensland, where 18 communities spread over 750,000 square kilometres have now been turned into a single oncology department for cancer patients,[101] improving remote and regional community access, as well as the quality of care. The 2008 Whole System Demonstrator programme, setup by the UK Department of Health, was one of the largest and most complex controlled telehealth and telecare trials in the world and illustrated the potential impact of remote care technology. Involving over 6,000 UK patients, including 3,000 with one of three specified chronic conditions, findings reported a 45% reduction in mortality rates, 20% reduction in emergency admissions and a 14% reduction in bed days.[102]
- **End-to-end remote patient management services** highlight future opportunities to provide long term care for the elderly and those with chronic illness. For example, low-cost sensors, monitors and systems are allowing physicians, carers and families to monitor a patient's vitals, identify changes in movement or to simply stay in touch.[103] Healthcare providers are linked to patients through cloud-based information and communication platforms, complemented by the provision of physical devices to monitor and manage care (such as use of tablet devices). In future, this may include monitoring of implantable and ingestible devices, such as a wireless heart pressure monitor, allowing a doctor to review patient vitals and potentially prevent a heart attack.[37]
- Hood and Flores predict that in 10 years, everyone will have their genome sequenced and **every consumer of healthcare will have a virtual cloud of personal data**[75]. It will contain conventional medical data, molecular and cellular data, as well as complex imaging and demographic information. This would have a profound impact on the nature of care delivered by providers to their customers, allowing for far greater depth in personalised and tailored care through access to the comprehensive data and evidence in an individual's unique health profile.

### Energy

**CUSTOMER-TO-PROVIDER/ PROVIDER-TO-CUSTOMER**

The relationship between customers and providers is evolving rapidly and will continue to do so as smart meters improve communication and real-time monitoring. This will lead to greater information sharing, improved demand management, personalised energy pricing schemes and models to incorporate personal electricity generation back into the grid.

#### Early indicators:

- Historically, energy retailers led the majority of customer interactions. However, advanced metering infrastructure has sparked a **new relationship between distributors and consumers.** Energy distributors, such as Jemena in Victoria, are providing customer portals that allow consumers to understand consumption habits and opportunities for savings.[104] In addition to creating a positive relationship between customers and distributors (beyond servicing and responding to faults and issues), increased communication will over time, improve consumer understanding of cost drivers in electricity billing and the long term value of the smart grid.

- **Demand management and cost-reflective pricing** is set to curb the staggering costs related to peak demands. As discussed earlier, today's electricity grid is structured around meeting peak demand. This results in consumers (no matter their income) sharing network costs – which account for 40-50% of energy bills[22] – to meet infrequent occurrences of peak demands. However, smart grid technologies offer opportunities to manage demand by shifting consumer and business behaviour through personalised pricing (cost-reflective pricing) and incentives that reduce bills and energy usage during peak demands.[105] For example, Queensland distributor Energex was able to attract 59% of consumers to change to off peak hot water, pool filtration and air-conditioning.[23]
- Opportunities for customers to **sell excess electricity back to the grid** are becoming available in some states. Future growth is not only dependent on energy generation and storage technologies but will rely on market and government policy. For example, the rate paid (feed-in tariff) for electricity fed back into the grid has dropped considerably in Australia (from 60 to 5-10 cents per kilowatt hour in some states[23]), making it a less attractive option. Nevertheless, a large number of customers are still making electricity contributions. In Victoria, over 88,000 customers (homes and small businesses) will continue to receive 60 cents per kilowatt hour until 2024 for any excess electricity sold to the grid.[106]

## Government

### CUSTOMER-TO-PROVIDER/ PROVIDER-TO-CUSTOMER

Citizen and business interactions with government are increasingly moving online, allowing for improved communication, greater control (via self-management), increased information accessibility, more efficient transactions, and a lower cost to serve. The net effect is an improved experience for citizens and businesses, particularly when dealing with multiple departments and/or agencies.

- **Governments are engaging closely with citizens and becoming more open.** Enabled by technology, leading governments globally are increasingly becoming flatter and decreasing the distance between government and citizens.[29] This is changing the citizen engagement model entirely, moving away from one or even two-way interactions and simplified toolsets such as online forms and discussion forums, to a more complex, comprehensive ecosystem of interactions, using more sophisticated tools such as blogs, e-petitions and virtual worlds.[29] Aligned with this, the Australian Government launched Gov 2.0 in 2010, declaring Australia an "Open Government", requiring better access to and use of government information, as well as improved collaboration with citizens on policy and service delivery, and greater participation with citizens through consultation, including via social networking and crowd sourcing.[107] In the US, the Administration has initiated several new technologies and initiatives leveraging social media to engage with the community,[29] including Challenge.gov, which facilitates collaboration between government agencies and the public to solve national problems.[29]
- **A new era of open data is here,** with governments all around the world opening up their information and making it more accessible to citizens online to analyse, reuse, build on, visualise, map and share.[29] As of 2011, ten countries or more have open data portals making government data accessible in a form that can be easily used by citizens, including Australia through the data.gov.au portal.[29] This is not only making governments more transparent and accountable, but also driving innovation through enabling the development of applications and solutions using the open data sets and application programming interfaces (APIs). In the US for example, an "Apps for Democracy" contest was launched, where citizens were challenged to develop innovative applications using open government data. The initiative cost the Washington government $50,000 and returned 47 iPhone, Facebook and web applications with an estimated value in excess of $2.3 million to the city.[108] It has inspired similar movements in over 50 countries and cities around the world.
- Given the growing use of social media, several government agencies have invested in **social media monitoring tools** to gain feedback about public perceptions and responses to campaigns, to observe and respond to citizen needs, as well as to engage in the conversation. In Australia, the Department of Human Services' Digital Media team uses a highly visual tool that collects and analyses online posts and comments from a variety of different channels, identifies trending topics of conversation and allows staff to respond to citizens and guide them to the right information or clear up any misunderstandings.[109] As more citizens take conversations online, social media monitoring tools can be incredibly powerful, as they allow governments to keep a finger on the public pulse and enable new, more direct feedback loops with citizens.

# Implications on ICT support infrastructures

Analysis clearly indicates that technology and digital processes are becoming more deeply embedded into operations and across key service offerings.

Whilst this report analyses the healthcare, energy and government sectors, the technology trends identified have commonality across all sectors. These combined trends will drive us towards a more digitally enabled and digitally mature Australia. They will also lead us to becoming more dependent on the use of technology, or more specifically, on the underpinning technology infrastructure that makes that usage possible.

ICT support infrastructure comprises a broad range of integrated systems, devices, networks and hardware, all controlled by a combination of people, processes and software programs. For many organisations, this also includes third party service providers managing large components of infrastructure, as well as onshore and offshore resources. Alongside the growing breadth of components encompassed within ICT support infrastructure, each of these is also undergoing continuous change as a result of technology advancements and business drivers.

For the purposes of this report, we have focused on four main categories – networks, end-points, data and processing (refer to Figure 2.0) – all of which can be seen as critical technology enablers.

## Networks

- **Network traffic is increasing.** Data growth trends are expected to impact network traffic over the next 5 – 10 years, placing strain on communication.(110) Analysis conducted by CISCO estimated that over the next five years, global internet protocol (IP) traffic will increase threefold and by 2017 will reach 1.4 zetabytes (1.4 billion terabytes) per year.(111) Whilst a majority of Australian traffic is currently from fixed-line broadband,(112) mobile data traffic has also been increasing. Data captured by the Australian Bureau of Statistics (ABS) has highlighted that over a three month period, data downloads from mobile handsets had increased from 3,695 Terabytes in 2011(113) to 19,636 Terabytes over the same period in 2013.(114)
- **Network boundaries are dissolving.** The concept of a corporate network boundary is being eroded through greater use of public and private networks (such as internet and cloud services), increasing use of third party providers needing access to internal systems, and the growing range of un-trusted customer and employee devices accessing systems and data.(115) This poses significant challenges to information management, particularly in maintaining productivity whilst at the same time, protecting sensitive data across systems, applications, devices and locations.

## End-Points

- **Devices are becoming increasingly connected.** The breadth of end-points connected to the network are growing beyond personal computers, smart phones and tablets to include wearable devices, sensors and displays (such as in-home energy displays discussed earlier) to name a few. CISCO has estimated that the number of connected end-points or objects (also called the 'internet of things') will increase from 8.7 billion in 2012 to approximately 50 billion by 2020.(116)
- Machine-to-machine (M2M) is evolving to become smarter and more autonomous. Frost & Sullivan define Machine-to-machine (M2M) communication as "digital communication between an endpoint and an enterprise's backend system over cellular networks".(117) M2M communication is growing and will serve as a key enabler for trends related to smart systems and remote monitoring, automation and control. In Australia, it is estimated that M2M communication will increase from 1.4 million connections in 2008 to 6.7 million in 2015, with an expectation of approximately 116.6 million M2M connections across Asia Pacific by 2015, driven primarily by smart metering and vehicle telematics.(118)

## Data

- **The amount of data is growing rapidly.** Globally, it is estimated that we create 2.5 quintillion bytes of data every day, with 90% of the data in the world generated in the last two years alone.[98] By 2020, data production is estimated to increase 4300% annually[99]. In addition to creating storage challenges, data growth is driving us towards information overload, which can impact productivity and decision making.[119]
- **Data is more available and accessible than ever before.** Improved network connectivity is enabling large volumes data to be accessible at any time, on-demand, via cloud services. However, cloud services are not without their challenges. It has been identified that cloud providers may transfer data between data centres and jurisdictions based on technical constraints, network efficiencies, or legal and economic factors, which may lead to uncertainty about where information is located and will be stored.[120] Aside from the legal ramifications of the different jurisdictions, sensitive data becomes harder to control and audit, which is particularly important for compliance and regulatory purposes.

## Processing

- **Greater volume, variety and velocity of data are creating new processing challenges.** Understanding and making decisions based on the complex interactions of information requires advanced analytics and processing capability. The processing challenge is compounded due to the sheer volume of data (with organisational transaction volumes ranging from millions to billions), the variety of data (both structured and unstructured), and the velocity in which we access the data (in near real-time).[121] To put this into perspective, per month Facebook reportedly services 570 billion page views and billions of photos, status updates and comments.[122]
- **Processing is becoming an on-demand service for a fractional cost.** By designing workloads and applications appropriately, cloud computing offers significant opportunity to scale up or down processing (or compute power) on-demand. In addition to offsetting large capital expenditure, cloud computing offers the ability to complete processing activities rapidly. For example, NASA JPL leveraged Amazon Web Services to process over 200,000 high-resolution images in a few hours for under $200, compared to using a single local machine that took 15 days on the same task.[123]

# A complex digital future

Our digital future is one that we are yet to fully comprehend – customers will be increasingly empowered with greater choice, providers will be data driven and borderless, and the boundary between these two groups will be virtually non-existent. In response, ICT support infrastructure and technology usage will continue to evolve, meeting customer and provider needs and generating new opportunities. The scale of change is vast and the pace at which it is occurring is increasing exponentially. These factors combined make for an increasingly complex technology landscape, and in turn, an increasingly complex landscape to secure. To understand the implications that this has on our level of vulnerability to cyber security threats, the following section explores the threat landscape, looking at types of threats, threat actors and their motivations and how the threat environment is changing.

# Cyber security threats:
## a familiar yet evolving landscape

The cyber security threat landscape is changing, with breaches (both intentional and unintentional) and tools evolving in complexity and sophistication.[1],[124],[125] This provides for a challenging environment in which to operate, as organisations are faced with new, more dynamic, multi-faceted threat challenges, alongside those that are familiar and persistent – all of which are becoming increasingly difficult to detect and counter.

In order to better understand this changing threat landscape and in turn, how it is impacting our level of vulnerability to cyber breaches, we have provided:

- an overview of cyber threats **(the what)**;
- a summary of threat actors and their motivations **(the who and why)**; and
- some examples highlighting how the threat landscape is evolving **(the how)**.

## Understanding cyber threats

**A cyber threat can be defined as:**

1. Any identified effort directed towards access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, security or availability of data, an application or a [federal] system without lawful activity.[126]
2. The possibility of a malicious attempt to damage or disrupt a computer network or system.[127]

As the definitions imply, cyber threats involve intentional, malicious efforts; however, it is important to highlight that accidental and negligent activities can also be regarded as cyber threats.[128] While not part of many formal definitions, an unintentional cyber threat can be as simple as the accidental leakage of information due to poorly trained staff[129] (discussed further in 'Threat actors' section).

There are many different types of cyber threats, which can be broken down and analysed in a multitude of ways. The varying literature looks at threats in terms of:

- the tools or technologies used (such as worms, Trojans, exploit kits);
- the techniques and methods used (such as phishing, spamming);
- the intent (e.g. denial of service, breaching of data);
- the threat actor at play (such as insiders, hacktivists, cybercriminals);
- the emerging threat and technology trends (such as evolution of botnets, threat commoditisation, malware in the cloud); and/or
- a combination of all of the above.

The subject of cyber threats is truly complex and multi-dimensional in nature, with a plethora of existing, in-depth material available from a range of different sources.[1],[126],[130],[124],[131],[125],[132]

For the purposes of this report, we have chosen to focus on the threat landscape more broadly, providing some initial context through summarising different threat actors at play and their motivations, followed by an overview and some key examples of how the overall threat landscape is evolving.

## Threat actors

A threat actor (or threat agent) can be described as an individual or group of people that can manifest a threat.[133] There are many different types of threat actors with a diverse range of motivations behind their actions; and they can be both hostile (intentional) and non-hostile (unintentional).[129] In order to better understand these threat actors, their motives and their capabilities, they are generally grouped into profiles. Drawing on a number of different sources,[128],[1],[131],[134],[129] we have consolidated a subset of threat actor profiles below, including both hostile and non-hostile.

**HOSTILE/INTENTIONAL**

| ACTOR | DESCRIPTION | MOTIVATIONS | SKILLS/ CAPABILITY |
|---|---|---|---|
| Script Kiddies and Cyber Vandals | Script kiddies are generally young hackers, looking for a challenge. They make use of existing tools and techniques and whilst they are often novices, can cause significant impact in large numbers or through being susceptible to other threat actors such as organised criminals. Cyber vandals are more knowledgeable and often develop their own tools, carrying out attacks because they can and to purposefully expose vulnerabilities. | • To play a prank<br>• To show they can<br>• For the challenge | Vary from Low to Medium |
| Trusted Insiders (Internal Actors) | Trusted insiders are individuals who are currently or were previously employed by an organisation, as a permanent staff member, contractor, temporary staff, suppliers etc. and who abuse their employee privileges. Due to access (at varying levels) to a vast range of organisational information and assets, this group can cause high impact damage. | • Disgruntled, dissatisfied<br>• Corruption<br>• Financial gain | Medium to High |
| Hacktivists | Hacktivists are individuals or groups of people who perform cyber attacks in support of a particular cause or ideal. Attacks are sometimes attributed to particular groups or can also be anonymous in nature. Often hacktivists gain support from other threat actor profiles, such as script kiddies and cyber vandals, who will contribute their skills and advice in support of a cause. | • Ideology<br>• Defending ideas<br>• Evoke change<br>• Public attention<br>• Embarrass target | Vary from Low to High |
| Corporations | Corporations can become threat actors in order to gain a competitive advantage over business adversaries, usually those they are in competition with for revenues or resources. Activities primarily encompass data breaches and intelligence gathering. | • Obtain business intelligence<br>• Gain competitive advantage<br>• Theft of IP | Medium to High |
| Organised Crime (Cyber criminals) | Organised criminals or cyber criminals are individuals or groups of people, who undertake criminal activity professionally. In cyberspace, this includes activities such as fraud, use of ransomware and delivering malicious tools and infrastructure. This is a very high impact group of threat actors, with significant resources, often possessing specialist skills or having easy access to such expertise through connected criminal networks. | • Financial gain | Medium to Specialist |
| Terrorists | A terrorist in cyber security terms, is someone who uses cyber technology to facilitate or execute malicious activity, such as violence or the threat of violence. Activities include social engineering, taking over critical infrastructure operations or communications and infiltrating government systems. Cyber terrorists have high access to resources and capability. | • Ideology<br>• Social and/or political change<br>• Evoke fear | Medium to Specialist |
| Nation States | Nation States or state-related actors refer to individuals or groups that form part of a country's government. Cyber attacks in this category are highly strategic, advanced in nature and very well-resourced. Activities include accessing secret information (political, economic and military-related) and threatening the availability of critical infrastructure. | • Access state and/ or military secrets<br>• Improve geopolitical position or position of power | Specialist |

When we reflect on the subset of threat actor profiles listed above, both hostile and non-hostile, we are presented with a complex mix of personalities, motives, actions, skill sets and capabilities to consider in the cyber security space. If we combine these with the plethora of existing and newly evolving threat tools and techniques, as well as the dimensions of digitally-enabled globalisation and increasing interconnectedness, the cyber threat playing field becomes ever more complex – increasing the difficultly in predicting how, when and why attacks might occur, as well as heightening the potential impact and reach of both intentional and unintentional manifested threats.

**NON-HOSTILE/UNINTENTIONAL**

| ACTOR | DESCRIPTION |
|---|---|
| Employees (Accidental or Reckless) | An employee can unintentionally become a threat actor either through:<br>• *accidental means* i.e. poor training in cyber security measures and the safe use of programs and systems, leading to unforseen mistakes; or<br>• *reckless activity* i.e. purposefully shortcutting safeguards to save time or cut corners, not fully understanding the consequences of their actions |
| Information Partners | An information partner is someone with whom a business has shared sensitive information (such as a supplier, a partner organisation etc). Information partners can unintentionally become threat actors through having poor internal security and protection measures of the proprietary information shared with them. |
| Researchers | Researchers in the cyber security space are individuals or groups who perform research activity into cyber security developments and challenges. Through their research, they often expose weaknesses in security areas, which although unintended, can lead to increasing vulnerabilities through the open dissemination of that information to hostile threat actors. |

## Evolving threat landscape

As with all technology areas, cyber threat tools and techniques have undergone continuous evolution and change over the years. This is due to a range of factors, such as the increased complexity of IT-products, new tools and skills, greater knowledge transfer, and new opportunities for profit(1).

Whilst there are many areas of change across the threats landscape, we have chosen to highlight three key examples: the growing number of threat vectors (or pathways) for attack; the evolving sophistication of attack approaches; and the increased accessibility of threat tools, through trends such as threat commoditisation.


### Threat vectors are multiplying

A threat vector is a pathway or tool that can be used to attack or compromise a target – which could be anything of value to the threat actor, such as a device, a bank account or even an individual i.e. stealing one's identity.(135) As technology continues to evolve towards more interconnected networks, systems and devices, the vectors that can be used to gain access to desired targets are significantly multiplied and become almost insurmountable.

The scale of this challenge becomes evident when you consider the growth of connected end-points which, as discussed earlier, are expected to hit 50 billion by 2020(116) (see 'Increased technology dependence' section). These end-points are increasing in power and sophistication and are often integrated with a broad range of accounts, applications and services. For example, smart phones and tablets often hold a large amount of personal information such as emails, contacts, credit card details and log-in details. These devices are increasingly being accessed on the corporate network (particularly given bring your own device (BYOD) trends), yet can still be easily exposed via malicious efforts, such as the fake Angry Birds Space and Instagram apps,(128) or be used as a form of intelligence (for example, taking photos of surroundings).(124) In addition, mobile devices have hardware resource-limits as a result of size and portability requirements, which make common desktop security applications unsuitable for use.(125)

### Attack approaches are becoming more sophisticated

Beyond improving technical sophistication, attackers have evolved their approaches (or practices), moving away from large-scale, disruptive activity, towards focused, tactical objectives, using lower-profile, multi-stage attacks.(136) This allows an attacker to target weaknesses across a number of individual physical and cyber components (i.e. multiple attack vectors), collecting small amounts of information that when combined, helps them reach a particular objective.(137) For example, stealing one's identity requires multiple sets of information (depending on the motivation and intended use) such as name, date of

birth, address, bank details, health records and so on. Rather than going straight to the source, which is likely to be very heavily protected, the information could be gathered by breaching multiple systems across one or more sectors. This could use a combination of password cracking, network sniffing, phishing, physical theft or even going through people's trash.[138]

This changes the game significantly, making every sector, person, system and device potentially an attractive target. Even if the information that is accessible does not appear intrinsically valuable, it may provide an easy pathway to something of greater value or provide the missing piece to a larger puzzle of cyber threat activity. Furthermore, these attack approaches can be extremely hard to detect. For example, in May 2013 over 40,000 domain names and site IPs were compromised using Darkleech, which cleverly ensured that breaches would fly under the radar by using techniques such as maintaining a list so that specific IP addresses were only sent malicious redirects once.[130]

### Threat tools are becoming more easily accessible

Software (malware) cyber threats are becoming commoditised, with a broad range of simplified and easily accessible tools now on the market. These tools (often supported by online tutorial videos) allow more people to execute cyber attacks including beginner-level threat actors, such as script kiddies.[128] One area of concern is the use of exploit kits, which the European Union Agency for Network and Information Security (ENISA) define as "ready-to-use software tools offering a large variety of functions, configuration options and automated means to launch attacks."[1] Sold online, these kits allow a user to simply select the desired target and payload (such as spyware, code, etc.), with the exploit kit then delivering the payload, which conducts its attack.[131]

In addition to being easy to use, exploit kits are often very effective as they target technical vulnerabilities in applications or devices that are commonly not up-to-date or patched for long periods of time.[128] For example, the internet security firm Sophos reported that Blackhole, one of the most popular exploit kits, facilitated 28% of all web threats it had detected in 2012.[131] The popularity and use of exploit kits have led to expectations that developers may focus on services for these kits (such as support, customisation, etc.) as a business opportunity[1]. Given the similarities to the software-as-a-service cloud model, some are calling this trend malware-as-a-service or crime-as-a-service.[131] Whilst this may sound appealing to a novice hacker, some exploit kits could also be used to take control of a large number of machines and launch a variety of attacks[131].

## Implications going forward

The evolving, complex threats landscape stresses the need for strong cyber security skills and capabilities. These skills will need to be supported by emerging prevention, detection and response technologies, harnessing data analytics and machine learning, cryptography and risk management modelling tools that are at the forefront of cyber research. In particular, the diverse range of threat actors highlights the importance of positioning cyber security as a business and national risk, rather than a purely technical one. To understand these implications in greater detail, the following section examines national and sectoral vulnerabilities relevant to Australia and uses three future scenarios to help explore the impact of one or more serious cyber breaches.

# An increasingly vulnerable environment

Through observing three key sectors (healthcare, energy and government) we have seen how Australia is set to evolve into a more mature digital economy and become increasingly dependent on technology to drive and enable this progress. Technology is becoming deeply embedded into our personal lives, into the way we do business and the way we govern our nations, with the lines between these dimensions blurring as digitisation drives us to greater convergence.

This digital evolution will open up new and exciting opportunities for our nation. However, with new opportunities also come new challenges. Increasing use of technology (and the resulting data being generated), which is digitally interconnected across multiple layers of networks, systems and end-points, leads to greater exposure to cyber space – making cyber security a capability of crucial importance. As we have explored, ensuring cyber security is a complex, multi-faceted challenge, as the threats landscape changes and evolves to encompass more sophisticated tools and attacks, as well as breaches (both unintentional and intentional) which are familiar and persistent, yet still difficult to detect and counter.

These factors combined make for a more vulnerable environment in which to operate. Vulnerability in cyber security terms can be defined as:

*A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.*[139]

When considering the complexity of the systems we operate within (at an individual, organisational and national level) and all of the inherent resources within those systems (both physical and virtual), vulnerabilities will always be present. It is impossible to protect against everything – as the Australian Government acknowledges in their National Plan to Combat Cybercrime, "As with crime in the physical world, no amount of action by governments and the private sector can combat every cybercrime".[4]

This does not mean that we should adopt an attitude of fear and move to reduce risk by shying away from technological progress or implementing measures that will stifle digital innovation and technology adoption – these are critical factors to the sustainability and productivity of our society and the economy. It does mean however, that a shift is needed in the way we look at cyber security.

## A changing paradigm

Traditionally, cyber security has been thought of as the responsibility of those with specialised skill sets - back-end IT teams, security experts and the like. It is something that is managed away from view and assumed to be inherent in our systems and processes, enabling the rest of us to safely communicate, do our jobs, perform transactions, access services, manage and share private information. However, as we have explored, we will continue to move away from closed, individualised systems, networks and even devices, to a more interconnected ecosystem with disappearing boundaries. In this environment, cyber security becomes an issue that is increasingly difficult to contain. Strong security at one point of a process can break down as data travels through multiple systems, platforms, networks and devices. This means that the security of the interconnected ecosystem we are moving towards will only be as strong as its weakest link – and that the responsibility for that security must move to becoming one that is shared, extending out to every organisation, every government department and agency, and every individual. It is important to acknowledge that many organisations and some industries are already making progress in this area. However, in order to be truly effective on a national scale, this progress needs to advance and extend across all players.

## Implications of a breach

A cyber security breach occurs when one or more vulnerabilities are successfully exploited (intentionally or unintentionally) by a threat actor, which usually results in a compromise of confidentiality, integrity and/or availability of resources. These elements are often referred to together as the 'CIA triad' and are a core principal of information security[140],[141]. The National Institute of Standards and Technology (NIST)[142] define this CIA triad as:

**CONFIDENTIALITY**

A requirement that private or confidential information not be disclosed to unauthorised individuals.

**INTEGRITY**

***Data integrity:*** A requirement that information and programs are changed only in a specified and authorised manner.

***System integrity:*** A requirement that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorised manipulation of the system.

**AVAILABILITY**

A requirement intended to assure that systems work promptly and service is not denied to authorised users.

Whilst a single breach of confidentiality, integrity or availability can lead to a range of consequences, broader impacts include reputational damage, loss of consumer and business trust, financial and productivity losses and significant disruption to the lives of citizens.

If we consider this at a sectoral level based on the three focus sectors of healthcare, energy (electricity) and government, breaches could lead to incidents such as misdiagnosis and inaccurate treatment of medical patients; inability to claim critical government benefits (such as Centrelink); loss of power to residential and industrial sites; incorrect billing; identity theft, fraud, blackmail or corruption using personal and/or business data – to name a few. The range of possible implications is vast and will continue to expand as we become a more digitised nation with increasingly connected systems, networks, processes and devices.

In order to tangibly illustrate some of these consequences and the range of potential impacts that could face us as a nation, the following section employs scenario analysis. Looking forward to 2025, in a highly digitised, interconnected Australia, what cyber security challenges could the healthcare, energy and government sectors be faced with? And how would a compromise to security play out if our maturity has not advanced at pace with our digital evolution?

## Scenario analysis

A scenario is a hypothetical but plausible story about future events, constructed from observed trends and historic data. In general, scenarios are more useful for broadening thinking, than giving a strong prediction of what will happen in the future. Therefore, the scenarios presented in this report are conceptual; no conclusive evidence exists that one scenario is more likely than another.

However, by exploring scenarios, one has the opportunity to test current day strategies and trends and actively plan for change. For example, Royal Dutch Shell plc, a pioneer of scenario planning, has been applying scenarios for decades, and this method is observed to have helped them navigate the highly disruptive oil price shocks in the 1970s.[143],[144]

The scenarios in this report explore the impact of one or more severe cyber attacks across the healthcare, energy and government sectors. They combine existing trends discussed in the 'Increased technology dependence' and 'Cyber security threats' sections, to highlight a future where Australia has failed to develop our cyber security capability at pace with technological change and adoption. Given that the impact of such failures will only become apparent once our technology reliance has increased, the scenarios have been set in 2025 – approximately a decade from now – allowing sufficient time for existing technology trends to play out.

The scenario presented for each sector is also intended to be self-contained. That is, it is implied that each scenario is happening independently, not that all three are occurring at the same time. However, the events portrayed in each scenario can be applied more broadly, as the different types of vulnerabilities explored are not necessarily unique to any single sector. For example, vulnerabilities caused by a disgruntled employee, weak security points or the inability to make a quick recovery from a major breach, are common and plausible across any sector and any organisation.

### Australia's digital economy: setting the scene in 2025

Australia's economy in 2025 has transitioned to one that is highly digitised and data driven. However, the evolved cyber threats landscape, combined with minimal progress of Australia's cyber security maturity, has created vulnerabilities across the nation. This has resulted in a steep increase of cyber breaches (both unintentional and intentional) impacting citizens, key sectors and the nation overall.

Australia's healthcare, energy (electricity) and government sectors have continued on their technology evolution trajectory (see 'Increased technology dependence' section) and by 2025, have radically transformed. Integration efforts have paid off, with data (namely personal health records, smart grid data, and integrated whole-of-Government information) at the heart of services, operations, and decision making.

The sectors have leveraged technology to curb costs and improve productivity. Customer and provider lines continue to blur as consumer experience, empowerment and personalisation take centre stage to create new service models and opportunities for growth. In addition, Australia's technology services and know-how provide us with competitive advantage overseas.

Unfortunately, our rapid digital 'coming-of-age' is not without challenges. When viewed in isolation, each sector has advanced dramatically. However, cracks in our digital economy are becoming evident and are chipping away at our previously realised savings and social benefits. Data breaches in 2025 have transitioned from being relatively irregular or unknown, to being highly visible and a common occurrence.

This challenge has stemmed from rapid digital adoption without an equally rapid phase of cyber security maturity. For example:

- cyber security education levels remain low, yet workers are expected to execute digitally sophisticated tasks;
- cyber security and information management investment and capabilities are noticeably varied across the nation and each sector;
- digital governance and control mechanisms are poor – particularly for processes that have not been redesigned (such as ones that simply transitioned a process from paper to electronic); and
- online behaviours of citizens and sectors have not changed as, unlike a physical act of theft, digital breaches remain less understood and visible, with the impact (on most occasions) not being felt until long after it occurs.

The result is a plethora of weak security links across a hyper-connected economy, allowing simple attacks to remain very effective. Malicious, as well as unintentional breaches, such as information leakages and data manipulation (i.e. adding, modifying or deleting information) have accelerated in recent times. Whilst technology advancements have been applied to help identify and eliminate breaches, they are also serving as tools for newer, more sophisticated cyber attacks, which take advantage of our technology and data dependence, as well as our propensity for error.

In this current environment with greater susceptibility to attack, a number of plausible scenarios have been considered that could eventuate across each of the key sectors, if no further action is taken towards raising cyber security maturity levels.

## Energy scenario: a not-so-trusted insider

Fears of a cyber attack on Australia's electricity grid have been realised, with a disgruntled third party contractor causing major power losses and cascading failures during a heatwave; resulting in significant strain on emergency services, lost productivity for businesses and significant community anger and frustration.

Australia's electricity grid has continued to follow technology adoption trends. In 2025, it is a smarter, highly automated, integrated and efficient grid, supported by moderate to high levels of smart meter penetration across a number of states. Data and networks across the grid play a pivotal role in communicating the billions of smart meter data reads, as well as supporting the increasing automation and remote management of industrial control systems such as supervisory control and data acquisition (SCADA) systems, which control assets across the entire grid. Peak demand challenges and electricity prices have also been reduced through incentive-based pricing and demand management.

However, the risk of a cyber security attack to the electricity grid, previously raised by the US Federal Government[145] and the World Economic Forum[146], has been realised. The carefully planned, malicious cyber attack, purposefully executed during a heatwave, has led to major power losses across an Australian state, and as a result, national uproar.

It is believed that the attacker, a disgruntled third party contractor, used a similar approach to that of the 2000 Maroochy Water Services cyber breaches in Queensland.[147] This Queensland incident, which was one of the earliest examples of a malicious control system breach, saw the attacker use his expert knowledge on at least 46 occasions, to remotely manipulate data within SCADA systems; causing malfunctions in sewerage pumping stations and "800,000 litres of raw sewage to spill out into local parks, rivers and even the grounds."[147]

The risk of this type of attack occurring has been well documented. Industrial control systems, which were once isolated from corporate IT systems, have over time followed trends towards greater integration.[148] This integration creates new risks, as attackers can tunnel from a corporate network into a SCADA system[149]. The evolved threats landscape has now also led to more sophisticated and easily accessible attack approaches, such as freely available exploit kits (as discussed in the 'Cyber security threats' section). These kits, like Metasploit, which directly targets SCADA systems, are enabling novice attackers (such as hacktivists and script kiddies) to cause significant damage, such as the case where a hospital security guard installed malware and took control of heating, ventilation and air-conditioning.[150] However, outside of the Maroochy Water Services breach, very few cases of confirmed SCADA breaches have been discussed publically, which may have over time contributed to the apathy and lack of cyber security investment.

Whilst the details of the current electricity grid attack are still being investigated, the impact is highly visible. There have been cascading failures across the grid resulting in public transport and traffic chaos, rapid redirection of emergency electricity supplies to priority facilities such as hospitals, and citizens and businesses left without power. In addition, the sweltering heat has caused significant pressure on emergency services. It is unknown as yet whether there has been a spike in deaths as a result, as seen with past heatwaves such as that of 2009 in Victoria, which is thought to have killed more than 370 people.[151] The extent of the current electricity outage has been compared to past natural disaster-related blackouts, such as the Victorian bushfires in 2007 and Queensland's Cyclone Yasi in 2011, both of which caused approximately 200,000 homes to lose power.[152],[153] Though hard to estimate, the financial impact of lost earnings and service costs as a result of the recent attack on the grid are believed to be very high – if the result is anything akin to the 2003 blackout impacting Canada and north eastern United States, it could amount to billions.[154]

Although lasting only a number of hours, the recent outages generated significant community anger and frustration as the attack was carried out by a single individual. This has led to diminishing trust in smart grid technology and security, much of which has been directed at energy companies, smart meter technology itself and the government for national expenditures on the grid. Calls for security reform have become polarised with those wanting drastic overhaul of the grid and its security controls, and others protesting that an overreaction in security procedures will lead to significant costs, higher electricity bills and little in the way of greater security guarantees.

## Healthcare scenario: weak-links start to crack open the system

Disparities in cyber security investment and capability across healthcare providers have led to an increased frequency of data misuse cases, exploiting weak-links across the sector; resulting in greater levels of fraud and concerns of a long term decline in patient-provider trust.

Spiralling healthcare costs and a greater level of care requirements have led to stronger policies and significant investment towards digitising Australia's healthcare sector. However, the decentralised provider landscape, combined with low levels of cyber maturity, has limited the overall digital sophistication of the sector. Whilst there has been a steep increase in the uptake of national electronic health records, particularly among GPs and hospitals, there are still large pockets of providers not yet on board. Nonetheless, greater technology adoption across the nation has led to almost all providers using computerised systems, devices, applications and electronic records in one form or another.

Recent calls for greater scrutiny of the digital health landscape have been sparked by a growing number of cases resulting in the misuse of patient health data. These types of cases are not new. Each year, a small portion of healthcare practitioners in Australia incorrectly bill for services, misrepresenting dates and procedures. In 2012-13, for example, the Australian Professional Services Review completed 44 cases, resulting in repayments totalling over $1 million for 19 cases, 14 reprimands, and 4 practitioners who had their access to Medicare benefits suspended and/or disqualified.(155)

However, while past incidents have been largely unintentional in nature, recent cases have become more targeted and malicious, including individual practitioners intentionally breaching the system for personal and financial gain. This is comparable to a past New Zealand case, where a single practitioner charged almost 6,000 fraudulent claims valued over $140,000 to a health board using repeat prescriptions for patients, including patients that were deceased.(156) In addition to individuals, a growing number of health institutions have been manipulating data for various competitive and economic reasons, including skewing their reporting. This is similar to the 2012 incident where an ACT hospital manipulated over 11,000 records to improve Emergency Department performance metrics.(157)

What is troubling is the fact that emerging cases are not localised, due to vulnerabilities across the sector and very few being related to core national eHealth systems (which tend to have stronger security protections in place). The vast majority of cases have exploited inconsistencies in cyber security and technology maturity across the varying players in the healthcare sector, including GP's, hospitals, specialists, pharmacists, dieticians, physiotherapists and chiropractors – specifically exploiting weak-links in cyber security.

The types of vulnerabilities across these players vary significantly, many of which have not improved by much over the last decade. There are a number of providers still with insufficient information management practices, similar to the hospital identified in 2012 that "gave employees greater access to the data than their role should have warranted."(128) Other providers continue to operate with very poor knowledge and practices related to medical devices and systems (especially legacy systems), such as those identified in 2013 by the U.S Food and Drug Administration (FDA), including malware in computers, smart phones and tablets, uncontrolled and poor use of passwords and issues related to software updates and patches.(158) Equally troubling is the continuation of major vulnerabilities using less sophisticated methods, such as physical theft, which in 2013 was identified as the largest cause of breaches to personal health records in the U.S. (specifically physical theft of laptops and desktop computers).(159)

This relative ease of access to patient records across the board has led to a surge in healthcare crime, in particular healthcare fraud. Criminals are transitioning from higher risk ventures, such as drug trafficking, to defrauding the health system, which is seen to be lower risk and more lucrative in the long run.(160) Accessing the information in electronic records, criminal syndicates have been using the identities of hundreds of patients and doctors to make falsified reimbursement claims, similar to past cases, one of which amounted to over $35 million in false medical bills.(161) Healthcare fraud has become a "high volume, low value" crime, with small operations adding up to billions of dollars each year in costs to the healthcare system, which could be spent on patient care.(162)

Given the disparate nature of recent healthcare cyber breaches, the full extent of the impact to the entire sector is not yet understood. Taking the effect of healthcare fraud alone as an example, the financial impact to Australia is

suspected to cost between 3 to 10% of national healthcare expenditures (i.e. approximately $5 billion to $16 billion in 2022-23[16]), in line with past international estimates.[163] Attackers have also become increasingly daring, no longer settling for small scale activities. In the past, blackmail and data ransom for example, were characterised primarily by demands for small amounts of money – such as the 2012 case where four Australian medical centres had their medical data locked and held for a ransom of $3,000 (increasing at $1,000 per day until paid).[164] Cases now are increasingly reporting high volumes of patient records being held ransom for much larger sums of money, similar to a past case where 8 million patient records were deleted and held ransom for the sum of $10 million.[165]

Whilst cyber security breaches across the healthcare sector have resulted in a large number of patient records being compromised, it is not exactly known if and how all of the records are being used. There are those who fear the information is associated with robbery cases, for example, using records to understand when a patient is in the hospital and not at their residence. Others have warned citizens that their compromised data may result in non-health related breaches if they are using similar passwords for other banking and government systems. There is even a resurgence of past fears that data access could lead to misuse by insurers, employers and pharmaceutical organisations.[166]

More concerning is the potential long term social impact. This includes past fears resurfacing of patients withholding information about conditions that may cause social stigma and discrimination (such as psychiatric conditions or HIV),[167] jeopardising the overall quality of treatment. The sector has reached an impasse – while data and technology provide immense value to the effectiveness of services and quality of care, they are also seen to be deteriorating patient-provider trust, which could unravel much of the progress made to date.

## Government scenario: sizeable data breach provokes a bold response

A significant data breach has driven the Government to take a large number of highly integrated government services offline for a sustained period while the breach is assessed and resolved; causing significant economic and reputational damage.

In 2025, services across the Australian government sector have largely transitioned online, decreasing costs and improving citizen and business experience. These services are a result of the highly successful, whole-of-government technology strategies that promoted significant infrastructure consolidation and greater use of analytics, cloud computing and mobility technologies, as well as greater integration of data across departments, agencies and where suitable, third party providers.

However, a major cyber breach across departments has caused the loss of highly sensitive information and large volumes of citizen data. Although a global activist group have claimed responsibility for the breach of classified Government records as part of their transparency movement, the specific malware used is believed to have been designed and exploited by a third party interested in the citizen records. Unfortunately, it is not yet understood if the third party actor is a nation state, organised criminal group or an individual actor.

This has driven the Government towards the bold action of taking impacted departments and their services offline while they assess the extent of the breaches, rectify security holes and understand the broader vulnerabilities across whole-of-government systems. The highly integrated nature of government services has also required additional state and federal systems to be disconnected from the network as a precautionary measure. Although some have considered the action to be extreme, it is not too dissimilar to past international cases, such as the 2011 Canadian Finance Department and Treasury Board incident where networks were targeted by attackers.[168] In response, it was reported that the Government disconnected the two departments from the internet and kept them offline for nearly two months, as security officials conducted their investigation and removed compromising software.[169]

Whilst there have been a series of breaches leading up to this event, it is not believed that they are connected to the recent incident, as attacks on Government websites are not unique. In 2011-12, there were more than 400 cyber incidents against government systems requiring a significant response by the Cyber Security Operations Centre.[5] During the same period, there were reports of at least 10 breaches to computers of Australian Federal ministers.[125] And in 2012 there were also reports of 26 "serious cyber threat incidents" to inner Victorian agencies.[170] Motivations for attack vary considerably (see 'Cyber security threats' section). However, recent times have seen a spike in activity from hacktivists, similar to the past group known as "Anonymous", who successfully performed a targeted attack on the Australian Parliament House website in 2010, protesting internet filtering legislation[171], as well as a 2013 attack to the ASIO website, which was taken down for a few hours.[172]

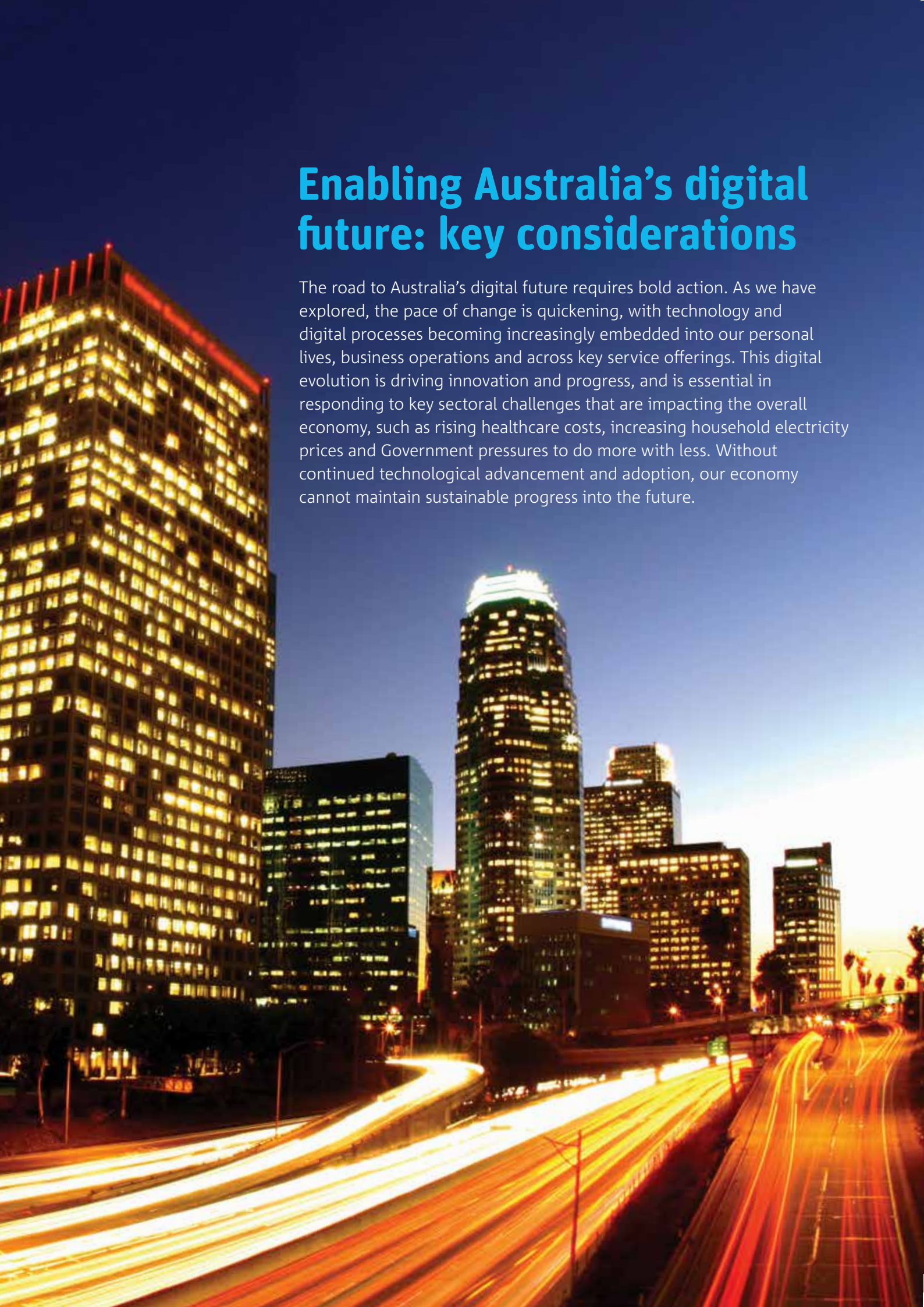
Many of the attempted breaches are believed to be malicious in nature. However, over the past year there have also been a number of non-malicious incidents reported, which are being investigated. These incidents highlight process and cyber security education flaws as major contributors to breaches, which are adding to the recent concerns. Most have been considered as accidental; however this does not mean they were without impact, resulting in diminished citizen trust and embarrassment to government departments and agencies, particularly from incidents disclosing classified information. These disclosures add to the negative impact of past similar incidents, including the 2014 inadvertent release of 10,000 Australian asylum seeker personal details,[173] the 2011 technical error that led to details of UK nuclear powered submarines to be published online,[174] and the 2007 accidental loss of discs containing information on the 25 million UK citizens that claimed child benefits.[175]


The recent breaches and halt of online government services have sent a shockwave across the nation. Whilst many of the departments and agencies have reverted to manual processes and work-arounds, the complexity of data and system integration, as well as greater use of cloud solutions and telework services, has made processes highly inefficient. Some have compared the loss of government services to the U.S. Government shut down in 2013, an event which lasted for 16 days and caused a $2 – $6 billion loss in output, delayed energy projects (such as the Bureau of Land Management was unable to process permits for drill applications), delays in trade due to a hold on import and export licenses and applications, impacts to business and sectors dependent on government verification services, delays to tax refunds and halts to federal loans.[176]

Whilst the total impact of recent events to the Australian economy is not yet known, the public has expressed fear and outrage about the breaches and the extreme measures that are now in place. Although citizen and business trust in online government services do not appear to be irreversibly damaged, future progress and opportunities through the use of technology have stalled, with calls for less integration and greater levels of manual processes.

# Enabling Australia's digital future: key considerations

The road to Australia's digital future requires bold action. As we have explored, the pace of change is quickening, with technology and digital processes becoming increasingly embedded into our personal lives, business operations and across key service offerings. This digital evolution is driving innovation and progress, and is essential in responding to key sectoral challenges that are impacting the overall economy, such as rising healthcare costs, increasing household electricity prices and Government pressures to do more with less. Without continued technological advancement and adoption, our economy cannot maintain sustainable progress into the future.



However, strong progress inevitably comes with risk. As we have investigated, increased technology adoption and greater digital interconnectivity expose us further to cyber security threats – a landscape which is changing, with breaches (both intentional and unintentional) and tools evolving in complexity and sophistication. These combined threat challenges with our increasing dependency on technology, together make for a more vulnerable environment in which to operate.

The challenges that are evolving out of our technological progress present what may seem like a daunting picture for our nation. However, the opportunities emerging from our digital evolution are vast. The development of new business models, products and services are enabling more productive businesses and a more innovative economy. Advancements in data analytics and machine learning are allowing us to better understand network anomalies and harness big data. Progress in cryptography techniques are helping to better secure information. And sophisticated risk management modelling tools are allowing leaders to make more informed cyber decisions. Technology may contribute to our ongoing security challenges, but it is also a key part of the solution.

Ensuring our future success will require bold cyber security leadership and investment now. It will require ongoing science and technology research that can identify emerging cyber security challenges and develop practical solutions. And it will require a cultural shift, extending cyber security responsibility out to every organisation, every government department and agency, and every individual. This change in culture must bring with it a change in behaviour – away from the historic approach of centralised containment and control, where breaches are considered failures and cyber security is considered a compliance burden. And towards a commitment to improving skills and education to lift security awareness and outreach; towards proactive investments in tools, processes and strategies that take advantage of new technologies and are on par with the maturity of evolving threat challenges; and towards evolving current perceptions about cyber security to understand the central role this capability has in enabling our digital future.

This new direction implies that cyber security is not simply a technology challenge. It is also a cultural challenge and one that extends beyond traditional information security practices. All of these important dimensions must be considered and included in the development of our strategies going forward. In the section that follows, we present what may serve as input to such forward planning and action, outlining key considerations in the areas of people, process and technology, as well as posing strategic questions for all to consider in the journey ahead to enabling Australia's digital future.

## People

The first step towards a more secure cyber environment is the acknowledgement that cyber security is a shared responsibility – i.e. it is not 'owned' by any single entity[125]. Every individual no matter what group – *citizen, business, research, government or defence* – has a crucial role to play in ensuring the security of the entire digital ecosystem. Greater knowledge is a key part of this and will help all individuals, organisations and sectors navigate the uncertain environment ahead.

Addressing knowledge gaps will not only help strengthen our security capability, but will enhance societal trust of all digital systems. Knowledge is essential to the success of any technology-driven strategy aiming to target future economic and social challenges faced by the nation or individual sectors.

Cyber security knowledge can be subdivided into a number of areas, including improving understanding of the cyber ecosystem and its inherent challenges, considering what new cyber skills and capabilities are required, and developing greater awareness of the business and personal risks that we assume through our actions

### Key considerations:

- **Ensure that all individuals understand the cyber ecosystem and its inherent challenges:**
  - How do we develop stronger leadership that promotes a positive digital culture and brings the cyber security conversation out of back-end IT and security and into all businesses, homes and board rooms?
  - What techniques can be used to extend cyber security education, tools and information out to customers, as well as employees, to strengthen and expand the cyber security team?

- What strategies can be applied to empower citizens and customers to better manage their digital identity, security and privacy across the growing range of online services used?

- **Develop and mature cyber capabilities across the nation:**
  - How do we expand cyber security capabilities to include social aspects, as well as technical aspects? Social aspects could include political and institutional theory, behavioural science, international law, ethics and social.(177)
  - What can we do to ensure that the evolution in our technology adoption and dependence is matched (or closely followed) by evolution in cyber security knowledge, skills and policies? How can this be supported through targeted education policies?
  - How do we create a culture that enables greater sharing of cyber security challenges and breaches, without fear of sector and/or shareholder repercussions?
- **Understand business and personal risks that we assume through our digital activities:**
  - What successful strategies can be applied to help all individuals better understand digital risks, allowing them to make more calculated and informed decisions?
  - How can we shed light on the increasing value of data, including how pieces of seemingly invaluable information can be combined and used to create significant negative impact?
  - What new approaches and techniques could be implemented to provoke a change in behaviour following a cyber breach? That is, how can we create better feedback loops that help people to understand the impact of a cyber breach - and thus modify their future behaviour to prevent repeated negative effects?

# Process

All organisations and systems operate within environmental constraints. These include financial and capability constraints, as well as those that are physical and geographical in nature. This often leads to the need for lower cost strategies and solutions that provide the same or higher levels of security. Whilst technology provides assistance in addressing this challenge, an often overlooked area is the value generated by improving processes and practices.

As an example, comprehensive compliance measures and strict policies can serve to reduce risk and enable greater control over security and systems. However in reality, people are inclined to cut corners if they know it will take days to decipher compliance measures and months to implement them, or if the prescribed devices and systems are slow and difficult to use. This is the nature of human behaviour and is a vital consideration in designing new cyber security solutions going forward.

As such, process considerations in cyber security should include practical considerations about the systems, their usability, and the way we deal with cyber breaches.

## Key considerations:

- Improve the way we design systems from the start of their lifecycle:
  - How do we enforce stronger measures to avoid simple design flaws, such as poorly coded software and poorly designed processes?
  - How can we avoid simplistic digitisation activities whereby processes are purely transitioned from paper to digital without any redesign or cyber security considerations?
  - What approaches can be applied to create greater resilience in systems and across sectors so that the impact of a breach is not as pervasive?
- Make systems usable, consistent and considered:
  - How can user-centred design techniques be applied to simplify interfaces, avoid over-engineering and minimise change required, while embedding 'invisible' (to the user) security sophistication?
  - What processes and policies should be applied to rapidly enable greater levels of data sharing and collaboration across sectors and diverse groups while maintaining privacy needs?
  - How can we devise processes that maximise the value of data without creating data overload, or simplifying data sets to the point where providers miss critical information?
- Foster cyber security approaches that are practical and actionable:
  - How do we maximise the value and impact of compliance, while reducing the time, energy and dollar investment needed? How do we avoid the false sense of security that comes with documentation?
  - How can we design processes that automatically make anomalous behaviour or breaches in data integrity apparent to the user?
  - What practical strategies and processes can be applied to improve the speed at which a potential breach is assessed and the vulnerabilities resolved?

# Technology

As our technology dependency increases and the threats landscape evolves, so too will the cyber security technology solutions employed by sectors, organisations and individuals. These technologies will continually evolve and mature, automating and simplifying tasks, as well as empowering employees and citizens to take advantage of the digitised environment.

However, as we have previously explored, ICT support infrastructure is also rapidly evolving and growing in complexity. Network boundaries are dissolving, yet network traffic is increasing; devices are increasingly connected and smarter; and data volume, variety and velocity are dramatically changing the way we need to process information. Together, these changes require greater levels of intelligence, pattern matching and analytics to be built into our cyber security technologies.

Whilst there are a number of cyber security technology changes to consider, we have chosen to focus on the areas of verifying trust, detecting and assessing intrusions and recovering from a breach.

## Key considerations:

- **Help systems and people verify digital identity and trust:**
  - What emerging strategies and techniques can be applied to improve identity management and ensure a system, application or individual can verify identity and establish trust?
  - How do we manage the increasing number of digital access points (and threat vectors) as a result of mobility trends, whilst still offering users greater flexibility?
  - How can advanced sensors and intelligent devices be applied to help verify the trust of an individual without over-complicating login processes?
- **Apply technology to improve the way we discover and assess a breach:**
  - What technologies can be used to discover unknown vulnerabilities and anomalous activities within the network? How do you differentiate this activity from normal human or machine behaviour?
  - How can we develop solutions to detect a breach, even if nothing has been leaked or altered (as yet)? For example, a criminal organisation may gain access to a system but not act until they have the right opportunity to exploit the data.
  - What technologies could be used to increase the frequency of audit across growing datasets without hampering business activities or incurring significant costs?
- **Develop strategies to swiftly recover from a breach or incident:**
  - What technologies can be applied to remove all known infected systems, applications and devices from the network, while maintaining business continuity?
  - How can we leverage technology to increase the speed at which cyber security breach information is shared across the community, without creating fear or panic?
  - How can we better understand cyber risks at the edges of organisations, systems and networks (including weak links), particularly given the mixture of legacy and new IT systems and the greater levels of integration with third party services?


## CONCLUSION

Addressing these key strategic questions form a starting point towards actionable change.

In the increasingly digitised, complex world we live in, ensuring cyber security can seem like an insurmountable challenge. However, a collaborative effort focussed towards addressing targeted cyber challenges, can lead to substantial positive impact.

Alongside existing national and defence-related strategies, the research community in partnership with industry and Government have a vital role to play in Australia's digital future. In an evolving cyber landscape with greater levels of change and uncertainty, innovation and cutting-edge technology are central to the people, process and technology solutions going forward.

Amidst an environment of economic uncertainty, shrinking budgets, increased competition and the growing cost of doing business, investment decisions among competing priorities are becoming increasingly difficult to make. In acknowledging this challenge, it is important to understand that taking a proactive approach to evolving current cyber security solutions will help to counter reactive measures, which are more disruptive, inefficient and costly to businesses and our economy. Targeted investments now, along with a commitment to evolve skills and capability, will help to curb risks and reduce financial outlays in the long run.

Australia's transition to a truly digital economy will drive our nation towards further economic, social and competitive success. However, realising this future vision is dependent on the actions we take now. Strong cyber security capability is central to a strong digital economy.

# References


1. European Union Agency for Network and Information Security (ENISA). ENISA Threat Landscape 2013 – Overview of current and emerging cyber-threats. ENISA: 2013.
2. Stahl S, Pease KA. Effectively Managing Information Security Risk: Citadel Information Group, Inc; 2007. Available from: **http://citadel-information.com/wp-content/uploads/2010/12/Effectively-Managing-Information-Security-Risk-0701.pdf**.
3. Moteff J. Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Theats, Vulnerabilities and Consequences. United States Congress: Congressional Research Service, Library of Congress, 2005.
4. Attorney-General's Department. National Plan to Combat Cybercrime: Commonwealth of Australia; 2013. Available from: **http://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/National%20Plan%20to%20Combat%20Cybercrime.pdf**.
5. Department of Defence. Australian cyber security centre to be established: Commonwealth of Australia; 2013. Available from: **http://www.defence.gov.au/defencenews/stories/2013/jan/0124.htm**.
6. Attorney-General's Department. Cyber Security Strategy: Commonwealth of Australia; 2009. Available from: **http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf**.
7. Patteson C. Cyber security – the facts Australian Security Magazine: 2013.
8. Australian Bureau of Statistics (ABS). Snapshot of Personal Fraud – Personal Fraud, 2010-2011, cat. no. 4528.0: ABS; 2012.
9. Australian Broadcasting Corporation (ABC). China blamed after ASIO blueprints stolen in major cyber attack on Canberra HQ 2013. Available from: **http://www.abc.net.au/news/2013-05-27/asio-blueprints-stolen-in-major-hacking-operation/4715960**.
10. Department of Human Services. Annual Report 2011–12: Commonwealth of Australia; 2012. Available from: **http://www.humanservices.gov.au/spw/corporate/publications-and-resources/annual-report/resources/1112/resources/dhs-annual-report-2011-12-full-report-web.pdf**.
11. Productivity Commission. An Ageing Australia: Preparing for the Future Australia: Commonwealth of Australia; 2013.
12. Australian Treasury. Australia to 2050: Future Challenges (Intergenerational Report): Commonwealth of Australia; 2010. Available from: **http://archive.treasury.gov.au/igr/igr2010/report/pdf/IGR_2010.pdf**.
13. Morris M, Ozanne, E. and Miller, K. Smarter technologies for older people: a systematic literature review of smart technologies that promote health and wellbeing of older people living at home. Australia: Institute for a Broadband-Enabled Society, 2012.
14. Hajkowicz S, Cook H, Littleboy A. Our Future World: Global megatrends that will change the way we live (the 2012 revision): CSIRO; 2012.
15. World Health Organization (WHO). Chronic diseases and health promotion: WHO; 2014. Available from: **http://www.who.int/chp/en/**.
16. Goss J. Projection of Australian health care expenditure by disease, 2003 to 2033. Canberra, Australia: 2008.
17. Daley J, McGannon, C. and Savage J. Budget pressures on Australian governments 2013. Available from: **http://grattan.edu.au/static/files/assets/ff6f7fe2/187_budget_pressures_report.pdf**.
18. CSIRO. Health Services: Better accessibility, productivity, and quality of care through digital innovation. Australia: 2013.
19. Productivity Commission. Caring for Older Australians. Canberra: 2011.
20. Health Professionals Workforce Plan Taskforce. Health Professionals Workforce Plan 2012-2022. 2012.
21. Fitzpatrick N. IBISWorld Industry Report Q8400: Health Services in Australia. IBISWorld, 2013.
22. Productivity Commission. Electricity Network Regulatory Frameworks. Canberra: 2013 Report 62.
23. CSIRO. Change and choice: The Future Grid Forum's analysis of Australia's potential electricity pathways to 2050 Australia: CSIRO; 2013.
24. Australian Energy Regulator. State of the Energy Market 2013 Victoria Australia: Commonwealth of Australia; 2013.
25. Syed A. Australian Energy Projections to 2049-50. Australia: Bureau of Resources and Energy Economics; 2012.
26. Global Smart Grid Federation. The Global Smart Grid Federation 2012 Report: Global Smart Grid Federation; 2012. Available from: **https://www.smartgrid.gov/sites/default/files/doc/files/Global_Smart_Grid_Federation_Report.pdf**.
27. Department of Finance and Deregulation. Interacting with Government: Australians' use and satisfaction with e-government services: Australian Government Information Management Office (AGIMO); 2011. Available from: **http://www.finance.gov.au/publications/interacting-with-government-2011/docs/interacting-with-government-2011.pdf**.
28. Online government service delivery: Department of Broadband, Communications and the Digital Economy; 2013. Available from: **http://www.archive.dbcde.gov.au/2013/september/national_digital_economy_strategy/advancing_australia_as_a_digital_economy/part_three_achieving_our_goalsbuilding_on_the_2011_national_digital_economystrategy/online_government_service_delivery**.
29. World Economic Forum (WEF). The Future of Government: Lessons Learned from around the World: WEF; 2011. Available from: **http://www3.weforum.org/docs/EU11/WEF_EU11_FutureofGovernment_Report.pdf**.
30. Department of Finance and Deregulation. Australian Public Service Information and Communications Technology Strategy 2012-2015: Australian Government Information Management Office (AGIMO); 2012. Available from: **http://www.finance.gov.au/files/2013/01/APS_ICT_Strategy.pdf**.

31. State Government of Victoria. Victorian Government ICT Strategy 2013 to 2014. 2013. Available from: **http://digital.vic.gov.au/wp-content/uploads/2013/02/Victorian-Government-ICT-Strategy-web.pdf**.

32. Organisation for Economic Co-operation and Development (OECD). Communiqué of Ms. Ann Steward, Chair of the 2012 OECD E-Leaders meeting; Australian Government Chief Information Officer and Chair of the OECD Network on E-Government.: OECD; 2012. Available from: **http://www.oecd.org/governance/eleaders/communique2012.htm**.

33. Archer N, Fevrier-Thomas U, Lokker C, McKibbon KA, Straus S. Personal health records: a scoping review. Journal of the American Medical Informatics Association. 2011;18(4):515-22.

34. National Electronic Health Transition Authority (NEHTA). NEHTA Scorecard, August 2013 Australia: 2013.

35. Allied Business Intelligence, Inc. Wearable Sports and Fitness Devices Will Hit 90 Million Shipments in 2017: Allied Business Intelligence, Inc.; 2012. Available from: **https://www.abiresearch.com/press/wearable-sports-and-fitness-devices-will-hit-90-mi**.

36. Pantelopoulos A, Bourbakis NG. A survey on wearable sensor-based systems for health monitoring and prognosis. Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on. 2010;40(1):1-12.

37. Turisco F. The Future of Healthcare – it's health, then care: Computer Sciences Corporation; 2010. Available from: **http://assets1.csc.com/innovation/downloads/LEF_2010FutureofHealthcare.pdf**.

38. Fox S, Duggan M. Mobile Health 2012 USA: Pew Research Center; 2012. Available from: **http://www.pewinternet.org/files/old-media/Files/Reports/2012/PIP_MobileHealth2012_FINAL.pdf**.

39. Dolan B. Report: 44M health app downloads in 2012 MobiHealthNews: Chester Street Publishing, Inc.; 2011. Available from: **http://mobihealthnews.com/15029/report-44m-health-app-downloads-in-2012/**.

40. Fox S, Duggan M. Health Online 2013: Pew Research Center; 2013. Available from: **http://www.pewinternet.org/files/old-media/Files/Reports/PIP_HealthOnline.pdf**.

41. eBizMBA Inc. Top 15 Most Popular Health Websites (March 2014): eBizMBA Inc.; 2014 [27 March 2014]. Available from: **http://www.ebizmba.com/articles/health-websites**.

42. Upbin B. PatientsLikeMe Is Building A Self-Learning Healthcare System Forbes.com: Forbes Media LLC; 2013. Available from: **http://www.forbes.com/sites/bruceupbin/2013/03/01/building-a-self-learning-healthcare-system-paul-wicks-of-patientslikeme/**.

43. PatientOpinion. Patient Opinion: Patient Opinion Limited; n.d. Available from: **https://www.patientopinion.org.uk/**.

44. Mental Health Network NHS Confederation. Patient Opinion - A case study Mental Health Network NHS Confederation; n.d. Available from: **http://www.nhsconfed.org/Documents/MHN_Case_study2.pdf**.

45. Department of Industry. Heating, ventilation and air-conditioning (HVAC): Commonwealth of Australia; n.d. Available from: **http://ee.ret.gov.au/energy-efficiency/non-residential-buildings/heating-ventilation-and-air-conditioning-hvac**.

46. Council of Australian Governments (COAG). National Strategy on Energy Efficiency Australia: Commonwealth of Australia; 2009.

47. Olimpiew E. APPS rEVOLUTION: Computer Sciences Corporation; 2013. Available from: **www.csc.com/appsrevolution**.

48. Niyato D, Lu Xiao, Ping Wang. Machine-to-Machine Communications for Home Energy Management System in Smart Grid. IEEE Communications Magazine. 2011 April 2011.

49. Harper-Slaboszewicz P, McGregor T, Sunderhauf S. Customer View of Smart Grid - Set andForget? Smart Grid - Integrating Renewable, Distributed & Efficient Energy. 2012.

50. Australian Energy Market Operator (AEMO). Rooftop PV Information Paper – National Electricity Forecasting (2012). Australia: 2012.

51. Liu X, O'Rear EG, Tyner WE, Pekny JF. Purchasing vs. leasing: A benefit-cost analysis of residential solar PV panel use in California. Renewable Energy. 2014;66:770-4.

52. Kinghorn R, Kua D. Forecast Uptake and Economic Evaluation of Electric Vehicles in Victoria. 2011.

53. NSW Government – Environment and Heritage (OEH). Plug-in vehicles: NSW Government - OEH; 2012. Available from: **http://www.environment.nsw.gov.au/cleancars/**.

54. Office of the Mayor – City and County of San Francisco. San Francisco Hits Milestone for Electric Vehicle Charging Stations: City and County of San Francisco; 2012. Available from: **http://sfmayor.org/index.aspx?page=740**.

55. Frost & Sullivan. 360-degree perspective of the Global Electric Vehicle Market-2012 Edition. Frost & Sullivan, 2012.

56. Joskow PL. Creating a smarter US electricity grid. The Journal of Economic Perspectives. 2012;26(1):29-47.

57. Department of State Development, Business and Innovation (DSDBI) Victoria. Smart meter safety: State Government of Victoria; n.d. Available from: **http://www.smartmeters.vic.gov.au/safety**.

58. Jemena Limited. Smart Meters – FAQs, Related Links & Documents: Jemena Limited; n.d. Available from: **http://jemena.com.au/customer/electricity/smart-meters/faq/**.

59. Borwein J, Bailey DH. Smart meters are about as dangerous as ...: The Conversation Media Group; 2012. Available from: **https://theconversation.com/smart-meters-are-about-as-dangerous-as-9413**.

60. Department of State Development, Business and Innovation (DSDBI) Victoria. Smart Meters eUpdate - Issue 2: State Government of Victoria; n.d. Available from: **http://www.smartmeters.vic.gov.au/News/smart-meter-eupdates/eupdate-issue-2**.

61. Bertot C, Jaeger PT, Grimes JM. Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. Government Information Quarterly. 2010;27(3):264-71.

62. World Economic Forum (WEF). Global Risks 2013 – Eighth Edition. 2013.

63. Magid L. What Are SOPA and PIPA And Why All The Fuss? Forbes: Forbes.com LLC; 2012. Available from: **http://www.forbes.com/sites/larrymagid/2012/01/18/what-are-sopa-and-pipa-and-why-all-the-fuss/**.

64. Wortham J. Public Outcry Over Antipiracy Bills Began as Grass-Roots Grumbling: The New York Times Company; 2012. Available from: **http://www.nytimes.com/2012/01/20/technology/public-outcry-over-antipiracy-bills-began-as-grass-roots-grumbling.html?pagewanted=1&ref=technology&_r=1&**.

65. Weisman J. After an Online Firestorm, Congress Shelves Antipiracy Bills: The New York Times Company; 2012. Available from: **http://www.nytimes.com/2012/01/21/technology/senate-postpones-piracy-vote.html**.

66. Wortham J. A Political Coming of Age for the Tech Industry: The New York Times Company; 2012. Available from: **http://www.nytimes.com/2012/01/18/technology/web-wide-protest-over-two-antipiracy-bills.html?scp=11&sq=SOPA&st=cse**.

67. Varyani R. Evolving Technology and its Effect on Healthcare. Frost & Sullivan, 2009.

68. Romeo S. The Evolution of Mobile Health. Frost & Sullivan, 2012.

69. Gulati N. Analysis of Healthcare Cloud in APAC. Frost & Sullivan, 2013.

70. Frost & Sullivan. Global Point-of-Care Testing (POCT) Market – Increasing Adoption of POCT in Emerging Countries will Provide Impetus to Market Growth. 2013.

71. Koninklijke Philips N.V. Experience the future of wearable technology - Philips Healthcare: Koninklijke Philips N.V.; n.d. Available from: **http://www.healthcare.philips.com/main/about/future-of-healthcare/index-video.wpd**.

72. Gary BH, Bowden T, Johansen I, Koch S. Electronic health records: an international perspective on" meaningful use". Issue Brief (commonwealth fund). 2011;28:1-18.

73. da Silva V, McGregor T, Rayman R, Luke PP. Telementoring and Telesurgery: Future or Fiction? Robot Surgery (InTech). 2010.

74. Anvari M, McKinley C, Stein H. Establishment of the world's first telerobotic remote surgical service: for provision of advanced laparoscopic surgery in a rural community. Annals of surgery. 2005;241(3):460.

75. Hood L, Flores M. A personal view on systems medicine and the emergence of proactive P4 medicine: predictive, preventive, personalized and participatory. New biotechnology. 2012;29(6):613-24.

76. The White House, Office of Communications. White House to Highlight Open Science "Champions of Change": U.S. Government; 2013. Available from: **http://www.whitehouse.gov/sites/default/files/microsites/ostp/openscience_release_6-18-13.pdf**.

77. Ustun TS, Ozansoy C, Zayegh A. Recent developments in microgrids and example cases around the world - A review. Renewable and Sustainable Energy Reviews. 2011;15(8):4030-41.

78. U.S Department of Energy (U.S DOE). Grid Energy Storage. U.S DOE; 2013.

79. Department of Primary Industries. Fact Sheet – Smart Meters Australia: The State of Victoria; 2010.

80. Frost & Sullivan. Data-Driven Utilities – Business Intelligence and Analytics to become the Top Investment Area for Energy Companies. 2013.

81. SAS Institute Inc. Analytics leads to wiser energy use: SAS Institute Inc. ; n.d. Available from: **http://www.sas.com/en_us/customers/oklahoma-gas-and-electric.html**.

82. Farhangi H. The path of the smart grid. Power and Energy Magazine, IEEE. 2010;8(1):18-28.

83. Varaiya PP, Wu FF, Bialek JW. Smart Operation of Smart Grid: Risk-Limiting Dispatch. Proceedings of the IEEE. 2011;99(1):40-57.

84. Australian Energy Market Operator (AEMO). Integrating Renewable Energy – Wind Integration Studies Report. Australia: 2013.

85. Sanders H, Kristov H, Rothleder MA. The Smart Grid Vision and Roadmap for California (Chapter 6). Smart grid: integrating renewable, distributed & efficient energy: Academic Press, 2011 0123864534.

86. Massachusetts Institute of Technology (MIT). The Future of the Electric Grid - An Interdisciplinary MIT Study: MIT; 2011. Available from: **http://mitei.mit.edu/system/files/Electric_Grid_Full_Report.pdf**.

87. Market Research Media. U.S. Federal Cloud Computing Market Forecast 2013-2018: Market Research Media; n.d. Available from: **http://www.marketresearchmedia.com/?p=145**.

88. Kundra V. Federal Cloud Computing Strategy: U.S. Government; 2011. Available from: **https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf**.

89. Cabinet Office. Government adopts 'Cloud First' policy for public sector IT: UK Government; 2013 [updated 5 May 2013]. Available from: **https://www.gov.uk/government/news/government-adopts-cloud-first-policy-for-public-sector-it**.

90. Department of Finance. Australian Government Cloud Computing Policy: Commonwealth of Australia; n.d. Available from: **http://www.finance.gov.au/cloud/**.

91. Department of Finance and Deregulation. The Australian Public Service Big Data Strategy – Improved understanding through enhanced data-analytics capability: Australian Government Information Management Office (AGIMO); 2013. Available from: **http://www.finance.gov.au/sites/default/files/Big%20Data%20Strategy.pdf**.

92. Australian Department of Immigration and Citizenship. 2012-13 - Annual Report Australia: Commonwealth of Australia; 2013.

93. Australian Signals Directorate. Risk Management of Enterprise Mobility Including Bring Your Own Device Commonwealth of Australia; 2013. Available from: **http://www.asd.gov.au/publications/csocprotect/Enterprise_Mobility_BYOD.pdf**.

94. Department of Finance and Deregulation. Australian Public Service Mobile Roadmap Adopting mobile technology across government Commonwealth of Australia; 2013. Available from: **http://www.finance.gov.au/files/2013/06/APS-Mobile-Roadmap.pdf**.

95. Department of Broadband, Communications and the Digital Economy. Advancing Australia as a Digital Economy: An Update to the National Digital Economy Strategy. Australia: 2013.

96. Department of Economic and Social Affairs. United Nations e-Government Survey 2008: From e-Government to Connected Governance 2008.

97. Department of Human Services. Service Delivery Reform: Transforming government service delivery: Commonwealth of Australia; 2011. Available from: **http://www.humanservices.gov.au/spw/corporate/about-us/resources/service-delivery-reform-overview.pdf**.

98. IBM. What is big data? : IBM; n.d. Available from: **http://www-01.ibm.com/software/au/data/bigdata/**.

99. Computer Sciences Corporation (CSC). Big Data Universe Beginning to Explode: CSC; n.d. Available from: **http://www.csc.com/insights/flxwd/78931-big_data_growth_just_beginning_to_explode**.

100. Ng SY, Lim, M. K., et al. GeoSpace for Singapore's Whole-of-Government Data Sharing: Singapore Land Authority; 2011. Available from: **http://proceedings.esri.com/library/userconf/proc11/papers/3323_50.pdf**.

101. Australian College of Rural and Remote Medicine. Telehealth turns 750,000 square kms into a 'local' oncology practice. Available from: **https://www.acrrm.org.au/files/uploads/pdf/news/Release_TeleHealth%20cancer%20practice-ACRRM-6.pdf**.

102. UK Department of Health. Whole System Demonstrator Programme (Headline Findings – December 2011): Crown copyright; 2011. Available from: **https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/215264/dh_131689.pdf**.

103. CSIRO. Smarter, safer homes Australia: CSIRO; n.d. Available from: **http://www.csiro.au/Organisation-Structure/Divisions/Computational-Informatics/Smarter-safer-homes.aspx**.

104. Jemena. Jemena Electricity Outlook Portal – A new service to help make your life easy: Jemena; n.d. Available from: **http://jemena.com.au/customer/electricity/smart-meters/portal/**.

105. CSIRO. Intelligent Grid - A value proposition for distributed energy in Australia. Australia: 2009.

106. Department of State Development Business and Innovation (DSDBI) Victoria. Energy and Earth Resources – Premium Feed-in Tariff: State Government of Victoria; n.d. Available from: **http://www.energyandresources.vic.gov.au/energy/environment-and-community/victorian-feed-in-tariff-schemes/closed-schemes/premium-feed-in-tariff**.

107. Department of Finance. Declaration of Open Government: Commonwealth of Australia; n.d. Available from: **http://www.finance.gov.au/e-government/strategy-and-governance/gov2/declaration-of-open-government.html**.

108. iStrategyLabs. Apps for Democracy Innovation Content: iStrategyLabs; n.d. Available from: **http://istrategylabs.com/work/apps-for-democracy-contest/**.

109. CSIRO. Vizie provides social media monitoring to identify customer needs: CSIRO; 2013. Available from: **http://www.csiro.au/Outcomes/ICT-and-Services/Social-media-monitoring.aspx**.

110. Frost & Sullivan. The Coming Data Deluge: The Advent of Big Data for Communications Service Providers. 2013.

111. Cisco Systems, Inc. The Zettabyte Era—Trends and Analysis: Cisco Systems, Inc.; 2013. Available from: **http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.pdf**.

112. Australian Bureau of Statistics (ABS). Volume of Data Downloaded – Internet Activity, Australia, June 2013, cat. no. 8153.0: ABS; 2013.

113. Australian Bureau of Statistics (ABS). Internet Activity, Australia, June 2011, cat. no. 8153.0: ABS; 2011.

114. Australian Bureau of Statistics (ABS). Mobile Handset Subscribers - Internet Activity, Australia, June 2013, cat. no. 8153.0: ABS; 2013. Available from: **http://www.abs.gov.au/ausstats/abs@.nsf/Products/8153.0~June+2013~Chapter~Mobile+handset+subscribers?OpenDocument**.

115. Durbin S. Information security without boundaries. Network Security. 2011;2011(2):4-8.

116. Cisco Systems, Inc. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013–2018: Cisco Systems, Inc.; 2014. Available from: **http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf**.

117. Frost & Sullivan. US Machine-to-Machine (M2M) Communications Markets (NC5E-65). 2013.

118. Frost & Sullivan. Asia Pacific M2M Market Outlook. 2011.

119. Jackson TW, Farzaneh P. Theory-based model of factors affecting information overload. International Journal of Information Management. 2012;32(6):523-32.

120. De Filippi P, McCarthy S. Cloud Computing: Centralization and Data Sovereignty. European Journal for Law and Technology. 2012;3(2).

121. Stratecast., Sullivan. F. Implementing a Big Data System? Infrastructure Readiness is Key 2013.

122. Sakr S, Liu A, Batista DM, Alomari M. A survey of large scale data management approaches in cloud environments. Communications Surveys & Tutorials, IEEE. 2011;13(3):311-36.

123. Amazon Web Services, Inc. AWS Case Study: NASA/JPL's Desert Research and Training Studies: Amazon Web Services,, Inc; n.d. Available from: **http://aws.amazon.com/solutions/case-studies/nasa-jpl/**.

124. Georgia Tech Information Security Center and Georgia Tech Research Institute. Emerging Cyber Threats Report 2013: Georgia Institute of Technology; 2012. Available from: **http://www.gtcybersecuritysummit.com/pdf/2013ThreatsReport.pdf**.

125. Choo K-KR. The cyber threat landscape: Challenges and future research directions. Computers & Security. 2011;30(8):719-31.

126. U.S. Department of Homeland Security (DHS). Privacy Impact Assessment for the Initiative Three Exercise: DHS; 2010. Available from: **http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3exercise.pdf**.

127. Oxford Dictionary. cyberthreat: Oxford University Press; n.d. Available from: **http://www.oxforddictionaries.com/definition/english/cyberthreat**.

128. National Cyber Security Centre (NCSC). Cyber Security Assessment Netherlands (CSAN-3). Ministry of Security and Justice, 2013.

129. Casey T. Threat Agent Library Helps Identify Information Security Risks: Intel Corporation; 2007. Available from: **https://communities.intel.com/servlet/JiveServlet/previewBody/1151-102-1-1111/Threat%20Agent%20Library_07-2202w.pdf**.

130. Sophos Ltd. Security Threat Report 2014 - Smarter, Shadier, Stealthier Malware: Sophos Ltd; 2013. Available from: **https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf**.

131. Johnson M. Cybercrime: Threats and Solutions: The Ark Group; 2013. Available from: **http://www.ark-group.com/Downloads/Cybercrime-Threats-and-Solutions-Sample1.pdf**.

132. Cisco Systems, Inc. Cisco 2014 Annual Security Report: Cisco Systems, Inc.; 2014. Available from: **https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf**.

133. Open Web Application Security Project (OWASP). Category:Threat Agent: OWASP; n.d. Available from: **https://www.owasp.org/index.php/Category:Threat_Agent**.

134. Industrial Control System Cyber Emergency Response Team (ICS-CERT). Cyber Threat Source Descriptions ICS-CERT: U.S Department of Homeland Security. Available from: **https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions**.

135. Withers P. Information Security Threat Vectors: ISACA; 2011. Available from: **http://www.isaca.org/chapters5/Virginia/Events/Documents/Past%20Pres%202011-03%20Threat%20Vectors.pdf**.

136. Barnum S. Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression: The MITRE Corporation 2013. Available from: **https://stix.mitre.org/about/documents/STIX_Whitepaper_v1.0.pdf**.

137. Burmester M, Magkos E, Chrissikopoulos V. Modeling security in cyber–physical systems. International Journal of Critical Infrastructure Protection. 2012;5(3-4):118-26.

138. Bertino E. Digital Identity Management Techniques and Policies: Purdue University; n.d. Available from: **http://www.itu.int/dms_pub/itu-t/oth/06/04/T06040040040001PDFE.pdf**.

139. Evans DL, Bond PJ, Bement ALJ. Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology (NIST) Special Publication. 2002;800(30).

140. Wikipedia. Vulnerability (computing): Wikimedia Foundation, Inc.; n.d. Available from: **http://en.wikipedia.org/wiki/Vulnerability_(computing)**.

141. Perrin C. The CIA Triad TechRepublic: CBS Interactive. ; 2008. Available from: **http://www.techrepublic.com/blog/it-security/the-cia-triad/488/**.

142. Guttman B, Roback EA. An introduction to computer security: the NIST handbook: National Institute of Standards and Technology (NIST) Special Publication; 1995.

143. Wilkinson A, Kupers R. Living in the Futures. Harvard Business Review. 2013.

144. Cornelius P, Van de Putte A, Romani M. Three Decades of Scenario Planning in Shell. Harvard Business Review. 2005.

145. Chopra A, Kundra V, Weiser P. A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future. Executive Office of the President - National Science and Technology Council, 2011.

146. World Economic Forum (WEF), Accenture. Accelerating Smart Grid Investments: WEF in partnership with Accenture; 2009. Available from: **http://www3.weforum.org/docs/WEF_SmartGrid_Investments_Report_2009.pdf**.

147. Abrams M, Weiss J. Malicious Control System Cyber Security Attack Case Study: Maroochy Water Services, Australia: The MITRE Corporation and Applied Control Solutions; 2008. Available from: **http://www.mitre.org/sites/default/files/pdf/08_1145.pdf**.

148. Stouffer K, Falco J, Scarfone K. Guide to industrial control systems (ICS) security. National Institute of Standards and Technology (NIST) Special Publication. 2011;800(82).

149. Slay J, Miller M. Lessons learned from the maroochy water breach. Critical Infrastructure Protection: Springer US; 2008.

150. Nicholson A, Webber S, Dyer S, Patel T, Janicke H. SCADA security in the light of cyber-warfare. Computers & Security. 2012;31(4):418-36.

151. Australian Broadcasting Corporation (ABC). Heatwave blamed for large spike in the number of deaths in Victoria last week: ABC; 2014. Available from: **http://www.abc.net.au/news/2014-01-23/heatwave-death-toll-expected-to-top-almost-400/5214496**.

152. The Age Company Ltd. Mass power outages hit state: The Age Company Ltd.; 2007. Available from: **http://www.theage.com.au/news/national/mass-power-outages-hit-state/2007/01/16/1168709751760.html**.

153. Australian Broadcasting Corporation (ABC). Cyclone Yasi n.d. Available from: **http://www.abc.net.au/news/specials/yasi/**.

154. Cashell B, Jackson WD, Jickling M, Webel B. The economic impact of cyber-attacks United States Congress: Congressional Research Service, Library of Congress; 2004. Available from: **http://www.fas.org/sgp/crs/misc/RL32331.pdf**.

155. Professional Services Review. Professional Services Review - Annual Report 2012-13: Commonwealth of Australia; 2013. Available from: **http://www.psr.gov.au/images/annualreports/psr_annual_report_201213.pdf**.

156. Chemist sentenced for medicine fraud. Dominion Post. 2009.

157. ACT Auditor-General's Office. Performance Audit Report – Emergency Department Performance Information (Report No. 6 / 2012) 2012. Available from: **http://www.audit.act.gov.au/auditreports/reports2012/Report%20No.%206%20Emergency_Department_Performance_Information.pdf**.

158. U.S. Food and Drug Administration (FDA). FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks: FDA; 2013. Available from: **http://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm356423.htm**.

159. Redspin, Inc. Breach Report 2013: Protected Health Information (PHI): Redspin, Inc; 2014. Available from: **http://www.redspin.com/docs/Redspin-2013-Breach-Report-Protected-Health-Information-PHI.pdf**.

160. Morris L. Combating fraud in health care: an essential component of any cost containment strategy. Health Affairs. 2009;28(5):1351-6.

161. Brooks G, Button M, Gee J. The scale of health-care fraud: A global evaluation. Security Journal. 2012;25(1):76-87.

162. World Health Organization (WHO). Prevention not cure in tackling health-care fraud. Bulletin of the World Health Organization. 2011;89(12): 853-928.

163. Federal Bureau of Investigation (FBI). Financial Crimes Report to the Public (Fiscal Years 2010-2011): U.S. Department of Justice; 2011. Available from: **http://www.fbi.gov/stats-services/publications/financial-crimes-report-2010-2011/financial-crimes-report-2010-2011#Health**.

164. O'Neill M. Ransomware targeting businesses, home PCs: Australian Broadcasting Corporation (ABC); 2012. Available from: **http://www.abc.net.au/news/2012-10-25/ransomware-targeting-aussie-businesses2c-pcs/4332526**.

165. Krebs B. Hackers Break Into Virginia Health Professions Database, Demand Ransom: The Washington Post; 2009. Available from: **http://voices.washingtonpost.com/securityfix/2009/05/hackers_break_into_virginia_he.html**.

166. Rindfleisch TC. Privacy, information technology, and health care. Communications of the ACM. 1997;40(8):92-100.

167. Appari A, Johnson ME. Information security and privacy in healthcare: current state of research. International journal of Internet and enterprise management. 2010;6(4):279-314.

168. Canadian Security Intelligence Services. Public Report 2010-2011: Public Works and Government Services Canada; 2012. Available from: **https://www.csis-scrs.gc.ca/pblctns/nnlrprt/2010-2011/2010-2011PublicReport_English.pdf**.

169. Austen I. Canada Hit by Cyberattack The New York Times: The New York Times Company; 2011. Available from: **http://www.nytimes.com/2011/02/18/world/americas/18canada.html?ref=technology&_r=1&**.

170. Cowan P. Big holes discovered in Vic Govt's cyber security IT news: nextmedia Pty Ltd; 2013. Available from: **http://www.itnews.com.au/News/365679,big-holes-discovered-in-vic-govts-cyber-security.aspx**.

171. Hardy K. Operation Titstorm: Hacktivism or Cyberterrorism. UNSW Law Journal. 2010;33(2):474-502.

172. Foo F. Indonesians step up cyber attacks against Australia The Australian: News Corp Australia; 2013. Available from: http://www.theaustralian.com.au/national-affairs/policy/indonesians-step-up-cyber-attacks-against-australia/story-fn59nm2j-1226758538363#.

173. Laughland O, Farrell P, Wolf A. Immigration Department data lapse reveals asylum seekers' personal details The Guardian: Guardian News and Media Limited; 2014. Available from: **http://www.theguardian.com/world/2014/feb/19/asylum-seekers-identities-revealed-in-immigration-department-data-lapse**.

174. British Broadcasting Corporation (BBC). Internet mistake reveals UK nuclear submarine secrets: BBC; 2011. Available from: **http://www.bbc.co.uk/news/uk-13107413**.

175. Bryan-Low C. U.K. Office Details Accidental Loss of Data. The Wall Street Journal: Dow Jones & Company, Inc. ; 2013. Available from: **http://online.wsj.com/news/articles/SB10001424127887323977304579003073111313500**.

176. The White House, Office of Management and Budget. Impacts and Costs of the October 2013 Federal Government Shutdown. U.S. Government; 2013.

177. Kallberg J, Thuraisingham B. Towards Cyber Operations The New Role of Academic Cyber Security Research and Education. Proceedings from the 2012 IEEE International Conference on Intelligence and Security Informatics (ISI 2012); 2012.

**CONTACT US**
**t** 1300 363 400
+61 3 9545 2176
**e** enquiries@csiro.au
**w** www.csiro.au

**YOUR CSIRO**
At CSIRO we shape the future. We do this by using science to solve real issues. Our research makes a difference to industry, people and the planet.

As Australia's national science agency we've been pushing the edge of what's possible for over 85 years. Today we have close to 6,500 talented people working out of 58 centres in Australia and internationally. Our people work closely with industry and communities to leave a lasting legacy. Collectively, our innovation and excellence places us in the top ten applied research agencies in the world.

We ask, we seek, we solve. We are CSIRO.

**FOR FURTHER INFORMATION**
James Deverell, CSIRO Futures
**t** +61 2 9490 8456
**e** james.deverell@csiro.au

Prof. Y. Jay Guo
Digital Productivity and Services Flagship, CSIRO
**t** +61 2 9372 4291
**e** jay.guo@csiro.au