gap
A Vision for Australia

PROTECTING THE NEW FRONTIER REPORT

GAP TASKFORCE
ON CYBER SECURITY

NOVEMBER 2017

DISCLAIMER

This document summarises the deliberations of the GAP Taskforce on Cyber Security - a cross-jurisdictional, multidisciplinary group of stakeholders brought together in 2016 by the institute for active policy Global Access Partners (GAP) in association with the National Consultative Committee on Security and Risk (NCCSR). The Taskforce was chaired by Alastair Milroy AM and co-funded by GAP with the financial support of Splunk, DXC Technology, FireEye and Herbert Smith Freehills (HSF).

The report reflects the diverse range of views and interests expressed by the individuals involved, and it should not be assumed that every member would agree with every point in full.

The report has been prepared in good faith from the information available at the time of writing and sources believed to be reliable. However, evaluation of the material remains the reader's sole responsibility and it should not be used as a substitute for independent professional advice.

Global Access Partners Pty Ltd

ACN 000 731 420
ABN 74 000 731 420

Postal address PO Box 978 Strawberry Hills NSW 2010 Australia
Telephone +61 2 8303 2420
Facsimile +61 2 9319 5754
Email info@globalaccesspartners.org

TERMS AND ABBREVIATIONS

ACIC	Australian Criminal Intelligence Commission
ACORN	Australian Cybercrime Online Reporting Network
ACSC	Australian Cyber Security Centre
ACSGN	Australian Cyber Security Growth Network
AFP	Australian Federal Police
AISA	Australian Information Security Association
ANU	Australian National University
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
ASPI	Australian Strategic Policy Institute
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
COAG	Council of Australian Governments
DDoS	Distributed Denial of Service
EU	European Union
GAP	Global Access Partners
GDPR	EU General Data Protection Regulation
HSF	Herbert Smith Freehills
IEC	International Electrotechnical Commission
IT	Information technology
ICT	Information and communication technologies
IoT	Internet of Things
ISO	International Organization for Standardization
NBN	National Broadband Network
NCCSR	National Consultative Committee on Security and Risk
NIST	National Institute of Standards and Technology, USA
NSW	New South Wales
SQL	Structured Query Language
STEM	Science, technology, engineering and mathematics
TAFE	Technical and Further Education
UK	United Kingdom
UNSW	University of New South Wales
US	United States
VoIP	Voice Over Internet Protocol

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The World Economic Forum warns[1] that cyber attacks are the third most serious threat to Australian economic security, after high energy prices and an asset price collapse. Cyber attacks top the list of risks for the Pacific region as a whole and are assessed as the eighth most serious issue facing the world. A succession of serious incidents hit the headlines in 2017, increasing pressure on firms and government agencies to take more effective action to safeguard consumer privacy and national security. Large companies suffered or revealed major data breaches, ransomware claimed thousands of victims, and state-sponsored espionage intensified.

The Australian Government has acknowledged the threat and launched a comprehensive new $230 million Cyber Security Strategy in 2016[2]. An International Cyber Engagement Strategy[3], released in October 2017, also stressed the importance of international cooperation to improve cyber security and combat cybercrime. However, continuing incidents, from the loss of F35 Lightning data at a poorly protected Adelaide firm[4] to growing concerns over vulnerable Internet of Things (IoT) devices[5], highlight the pervasiveness of cyber attacks and the need for intensified awareness and action.

The latest *Threats* Report[6] by the Australian Cyber Security Centre (ACSC) notes a sharp increase in the targeting of smaller businesses. Reported losses from business email compromises alone totalled over $20 million – an increase of 230% over the previous year – and an 11% surge in attacks on 'non-traditional' sectors underlines the importance of the issue for all Australian firms.

The following document by the GAP Taskforce on Cyber Security summarises the views of industry and business experts on issues of concern and offers suggestions for improvements for government, industry and the community. A number of themes emerged from Taskforce discussions, including the need for additional research into the scope and extent of cybercrime in Australia, enhanced corporate awareness, improved training for cyber security professionals, and standardised accreditation. Appropriate industry protocols must also be developed and enforced for the host of IoT devices entering the marketplace.

The Taskforce advocated a proactive, holistic, end-to-end approach to cyber security, with better cross-sectoral collaboration and clarified objectives in both the public and private sphere. Its recommendations should complement current government policy by strengthening the research base, encouraging business awareness, enforcing industry standards, upgrading skills and improving accreditation for cyber security specialists. Australian cyber security practice should become an economic asset, creating a global commercial advantage for domestic firms, as well as assuring allies and customers that their data is safe in Australian hands.

Taskforce Findings and Recommendations

A new home affairs portfolio or a strengthened role for the Attorney-General could be created to assume responsibility for all cyber security activities to drive a more authoritative and integrated strategic approach. Cyber threats respect no borders, and greater international cooperation and stronger partnerships must be pursued to tackle cybercrime as well as better threat protection.

The Taskforce stressed action in five key areas to support existing policy, address emerging challenges and close gaps in future provision.

1. Research

A stronger research base would help Australian policy makers and commercial stakeholders understand the growing scope of cyber threats and install effective counter-measures. The Commonwealth should therefore consider the establishment of an Independent Research Authority to improve and coordinate research and quantify the nature, scale and impact of cybercrime in Australia.

A university-based research project could be commissioned for around $100,000, leading to the establishment of a permanent university-based research team with an annual budget of $3 million to study the deeper interaction of technology and human behaviour, monitor international research, analyse future needs for cyber security skills, and support wider policy development.

Steps to understand the ‘human factor’ are required to successfully align abstract cyber security frameworks with actual human activity, as criminals can access apparently impermeable systems through social engineering, or exploit the neglect of standard procedures.

New models of accelerated research, such as joint venture centres between universities and business, should also be explored, as well as capacity to translate findings into practical outcomes and escalate serious issues when detected.

Research efforts must be informed by better reporting of cybercrime incidents. Questions on cyber issues should be incorporated into ongoing monthly and quarterly business surveys, such as Roy Morgan’s, to generate more comprehensive figures. All Australian firms and government agencies should be encouraged to complete the annual ACSC survey.

In addition to reactive research on current threats, proactive research into future issues and making the internet inherently more secure is required. 'Security by design' is required across the whole internet and for all electronic devices, rather than just IoT devices. The entire system must become more resilient and robust, rather than holes being plugged and patched when they are discovered. While current issues must be dealt with, stakeholders should look ahead to strengthen the system as a whole over time.

2. Awareness

A 'technology first' approach will always leave firms and individuals struggling to meet new threats, and all Australian citizens must understand the need for personal vigilance to protect themselves from exploitation. Awareness should be fostered by awareness campaigns targeted at the community, small business and the corporate sector and greater publicity for existing initiatives such as Cyber Security Week.

Small and medium-sized enterprises could be invited to education seminars on cyber security, hosted annually in metropolitan and regional areas of each state, while cyber security starter kits should be given to start-ups in every sector.

The case for small and medium-sized enterprises must be easy to understand and implement, given their limited resources. Executives of larger firms must accept cyber security as a core management function and know enough to understand the scope of the threat, the consequences of intrusions and the need for investment in infrastructure and staff to safeguard their companies.

Smaller companies should embrace the Australian Signals Directorate's (ASD) 'Essential Eight'[7] mitigation strategies, while larger company boards and industry organisations should be familiar with the World Economic Forum's principles of cyber resilience[8]. Disaster and management plans must include cyber security, just as cyber security must be integrated with other aspects of a firm's risk mitigation. Preservation of data and chain of custody concepts for evidence preparation and criminal prosecution should be introduced into business practices to increase the understanding of law enforcement requirements and encourage early reporting and cooperative investigation strategies.

Firms should adopt a cyber-resilience model, encompassing education, technical capability and risk management which allows a rapid response to changing threats. However, if voluntary measures and awareness raising continues to prove ineffective, legislation for reporting, detection and deterrent activities should be further strengthened to ensure compliance with ISO/IEC 27000 standards.

Companies in vulnerable sectors, such as telecommunications, energy and defence, should be explicitly warned of state-sponsored intrusion from hostile nations. While these threats can be mitigated in part by strengthening agency partnerships and sharing information with allies, companies have a responsibility to protect themselves.

3. Standards and Protocols

While protocols for self-regulation could be negotiated with industry bodies and firms to meet the ISO/IEC 27000 standard, such voluntary schemes must be rigorously applied and maintained to ensure the protection of customer data and classified information. Whether standards are government or industry-led, firms must be tested to ensure they meet the standards of compliance they claim to maintain. Recent anti-terrorist measures could offer a model for cyber security self-regulation in business.

The use of risk-assessment questionnaires could be encouraged to allow firms to decide the appropriate level of cyber security required. Such self-diagnostic tools allow firms to assess the threats they face and the consequences of breaches to themselves, their partners and customers and society. This process should be based on international standards and supported by advice from supply chain partners and government agencies as required.

Industry-specific standards of skills, experience and training should be issued for responsible personnel to ensure competent IT management protects companies and agencies from risks. The frequency and standard of cyber security training for all staff could be evaluated in the course of such assessment, with more frequent and comprehensive training generating higher scores.

Just as mandatory data breach legislation[9] for larger firms proved necessary, given chronic under-reporting of events, similar provisions for smaller companies might also be required to improve standards.

Higher standards for acceptable cyber defence measures should be incorporated into public tenders and larger firms, and those in vulnerable sectors should be required to conduct regular cyber threat assessments and establish in-house cyber security incident response teams[10] for incident detection and response.

Cyber risk assessment in small and medium-sized enterprises may be thought of as ‘cyber auditing’. Such audits could be carried out for insurance and compliance purposes, akin to financial auditing. Capacity must be viewed holistically, with the auditing of both technology and human interaction in a business to inform the adoption of preventative measures.

Many firms and agencies rely on legacy infrastructure which is increasingly insecure. Although it is difficult to discuss the need for company-wide cyber resilience with government executives and company boards, it is still important to build resilience into legacy applications and infrastructure. Resilience allows disaster recovery and business continuity after issues occur.

Help for small and medium-sized businesses to implement cyber security protocols is as important as education about their content and use. Smaller firms can feel overwhelmed by the task and need advice and assistance which they can afford. They are paralysed by a surfeit of information, but do not know who to turn to for practical implementation advice.

If efforts to encourage 'security by design'[11] in IoT devices fail to bear fruit, proposed consumer security ratings[12] should be buttressed by legislation to enforce the use of ISO/IEC 27000 standards.

Cryptography plays a vital role in securing networks, devices and communications and should be considered at the start of developing devices, software or systems.

4. Education and Skills

All stakeholders and Australian citizens would benefit from better cyber education, in addition to wider provision for IT professionals. The broad concepts which secure businesses apply equally well to private individuals, and well-structured, coordinated public information campaigns, similar to those for driver safety or against smoking, could be funded at the state or federal level.

Children at school should be taught about cyber security issues as they use IT in the classroom and participate online from a young age. Family-friendly versions of business security courses could be offered online, and a common curriculum for cyber security courses could be developed for schools.

Better coordination of public information campaigns on cyber security will help raise community awareness of resources such as *Stay Smart Online* and *Security, Influence and Trust*.

Companies should be encouraged to offer internal cyber training and mentoring for employees and fund external courses for selected personnel. Public/private scholarships could foster a new generation of cyber security professionals. A Digital University offering online courses could be established to improve ICT skills in a cost-effective and practical manner, while the internationalisation of training content could be encouraged through partnerships abroad.

Executives and managers also need education on cyber issues. The problem for many firms is not a shortage of services to suit their needs and budgets, but the difficulty of choosing between them. The new state-based Cyber Security Centres could be asked to reach out and educate the private sector in their regions.

Older people are also at risk, as their digital skills may stagnate after they leave the workforce. Cyber security awareness for retiring ‘baby boomers’ is as important as training for young people and employees to ensure networks are not penetrated and identities remain uncompromised.

5. Accreditation

The introduction of improved licensing and registration for technology personnel should improve security and performance. A rigorous accreditation process for cyber security courses would reassure students and companies of their utility.

Accreditation for non-specialist personnel, including managers and frontline staff, could use international frameworks which are already widely utilised to offer a common framework for comparison.

Accreditation for cloud providers, which firms increasingly rely upon for cyber security as they put more of their operations into the cloud, could reassure stakeholders while giving small and medium-sized businesses greater security *en masse* then they could provide themselves.

INTRODUCTION AND CONTEXT

The GAP Taskforce on Cyber Security

In July 2015, the ACSC – Australia's top security agency – released its inaugural unclassified *Threats* report[13] and revealed, for the first time, the scale of the cyber threat. It highlighted the vulnerability of Australian businesses to persistent and escalating criminal activity and state-sponsored espionage against government, defence and other critical interests. The document called for private-public sector partnerships to improve awareness and defensive measures, while identifying several sectors which had failed to invest and risked financial loss, damage, damage to their reputation, theft of intellectual property, and disruption to trade as a result. While energy, banking and finance, communications, defence and transport were the sectors under greatest risk of attack, the ACSC report emphasised that all Australian firms, whatever their size or area of business, must take adequate precautions to protect themselves and their customers.

The threat has only grown in scale and complexity since then. Indeed, in 2016 the Australian Security Intelligence Organisation (ASIO) warned of *"growing hostile cyber activity"* from terrorists and hostile states and a widening *gap "between the scale and scope of harm experienced to Australia's sovereignty, government systems, and commercial and intellectual property, and the ability of ASIO and partner agencies to successfully mitigate that harm".*[14] Attacks have multiplied over the last twelve months, with 47,000 reported this year, an increase of 15%. Many attacks are not reported to the police, although they constitute a crime, which complicates the development of defences. Attack vectors include business emails and insecure IoT devices, demonstrating that current self-regulation is insufficient. Cyber criminals have used social media to impersonate CEOs to claim six-figure invoices from their firms.

Acknowledging the vital importance of cyber security to Australia's commercial and national interests, Global Access Partners, in association with the NCCSR, assembled a multidisciplinary group of experts and executives in July 2016 to form a taskforce on Cyber Security. Supported and co-funded by GAP and industry partners DXC Technology, Splunk, FireEye and HSF, the Taskforce discussed practical steps to counter cybercrime and espionage and improve collective awareness.

Chaired by Alastair Milroy AM, former Chief Executive Officer of the Australian Crime Commission, the Taskforce and associated subgroups met between July 2016 and October 2017 to develop their proposals. Members attended in a personal capacity, and their contributions were noted under the Chatham House rule of non-attribution to encourage frank debate. This report outlines key discussion points but, given their diversity, it should not be assumed that all members agree with all recommendations.

Policy Responses

The Turnbull administration has made cyber security a high priority issue, but the previous Labor government also released a strategy in 2013 to combat attempts by cyber criminals to steal money, data and identities.

The National Plan to Combat Cybercrime[15] by the Attorney-General's Department (AGD) admitted that *"combating cybercrime requires more than just an enforcement response"* and highlighted prevention, mitigation and education as *"important aspects"* of defence. It underlined that *"combating cybercrime is a shared responsibility - between individuals, industry and governments"* and that *"no one can combat this threat alone"*. The plan sought to entrench these ideas *"in a framework that will unify efforts across jurisdictions and form a key plank of the Government's broader digital agenda"*. It committed states and the Commonwealth to ensure that responsible agencies *"have the capabilities and capacity they need to detect, disrupt, investigate and prosecute cybercrime and manage digital evidence"*. A National Cybercrime Working Group was also asked to encourage the inclusion of cybercrime and digital evidence in police training, supported by nationally consistent training and education resources. Law enforcement agencies were asked to access expertise from the private and tertiary sectors through secondments where appropriate.

The continuing calls for similar measures today suggests the implementation of these ideas remains to be completed. The National Plan to Combat Cybercrime was criticised for not being fit for purpose at its inception, and those claims have only grown over time.

Malcolm Turnbull's National Innovation and Science Agenda was presented as the key to modernising Australia to meet the economic and technological challenges of the 21st century. It included the creation of a $22 million Cyber Security Growth Centre[16] to protect the online environment on which innovation and modern economic activity depends. However, the innovation theme did not resonate with the electorate at the subsequent general election, and the $230 million Cyber Security Strategy[17] released in April 2016 was accordingly presented as a plank of national defence.

Although most cyber attacks are criminal, rather than state-sponsored, most governments see cyber security as part of national defence, rather than the protection of individual, social, and economic assets or a means to safeguard innovation. The 2016 Cyber Security Strategy outlined plans for Academic Centres for Cyber Security Excellence, an expansion of CERT Australia, the creation of a CERT information sharing portal and an AGD Critical Infrastructure Centre, and strategies to improve national cyber security awareness. A special adviser in the Department of the Prime Minister and Cabinet was appointed, while a Cyber Ambassador now leads the country's cyber efforts overseas.

The Strategy outlined five 'themes of action' until 2020 – a national cyber partnership, stronger cyber defence, global responsibility and influence, growth and innovation, and the creation of 'cyber smart' nation. Over 100 cyber security experts were hired across government agencies, including 50 serving as officers in the two main crime-fighting agencies. The Australian Federal Police (AFP) were also awarded a further $20.4 million and the Australian Crime Commission $16 million to conduct threat detection, technical analysis and forensic assessment over the next four years.

December 2016 saw the announcement of the Australian Cyber Security Growth Network (ACSGN), an industry-led non-profit organisation responsible for delivering the activities of the Cyber Security Growth Centre. The ACSGN will help businesses and researchers develop the next generation of products and services required to *"live and work securely in our increasingly connected world"*. Operating across the nation, it hopes to reduce often criticised fragmentation of cyber security activities and unite capability and expertise throughout Australia.

Government Cyber Security Agencies

Although a plethora of public agencies have a role to play, the AGD is the most prominent player in the fight against cybercrime. It handles Commonwealth criminal law policy, as well as identity and protective security, privacy, critical infrastructure resilience and telecommunications interceptions. The Secretary of AGD also chairs the National Cybercrime Working Group, which includes representatives from Commonwealth, State and Territory police and justice agencies. The Department also bolsters the capacity of partner countries in the Pacific region and beyond and makes and receives formal requests for evidence in cross-border investigations.

AGD is also responsible for CERT Australia, which offers an initial point of contact for industry to report cyber security incidents. It also offers information to individuals and businesses on ways to protect their systems and data from cyber threats.

Australia's federal system complicates these administrative responsibilities, as State and Territory agencies have primary responsibility for cybercrime targeting individuals, businesses and government systems in their jurisdictions, while Commonwealth agencies are responsible for cybercrime directed at critical infrastructure, national IT interests and federal systems.

The National Cybercrime Working Group includes representatives from State, Territory and Commonwealth law enforcement and justice agencies to align their efforts, but a range of other agencies are also involved, including consumer protection agencies and offices of fair trading reacting to online scams. Responsibility for combatting data theft, online harassment and fraud is split between federal and state attorney-general's departments, the ACSC and AFP, state police, courts, directors of public prosecutions (DPP), the Department of Defence, Australian Secret Intelligence Service (ASIS) and private contractors.

National security and intelligence agencies tackle state sponsored attacks to government networks and cooperate through the multi-agency Cyber Security Operations Centre in the Department of Defence. However, the picture is complex, as issues of cyber warfare, espionage and counter terrorism are covered by a range of defence white papers, ASIO strategic plans and counter terrorism reviews and are the subject of attention by the Department of Defence, ASD, ASIS, Department of Foreign Affairs and Trade, Office of National Assessments, Defence Intelligence Organisation, the nation's courts and state attorney-general's departments, as well as private contractors.

Responsibility for protecting critical national systems, outlined in the National Critical Infrastructure Plan of 2015 and the 2016 Defence White Paper, rests with the Attorney General, ASD, AFP, state attorneys general, police, courts, DPP, Defence, ASIO, ASIS and private contractors. Individual privacy is safeguarded by the Australian Information Commissioner, Human Rights Commission and federal and state attorneys general, although other government agencies seek access to otherwise private data in pursuit of criminal investigations.

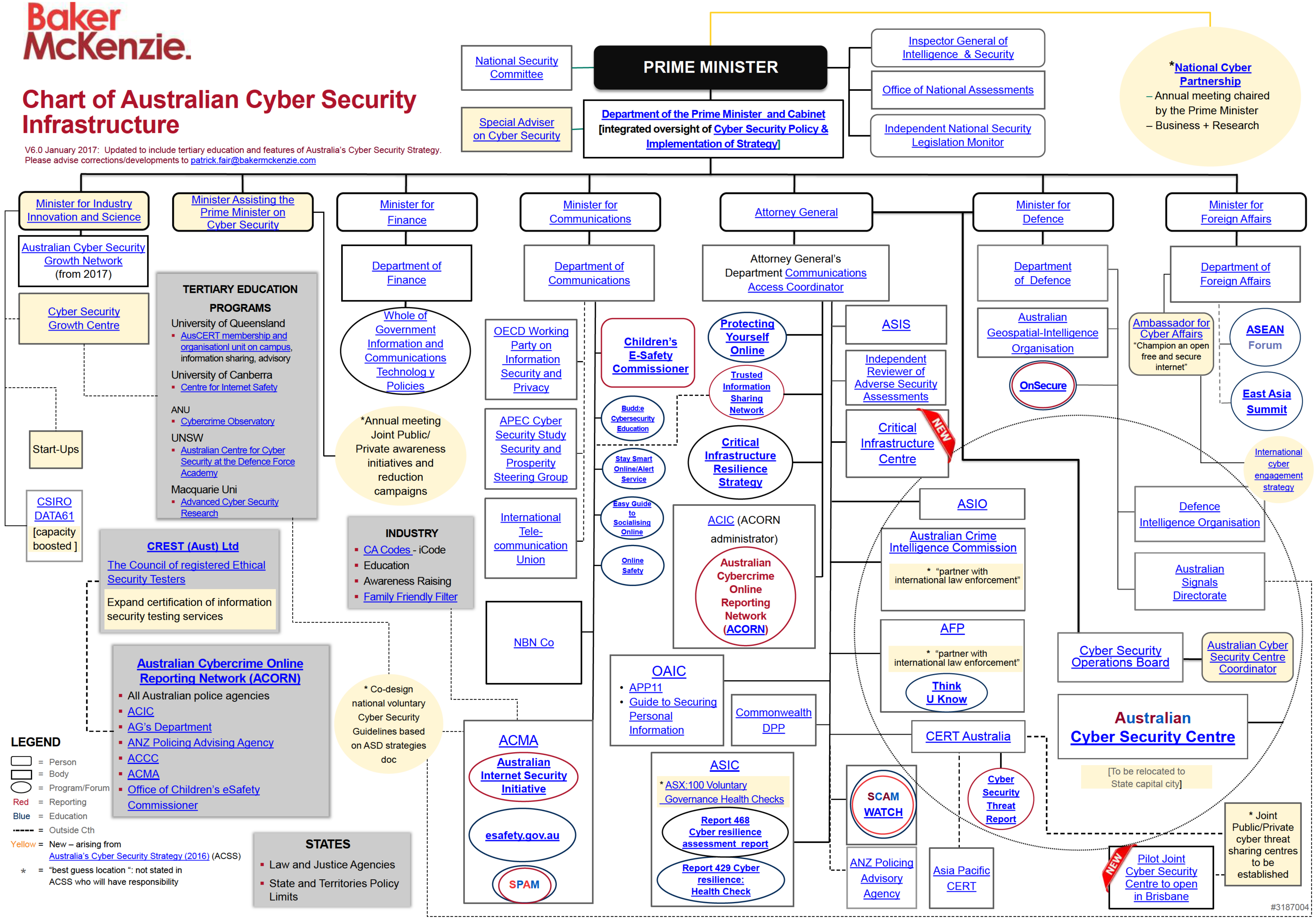
The Australian Criminal Intelligence Commission (ACIC) produced threat assessments for the National Plan to Combat Cybercrime, and its National Cybercrime Intelligence Assessment has now merged with ASD's National Cyber Threat Assessment to form the ACSC National Strategic Cyber Threat Assessment.

It is little wonder that lines of responsibility remain blurred or opaque, and any cracks will be exploited by the world's cyber criminals and hostile state actors *(see next page for Baker and McKenzie's Chart of Australian Cyber Security Infrastructure as of January 2017).*

Baker McKenzie.

Chart of Australian Cyber Security Infrastructure

V6.0 January 2017: Updated to include tertiary education and features of Australia's Cyber Security Strategy.
Please advise corrections/developments to patrick.fair@bakermckenzie.com



PRIME MINISTER

National Security Committee

Special Adviser on Cyber Security

Department of the Prime Minister and Cabinet [integrated oversight of Cyber Security Policy & Implementation of Strategy]

Inspector General of Intelligence & Security

Office of National Assessments

Independent National Security Legislation Monitor

*National Cyber Partnership
– Annual meeting chaired by the Prime Minister
– Business + Research

Minister for Industry Innovation and Science

Australian Cyber Security Growth Network (from 2017)

Cyber Security Growth Centre

Start-Ups

CSIRO DATA61 [capacity boosted]

Minister Assisting the Prime Minister on Cyber Security

TERTIARY EDUCATION PROGRAMS

University of Queensland
- AusCERT membership and organisationl unit on campus, information sharing, advisory

University of Canberra
- Centre for Internet Safety

ANU
- Cybercrime Observatory

UNSW
- Australian Centre for Cyber Security at the Defence Force Academy

Macquarie Uni
- Advanced Cyber Security Research

CREST (Aust) Ltd

The Council of registered Ethical Security Testers

Expand certification of information security testing services

Australian Cybercrime Online Reporting Network (ACORN)
- All Australian police agencies
- ACIC
- AG's Department
- ANZ Policing Advising Agency
- ACCC
- ACMA
- Office of Children's eSafety Commissioner

LEGEND
▭ = Person
▭ = Body
⬭ = Program/Forum
Red = Reporting
Blue = Education
------ = Outside Cth
Yellow = New – arising from Australia's Cyber Security Strategy (2016) (ACSS)
* = "best guess location ": not stated in ACSS who will have responsibility

STATES
- Law and Justice Agencies
- State and Territories Policy Limits

Minister for Finance

Department of Finance

Whole of Government Information and Communications Technolog y Policies

*Annual meeting Joint Public/ Private awareness initiatives and reduction campaigns

INDUSTRY
- CA Codes - iCode
- Education
- Awareness Raising
- Family Friendly Filter

* Co-design national voluntary Cyber Security Guidelines based on ASD strategies doc

Minister for Communications

Department of Communications

OECD Working Party on Information Security and Privacy

APEC Cyber Security Study Security and Prosperity Steering Group

International Tele-communication Union

NBN Co

ACMA

Australian Internet Security Initiative

esafety.gov.au

SPAM

Children's E-Safety Commissioner

Budd:e Cybersecurity Education

Stay Smart Online/Alert Service

Easy Guide to Socialising Online

Online Safety

Attorney General

Attorney General's Department Communications Access Coordinator

Protecting Yourself Online

Trusted Information Sharing Network

Critical Infrastructure Resilience Strategy

ACIC (ACORN administrator)

Australian Cybercrime Online Reporting Network (ACORN)

OAIC
- APP11
- Guide to Securing Personal Information

Commonwealth DPP

ASIC

* ASX:100 Voluntary Governance Health Checks

Report 468 Cyber resilience assessment report

Report 429 Cyber resilience: Health Check

ASIS

Independent Reviewer of Adverse Security Assessments

Critical Infrastructure Centre

NEW

ASIO

Australian Crime Intelligence Commission

* "partner with international law enforcement"

AFP

* "partner with international law enforcement"

Think U Know

CERT Australia

SCAM WATCH

ANZ Policing Advisory Agency

Asia Pacific CERT

Cyber Security Threat Report

Minister for Defence

Department of Defence

Australian Geospatial-Intelligence Organisation

OnSecure

Defence Intelligence Organisation

Australian Signals Directorate

Cyber Security Operations Board

Australian Cyber Security Centre Coordinator

Australian Cyber Security Centre

[To be relocated to State capital city]

* Joint Public/Private cyber threat sharing centres to be established

NEW

Pilot Joint Cyber Security Centre to open in Brisbane

Minister for Foreign Affairs

Department of Foreign Affairs

Ambassador for Cyber Affairs "Champion an open free and secure internet"

ASEAN Forum

East Asia Summit

International cyber engagement strategy

#3187004

DEFINING CYBERCRIME

Even the definition of cybercrime and cyber security can be contested, confusing or opaque. The ACSC[18] defines a cyber attack as a deliberate act to disrupt, deny, degrade or destroy computers or networks, or the information they hold, to compromise national security or economic prosperity. Such cyber attacks can be launched by vandals for their own amusement, but are more commonly the work of criminals seeking financial gain through fraud, identity theft or blackmail, or hostile foreign governments.

The International Telecommunications Union[19] sees cyber security as a collection of tools, policies, safeguards, training, practices and technologies protecting an organisation and its assets, rather than any single activity.

The USA's National Initiative for Cybersecurity Education[20] also stresses the breadth of the task and the shared responsibility of many different stakeholders, including computer network operators, law enforcement bodies and diplomatic, military and intelligence missions. It views cyber security as the process by which all information systems and the data they hold are protected against damage or exploitation[21], including national strategy and policy, standards to reduce threats and vulnerabilities, international cooperation to reduce attacks and procedures to improve incident response and resilience.

As the scope of cybercrime increases, its definition continues to evolve and measuring its true impact becomes more complicated, making research methodology more error-prone. New types of cyber attack could even create the need for additional categories of crime, which are not covered by current legislation.

If cybercrime is seen as criminal activities carried out using computers or the internet, then cybercrime could include the use of computers to assist with 'traditional' crimes or offences, as well as crimes perpetrated entirely through technology. The Council of Europe Convention on Cybercrime, which Australia signed in 2013[22], defined it as offences against the confidentiality, integrity and availability of computer data and systems, but the scope of the problem has long since broken these bounds.

While various law enforcement, government, business and academic bodies collect data on cybercrime around the world, their figures can be based on different assumptions and use widely varying methodologies. Businesses will suppress or under-report incidents to avoid negative publicity, while IT security companies unleash a string of dire warnings to drum up customers. Many criminal cyber attacks affecting Australia originate in countries lacking the ability or will to monitor or tackle their perpetrators – indeed, their authorities may perpetrate attacks of their own or use willing proxies.

Ambiguity over the law can affect even domestic law enforcement. Cyber attacks may breach long-established laws of theft, fraud or criminal damage, but some clearly damaging activities, such as the Russian-backed efforts to spread 'false news' during western election campaigns, may not fall foul of existing legislation. Law-makers must continuously analyse novel cyber activities to ensure their effective criminalisation, although the difficulty of identifying, apprehending and prosecuting cybercriminals in foreign jurisdictions remains. Laws will always lag behind technology and its inevitable abuses, and this delay will only grow as the pace of change increases. Legal ambiguities can also hinder services and measures designed to protect against cyber attack. The security industry is subject to stringent state laws, but their inconsistencies leave many firms contravening particular measures.

The harm caused by cybercrime extends far beyond the financial loss of fraud or blackmail, but damage to reputation, for example, is not easy to objectively assess.

Estimates of the cost and extent of criminally motivated cybercrime are incomplete and vary wildly, with Prime Minister Turnbull himself citing estimates between $1 billion and $17 billion in April 2016. Whatever its actual extent, cybercriminals are unlikely to be brought to justice, and given their safe havens abroad, there is limited scope for the Australian police to pursue prosecutions.

Common Cyber Threats

While there are innumerable variations on each theme, most criminal attacks on computer systems fall into a number of familiar categories[23].

Spear Phishing sees malicious links or file attachments hidden in emails which can compromise networks when opened. Attackers target industry personnel to access corporate networks, and social media offers more than enough data to identify suitable victims. Ransomware software encrypts data on victims' computers and demands a fee, often paid in bitcoin, for its release. Secondary targeting sees attackers penetrate poorly defended targets, which enjoy a trusted relationship with higher value organisations they can then exploit.

Keystroke Logging is carried out by surreptitious software which records and relays every keyboard entry, betraying passwords or sensitive information.

SQL Injection involves the addition of SQL code to a web form input box for malign purposes. An SQL query is a request for an action to be undertaken on a database and attackers can use the input boxes to silently request all the information it contains or interact with it in illicit ways.

Bug Poaching occurs when attackers penetrate a network to reap private information and assess vulnerabilities. They will then exploit that data with further attacks, or attempt to extort money for not doing.

Distributed Denial of Service (DDoS) attacks crash targeted websites by massing a multitude of compromised systems to bombard it with requests for information and can offer a smokescreen for other attacks.

Cross-Site Scripting can compromise web applications which accept input, but do not separate data and executable code before it is delivered back to a user's browser. It allows an attacker to load malicious script on a webpage, which can infect the computer of anyone who visits it through their web browser.

ISSUES AND OPPORTUNITIES

Despite the efforts of by successive Australian governments to combat both criminal and state-sponsored cyber attacks, the unabated incidence of major cyber incidents, and the plethora of attacks which never merit a headline of their own, proves that still more must be done by all stakeholders and citizens.

The Turnbull Government's Cyber Security Strategy was launched in response to 'unprecedented' levels of state-sponsored attacks, rather than the growing level of criminal activity. The Prime Minister termed cyber security the 'new frontier' of warfare, espionage and threats to Australian families, governments and businesses in January 2017[24], after revelations of Russian interference in the US Presidential election. He stressed that "*awareness is the most important first step*", as "*you can pretend the threats are not there, if you like, but that will only make you susceptible to being taken in by them".*

In October 2016, ABC News had revealed that Austrade and the Department of Defence's elite research division, the Defence Science and Technology Group, had been infiltrated by Chinese-based hackers, while a foreign power also managed to install malicious software on the Australian Bureau of Meteorology's computer system to steal sensitive documents and perhaps compromise other government departments[25].

While it might be hoped the fruits of the Government's $230 million cyber security investment would render Taskforce discussions moot, the October 2017 *Threats* report[26] by the ACSC underlines the need for even greater attention and action. Far from being blunted by the measures already announced, the threat posed by cyber criminals and foreign actors continues to grow. The subsequent revelations of woeful security precautions by the Adelaide aerospace firm which lost F35 fighter information shows the need for companies to protect themselves, as well as more rigorous government oversight.

These problems are not confined to Australia. The cyber threat respects no international borders, and 2017 has seen another spate of incidents, despite significant efforts to forestall them. The online services company Cloudflare, which protects 6 million customer websites and organisations against DDoS attacks, was itself hacked[27], exposing packets of user data which could, theoretically, have been accessed by search engines. This highlighted the danger of relying on large infrastructure services which can themselves be compromised. In the same month, the mysterious Shadow Brokers group released a set of spying tools which exploited vulnerabilities in commercial software, and the following month the WannaCry ransomware, which UK officials believe to have been a North Korean attempt to raise revenue and disrupt western nations[28], temporarily crippled National Health System hospitals and infected thousands of computer systems around the world. The ransomware exploited a Windows vulnerability exposed by the Shadow Brokers group in 2016 which had been patched by Microsoft in March, but which many organisations and users had neglected to apply. The incident underlined the need for software to be patched promptly to fix known vulnerabilities and prompted calls for baseline compliance in the public and private sector.

While the replacement of legacy software, such as Windows XP, with modern alternatives is clearly desirable, some older equipment may be incompatible with replacement operating systems. The panic caused by such incidents can be as damaging as the attacks themselves, but many individuals and firms still neglect the most basic computing procedures, such as keeping software up to date. Smaller firms, not subject to compliance requirements demanded of larger firms, may lack the know-how and resources of their larger brethren and prioritise day-to-day survival over apparently obscure issues such as cyber security, but their vulnerability imperils the rest of the community in turn.

Lessons might be borrowed from the broad acceptance of occupational health and safety regulations. Small businesses are not allowed to forego their safety responsibilities by pleading pressures of cost or time and should be held to similar basic standards in their cyber security. Amalgamating the needs of small and medium-sized enterprises might allow the market to offer cheaper services to protect them as a group. While insurers are taking advantage of the chance to offer cyber insurance policies, compensation cannot restore the harm caused to a company, and insurers offer little in the way of threat advice, although their terms and conditions may encourage better cyber provisions.

A more advanced set of ransomware based on known Windows exploits, known as Petya, emerged in March 2016, infecting companies in the USA, Denmark and other nations. It was attributed to Russia as a cyber strike against Ukrainian utilities, transport systems and banks, timed to coincide a holiday celebrating Ukraine's independent constitution[29]. Kaspersky, a Russian firm which produces popular anti-virus products, was also implicated recently in Russian state attacks on the USA, leading to the software being removed from American government departments[30].

Even the largest tech firms can be compromised and fail to take appropriate action to safeguard the community. In October 2017, it was revealed[31] that hackers who infected a website used by software developers in 2013 then stole data from Microsoft's internal bug-tracking database. Unpatched vulnerabilities were then used by the 'Butterfly' hacking group to attack 50 law firms, investment companies, bitcoin sites and IT providers in 20 countries, including some billion-dollar corporations[32]. Microsoft did not disclose the seriousness of the breach at the time, and has still not admitted its scope – indeed, officials at the US Department of Homeland Security and the Pentagon only learned of the incident when Reuters informed them, having been tipped off by five current and former Microsoft employees.

The hackers also penetrated Facebook, Twitter and Apple by the same measure. October also saw Google ban eight Minecraft: Pocket Edition skins from its Google Play store after discovering they linked devices to a botnet which could launch DDoS attacks – but only after they had been downloaded up to 2.6 million times[33].

Although a 2016 *Cyber Maturity* report[34] by the Australian Strategic Policy Institute (ASPI) ranked Australia fourth out of 23 Asia-Pacific nations in terms of cyber protection, enforcement and cross-sectoral engagement, the Government's ambitious programmes have been criticised for inadequate implementation. Attendees at the 2017 *Safeguarding Australia* Summit[35] criticised a perceived lack of engagement from the Attorney-General's Department, noting that both industry and government call for collaboration, but expect the other to take the lead. Australia's Joint Cyber Security Centres may improve the situation, but are still to make their mark. Speaking at the Summit, an American law enforcement official noted that time limits on the release of information from official sources reduce its relevance and value, prompting most organisations to use private sector expertise.

In May 2017, over a year after the launch of the Government's Cyber Security Strategy, ASPI criticised the tardiness of efforts to protect public service networks[36], calculating that only four of the Strategy's 83 outcomes had been achieved. ASPI, a think tank partly funded by the Department of Defence, pressed the government to offer more details on its cyber security campaign, communicate more effectively with the commercial sector, improve partnerships with international allies, offer clear procurement guidelines and commit more funding to reforms. It called for a dedicated Minister of Cyber Security to take responsibility and warned that *"the absence of timelines leaves the government room to mask underperformance, and means that promises to 'accelerate' or deliver initiatives 'ahead of schedule' hold very little meaning"*. ASPI observed that the "*failure to provide a timeline has opened the government up to criticism, since stakeholders are left with nothing but their own expectation against which to judge the pace of activity*" and that stakeholders worried that "*the speed of tangible on-the-ground delivery isn't yet commensurate with the importance of the issue or reflective of the government's narrative of urgency".*

The Government's Special Advisor on Cyber Security Alistair MacGibbon also worried a 'tick box' mentality in the public service meant compliance procedures might be followed in theory rather than practice[37]. Over the last two years, a number of government agencies have had the resilience of their infrastructure tested and were warned that a lack of proper security may leave them vulnerable to cyber attacks and expose a wealth of highly personal data.

While the government's plans to create Academic Centres for Cyber Security Excellence to produce work-ready graduates, conduct research and maintain an information sharing portal to help small and medium-sized enterprises are commendable, the need for accelerated action to back good intentions is clear.

Problems can often be opportunities in disguise, and Industry Minister Arthur Sinodinos has framed the growing cyber threat as a major opportunity for Australia to improve its capability and export cyber defence services around the world[38]. Lloyds of London estimates that cybercrime costs the world about USD$400 billion a year, and the global cyber security market is expected to grow from about AU$100 billion in 2015 to more than AU$200 billion by 2020[39]. Australia can also leverage its membership of the Five Eyes intelligence community, alongside the USA, Canada, the UK and New Zealand, to offer new security strategies as well as share intelligence and resources. However, despite the government's acceptance of the need for greater cyber security measures, and the action it has taken so far, more clearly needs to be done.

The backbone of Australia's connectivity, the National Broadband Network (NBN), should not escape scrutiny. The ideas about technology which informed the design of the NBN several years ago have moved on, and the system has already proved inadequate to cater for new use patterns and developments. However, it must be remembered that the NBN being rolled out today is not the system which was initially proposed. While main lines have high-capacity fibre-optic cables, they are still linked to businesses and homes with slow copper wire. Furthermore, internet providers in some areas deliver a poor service because they did not book enough bandwidth from the system, rather than because the network itself is flawed. Resilience and adaptability should have been designed into the system, but the need to work inside a budget has capped its capability to meet future needs.

AREAS FOR ACTION

The Taskforce considered a range of measures which the government could intensify or adopt to improve Australian cyber security. Efforts to integrate public and private sector efforts must continue to create a comprehensive national architecture for cooperation between state and federal government, businesses, academia, law enforcement, defence agencies and international partners. However, the communication and integration required continues to be hampered by sectional interests and a reluctance to divulge information on sensitive issues.

While acknowledging the significant efforts already underway, the Taskforce stressed five specific areas requiring redoubled activity - research, awareness, standards, skills, and accreditation.

Research

Cyber security is a risk management issue for both public and private organisations, but that risk cannot be managed, unless its dimensions are properly understood. Organisations only respond to problems which are clearly articulated, and cyber precautions are hampered by a lack of granular detail on the threat. More fundamentally, policy makers fail to appreciate the interaction between digital technology and human behaviour, meaning theoretical precautions can fail everyday use. No system, however 'smart', is impregnable when neglected or used carelessly and attacked constantly by determined and imaginative assailants.

The National Cybercrime Working Group called for national statistics on cybercrime in 2010; however, comprehensive figures on offences and prosecutions have never been released. Despite the creation of the Australian Cybercrime Online Reporting Network (ACORN), a voluntary reporting system, and the annual high-level threat report, the lack of robust and freely available data increases the lag between threat manifestation and effective response. Unspecific warnings can struggle for acceptance in companies which do not see a business case for action, whether they operate in a highly regulated sector or not. A lack of granular detail on the scale and frequency of attacks suffered by ordinary individuals and firms gives free reign to both scaremongering hyperbole and corporate complacency in the absence of objective facts.

Individuals and businesses remain reluctant to reveal their vulnerability to cyber attack, a reticence which finally forced the federal government to insist on mandatory data breach notification after years of industry inaction. The ACSC Cyber Security Survey received just 113 responses from 68 private sector firms and 45 government agencies in 2016[40], a response the ACSC generously termed 'modest'.

The Taskforce urged more firms and agencies to complete ACSC's annual survey, if requested to do so to offer a more complete picture of the true situation, as headlines, anecdotes and hearsay are no substitute for verifiable information. The true situation may even be less dangerous than some commentators – and security vendors – suggest. Dire warnings that poor identity management would doom online banking proved incorrect, for example, but it is more likely that incidents against individuals and smaller firms remain under-reported. Adding cyber security questions to general business surveys, such as Roy Morgan's monthly polling of thousands of Australian companies[41], could help chart trends over time.

In addition to the annual ACSC Threats report, AusCERT produces an annual conference report, while the ASD reports on Commonwealth government incidents and analysts, such as Deloitte, produce their own reports. However, these reports lack the detail required on the incidence and economic and human costs of cyber attacks, the success rate of different policies or the conviction of cyber criminals. Cybercrime threat assessment is the responsibility of the ACIC and is produced at various classifications for various audiences, but the lack of contributions from the business community means they offer less guidance than they should to frame evidence-based policy.

Despite the importance of the issue, there are no full-time researchers of cybercrime issues in any Australian university. The Cambridge Computer Crime Database in the UK was developed by an Australian criminologist who emigrated when funding of the Australian Institute of Criminology was cut in 2013. Leading Australian researchers, such as Broadhurst and Grabowsky at the Australian National University, do study related issues, but do not focus on Australian cybercrime policy and measurement.

The lack of meaningful Australian cybercrime statistics in the public domain was demonstrated by the government's inability to specify its costs within a range of $1 billion to $17 billion, when the Cyber Security Strategy was released in April 2016. This uncertain data reduces public pressure for improvement, reduces the priority afforded by law enforcement agencies and company boards, and invites suspicion that government policy is motivated by grandstanding as much as reality.

The establishment of an Independent Research Authority to quantify the scope, extent and impact of cybercrime in Australia could offer a more credible and consistent research base. It could publish its findings freely, to complement the classified threat assessments produced by the ACIC for the government. As well as monitoring current trends to encourage appropriate defensive measures, it could inform planning to improve cyber security skills, anticipate incipient problems and improve understanding of the impact of technology on human behaviour, a task well beyond the ACIC purview. As a first step, research could be commissioned from the university sector at a modest cost of perhaps $100,000, with a permanent university-based research capability on cybercrime then established, costing $3 million per year. The research centre could include an obligation for its academic staff to engage in teaching and professional development, allowing it to be partially self-funding. The federal government could avoid the cumbersome procedures of the Australian Research Council by setting up a COAG funding mechanism, with each state providing a fraction of the total depending on its population size. Private sector funding could also be sought from major corporations to reduce the cost to all stakeholders, offering them access to valuable resources at a fraction of the cost of funding them independently.

New models of accelerated research, such as joint venture centres between universities and business, should also be explored, as well as capacity to translate findings into practical outcomes and escalate serious issues when detected.

Corporate and Public Awareness

Several Taskforce members criticised a lack of interest in cyber security issues in companies of every size and sector. One independent survey found that only a third of company boards have a 'clearly defined risk appetite for cyber'[42]. Firms focused on their bottom line can see information security as a short-term cost, rather than a long-term asset, and risk management is complicated by their inability to relate agency threat assessments to effective measures to mitigate them.

Cyber security is a highly volatile environment with high degrees of uncertainty, and so legacy tools for traditional risk management derived from actuarial science have limited utility.

Corporate Security

Research outlined to Taskforce members by DXC Technology paints a damning picture of corporate cybercrime. Companies take a median time of 146 days to detect a data breach, and a further 46 days to respond. Over half these breaches are reported by a third party, rather than detected by the company itself. The assumption that major firms have strong security operations is all too often misplaced. While budgets and staff may be dedicated to the task, they may not be effective, and smaller firms may have no security budget or staff at all.

Companies still tend to focus on their 'front end', rather than their 'back end', to ensure security. When compromised, they may seek legal advice on ways to limit the fall-out, before taking proactive steps to help affected customers or revise internal policies. Firms in heavily regulated sectors are accustomed to complying with tight regulations and may hesitate in the absence of detailed mandatory preventative measures to enter a 'bottomless pit' of cyber security costs.

While boards and executives will naturally cede technical responsibility to their IT specialists, they cannot abrogate themselves from the consequences of inadequate provision. Audit and risk committees may assure compliance with the law, but regulation always lags behind risk. The breadth of the subject means a holistic, end-to-end approach is required, involving every process and employee which uses or depends upon computing. Cyber breaches may provoke class action suits when poor procedures are revealed, increasing the urgency of corporate reform.

Larger firms can also encourage better practice from supply chains. While they may expect vendors and suppliers comply with acceptable standards, they can be compromised themselves through secondary targeting, if procurement-wide cyber security policies are not in place.

The Taskforce suggested that a series of small seminars, organised by the Attorney-General's Department or other agencies and designed to share information on particular issues or sectors, could engage small and medium-sized enterprises or larger companies. While broad but underfunded information schemes, such as a Cyber Awareness Week, are of limited utility, more focused sessions could have a greater effect.

Industrial sectors in the USA have also created their own information sharing groups, and Australian firms could follow their example. Major banks must maintain stringent security to retain consumer trust and can offer pointers which others could follow. They focus on informed risk management, rather than minimal compliance, to protect their vast data stores, and 10 minutes of every Westpac board meeting is dedicated to cyber security reports. The bank uses its position as a lead customer to ensure suppliers maintain their own security and collaborates with other financial firms and law enforcement bodies to manage threats. It also supports research at the Internet Commerce Security Laboratory at Federation University Australia into customer views and responses to identity theft.

Cyber attacks are escalating in scale, scope and sophistication, and companies can struggle to hire and retain suitably qualified security staff. However, while many firms now outsource computing activities or use cloud services, they cannot outsource responsibility for risk. While phones, email, the web and IoT are all vectors of attack, trusted third party services can also be compromised.

Firms have a responsibility to the rest of society, as well as their customers, shareholders and employees, to improve their cyber security. Beyond individual organisations, cyber risk is a systemic challenge and cyber resilience a public good. Every organisation acts as a steward of information they manage on behalf of others, and every organisation contributes to the resilience of not just their immediate customers, partners and suppliers, but also the overall shared digital environment.

A set of principles for boards developed by the World Economic Forum's Initiative on the Digital Economy[43] argues that cyber resilience is a leadership issue. Sound cyber defence is more a matter of long-term strategy and deep-seated culture than day-to-day tactics. Being cyber resilient requires those at the highest levels of a company, organisation or government to recognise the importance of avoiding and proactively mitigating risks and promoting cyber experts to influential positions in the hierarchy.

However, investment in sophisticated cyber security approaches, from advanced analytics and threat intelligence to insider threat programmes, will prove worthless if the most basic precautions are allowed to lapse in everyday operations. Any number of breaches proves that one chink in the armour can compromise an entire network, and so resilience requires a culture of security. While all stakeholders agree on the need for greater employee training and mentoring, the commitment of time and money involved will only be forthcoming, if executives recognise its importance to the company's future. The cost of such training could be reduced through online cyber security courses, produced by partnerships involving industry professionals and the tertiary sector.

The ability to recover from attacks should be remembered alongside the need to prevent them. Although it is difficult to discuss the need to invest in company-wide resilience with executives and company boards, steps can still be taken to improve the resilience of legacy applications and infrastructure. Resilience allows disaster recovery and business continuity after issues occur, and many government departments and agencies rely on legacy infrastructure which may date back as much as 30 years. Disaster and management plans must include cyber security, just as cyber security must be integrated with other aspects of a firm's risk strategy.

Although ongoing information sharing systems are being improved, the idea of a cyber alumni network to escalate a response to a major national cyber threat was floated at the *Cyber Security Leadership Imperative* event in May 2017[44]. Such a network would bring Australia's best and brightest digital security brains together as a 'surge capability' and help combat a national cyber emergency in the event of a major cyber security incident.

Developing a Voluntary Approach

Although many have failed to do so in the past, companies which address the five main themes of the ISO/IEC 27000 standards, or, at a more basic level, the ASD's 'Essential Eight'[45] can protect themselves from most attacks. Small and medium-sized enterprises may lack the skilled staff or resources to fully protect themselves, but Thales and the Centre for Defence Industry Capability are developing a model by which groups of smaller firms in vulnerable sectors could buy security capability together, supported by expertise from their prime contractors.

The business community does not want government legislation of cyber security beyond the realm of classified material. They would prefer a standards-based model, drawing on international best practice, as different enterprises have different vulnerabilities to targeted attacks. The compromised Adelaide defence contractor[46] had not followed the most basic of security precautions, and so testing of claimed security precautions must be introduced, but businesses would favour an audited self-regulated system, tested against ISO/IEC 27000 standards. Certification to this standard is already available, but remains expensive. The Adelaide firm had an obligation to protect sensitive material under the Defence Trade Control Act of Australia[47], and NIST will force Australian suppliers of controlled technology to certify to its standards from December 2017. The firm's lax security could incur severe penalties of up to a $1 million fine and repercussions under criminal law in the USA. It is therefore in all company's interests to ensure they are secured, whatever method is adopted to enforce it.

Cyber security has several strands and involves numerous actors. Different sectors and sizes of firms face different problems, albeit with common root problems of identity management, skills and education. Organisations must define their position, their issues and the actions they can take, and a range of granular solutions are required. Firms need effective guidance, and a risk assessment questionnaire could indicate the appropriate level of computer security, based on international standards and advice from supply chain partners and government agencies. Recent anti-terrorist measures could offer a model for cyber security self-regulation.

A risk assessment guide should not only offer a self-diagnostic tool to help a firm assess the threats it faces, but scope the consequences of breaches to itself, its partners, customers and the nation. The frequency of mandated cyber security training would be assessed, for example, with more frequent and thorough training generating higher scores. If the total score was less than required, help could then be sought from private services and public agencies. All firms would have a unique score, generated by their circumstances and their approach to meeting it, which would also help business partners assess their relationship with the firm, assuming such scores were made available. This approach would help firms adopt a cyber-resilience model encompassing education, technical capability and risk management which allows a rapid response to changing threats, rather than tick boxes to signal compliance to compulsory government schemes.

However, the argument that cyber security is about governance and risk and that compliance should depend on whether activities are being undertaken to protect the enterprise and stakeholders from harm should not obviate the need for those capabilities to be regularly tested and rigorously enforced. The lamentable safety record of firms both large and small suggests they cannot be left to their own devices.

Small and Medium-Sized Enterprises

Better guidance for small to medium-sized enterprises is required, as larger enterprises have the funds and resources to protect themselves, even if they sometimes fail to do so. Existing guidelines are too broad to help small and medium-sized enterprises design and implement practical protection measures. Smaller businesses in sectors such as healthcare, including general practitioners and medical centres, can amass huge stores of sensitive information, but have limited security safeguards. Such companies will not be forced to report data breaches under current legislation, reducing their incentive to take more effective defensive measures.

Effective advice for small and medium-sized enterprises should be tailored to their limited resources and skillsets and targeted at the most vulnerable sectors. Cyber security 'starter kits' could also be issued to start-ups and new businesses along with other official documentation, while established businesses need simple ways to measure the maturity and effectiveness of their provisions. There are no shortage of complicated standards and frameworks for IT specialists, but there are no yardsticks to help non-specialist CIOs or small businesses decide what level of security is appropriate to their situation. A benchmark based on anonymised data from similar firms could help them decide where they stand.

While standards and accreditation are important, implementation of cyber security is the major issue for small and medium-sized enterprises. Smaller firms can feel overwhelmed by the task and need advice and assistance which they can afford. They are paralysed by a surfeit of information, but do not know whom to turn to for practical implementation advice. Furthermore, a bewildering range of commercial security services are available, from penetration testing and red team attacks to audits against a range of standards. Such vendors offer every conceivable service required to secure a business against attack at a variety of prices to suit customer circumstances and resources. The difficulty lies in choosing from so many options, rather than a lack of services.

Cyber risk assessment in small and medium-sized enterprises could be thought of as 'cyber auditing', in a similar way to financial auditing, to make it less intimidating to smaller firms. There could be a new market auditing the cyber resilience of smaller firms for insurance and compliance purposes. A company's defensive capacity must be viewed holistically, with the auditing of both technology and human interaction, to guide preventative measures. Cyber-auditing capabilities should therefore be included in discussions of the need for awareness, training and skills, as companies cannot choose the right direction if they do not know where they stand.

Some small and medium-sized enterprises are putting all their computing on the cloud and rely on their service provider to secure it. The US is developing a system to accredit cloud providers, and a similar model is being looked at in Australia. Firms which offer threat assessments may need special arrangements to deal with multiple companies in a cloud environment, but these issues are certainly surmountable. Through indolence, ignorance or inability, many small and medium-sized businesses fail to patch their basic operating system, and so a cloud-based model for such firms could be more effective, if service companies were prepared to offer cover.

Whole-of-government models in other countries are following this approach, and models are being built to service cloud providers for small and medium-sized enterprises on the same platform. This allows these businesses to be grouped and share threat awareness. A repeatable model can be created for other providers and industries to use, including those in critical infrastructure such as energy, food distribution and transport.

Individuals and Personal Data

The government is supporting digital privacy by enforcing mandatory disclosure of data breaches by larger firms in the hope the glare of publicity will force corporates to secure themselves. Individuals are slowly realising the value of their personal data and further education, rather than legislation, will encourage people to protect themselves. The GDPR will force the issue internationally, as multinational firms will be forced to meet the high standards demanded by the European Union, and the Australian government is likely to rely on EU standards in this area.

Ownership of personal data will become an increasingly important issue, and may provoke more government involvement, as companies look to mine and monetise data ever more aggressively. While legal issues preclude information sharing between departments and may require legal review, the use of government data for commercial use could be equally contentious. Sydney's Opal travel cards, for example, generate a huge amount of valuable information on people's habits and activity and this information would be highly valuable if sold, even on an anonymised basis, to commercial companies, as it is in Hong Kong. Given that Opal cards are mandatory on a growing section of the transport network, the ability to opt out of data sharing – or perhaps a discount to allow individuals to share the benefits of the data they share – could be organised.

International Links

The global origins and scale of cyber criminality and espionage demands stronger international partnerships in response. Australia can learn from international best practice and encourage secondments as well as data sharing with its strategic allies and multinational firms. The internet allows small, determined groups to wield great power online, just as terrorists can threaten the rest of society, and democratic nations must stand united in defence of freedom as well as commercial activity.

International boundaries are almost meaningless in cyber space, affording criminals access to targets all over the world. A recent case study found one incident could be traced through three countries and five jurisdictions, creating a debate about who should take ownership of the issue. Law enforcement measures are still hampered by jurisdictional barriers; however, just as criminals could once cross state lines to escape pursuit by state police. Australian law enforcement must try to deal with global offenders based on crimes they commit in Australia, but apprehending the miscreants in other jurisdictions is almost impossible.

The traditional justice model based on national location is irrelevant in cybercrime, and so, in the short term at least, security against attack, rather than prosecuting offenders, is the most practical course.

While state-based groups will target particular firms or industries, criminals will probe thousands of firms for vulnerabilities, and if they cannot breach a particular one, will move on to find easier prey.

In the longer term, international cooperation will have to create a new cross-border justice model. Criminals often attack firms which themselves cross borders, creating a jurisdictional nightmare which will protect them from consequence even if they are identified. A new non-jurisdiction model is required, with Australia working with allied international agencies, to create a new paradigm.

Counter Measures

Recent reports reveal[48] that Australia has an offensive capability to disrupt cyber attackers targeting Australian national security. Australia's offensive programme has two tiers of capabilities, which either penetrate targets to passively collect of information, or pre-emptively disrupting their activities. While information collection is undertaken by law enforcement bodies and the intelligence community, second-tier disruption is usually the preserve of intelligence bodies and the Department of Defence.

Although it appears an attractive option, the unintended consequences of taking offensive action in cyberspace must not be forgotten. The apparent source of an attack, for example, may well be an innocent party who has been ‘spoofed’ through multiple levels to unknowingly launch proxy attacks. Australian policy therefore follows the sensible course of only attacking sites which pose the highest level of risk. However, given this conservative approach to active counter measures, some businesses are ‘hacking back’ to stop or prevent attacks on themselves.

Standards and Protocols

Cyber security is subject to a complex range of international law, federal and state legislation, voluntary codes of conduct, recommended best practice, and individual company policy. All facets of these must be improved, rather than voluntary measures necessarily being replaced by government legislation; however, most stringent measures may be required, if private actors continue to fail in their responsibilities. We should not accept continually plugging gaps in cyber security. A proactive campaign is required to raise the standards of all software and devices that connect to the internet to ensure security is designed in from the start, not patched up later.

Mandatory data breach disclosure was quietly passed by Parliament after nearly a decade of discussion[49], as companies consistently refused to notify affected customers of potentially ruinous data breaches or improve their security measures. From 22 February 2018, any Australian business generating $3 million or more in revenue and covered by the Privacy Act 1988 will have to disclose data breaches, which should encourage more stringent preventive measures. Similar legislation has already been passed in the USA and Europe, although Australia's legislation is less stringent than in the EU after concessions to industry pressure. Companies are still not obliged to inform law enforcement agencies, for example, after a data breach even though unauthorised access to information is a criminal act.

Just as there are material standards for consumer goods and commercial materials and processes to ensure public safety, so agreed protocols can be applied to improve cyber security. ISO/IEC 27000 standards are adopted in various forms around the world and offer a tool kit for companies to certify themselves, although the expense can deter Australian companies from using it. International discussions on further system standards is already underway, mirroring the Protective Security Policy Framework in Australia, and ISO 28000 standards on supply chain security can also be instructive.

However, there is always a balance to be struck between security and ease of use. Most individuals clearly prioritise ease of use over privacy in their use of social media and expect major platforms to ensure security on their behalf. Software is often released with known vulnerabilities, which are gradually patched in ways which would be illegal if applied to hardware. This transfers much of the cost of such flaws to businesses, governments and individuals, as they must protect themselves and cannot sue for loss, although no software can ever be entirely impervious to cyber attack.

Legislation for reporting, detection and deterrent activities already includes mandatory guidelines for reporting cyber security breaches. Enforcing the use of ISO/IEC 27000 standards, insisting on 'security by design' for new appliances and devices, and using the power of government procurement to enforce cyber security through the tender process could all encourage more effective defensive measures to become standard in vulnerable devices and businesses.

Some threats originate within organisations, rather than from outside, just as fraud and theft can be perpetrated by employees in more traditional ways. Although some firms have stringent screening processes, these can increase complacency, once individuals are admitted and given access to sensitive systems. Detecting internal malicious activities is a challenge, and while security vendors try to analyse behavioural anomalies to discover unauthorised activity, there are legal and privacy barriers to monitoring and investigating employees.

NIST Compliance

Industry always favours self-management, voluntary schemes and self-certification to more onerous government legislation; however, further measures will be required, if industry measures are not deemed sufficient. Even the United States has acknowledged that additional legislation is required to tackle the problem of business non-compliance with voluntary schemes[50], and constant attacks from Chinese and Russian hackers have spurred stringent measures to insist on high standards of security from domestic and foreign suppliers of software and technology. The US government requires foreign firms to meet the standards of the NIST Cybersecurity Framework[51], and firms such as Boeing are already asking their Australian suppliers to confirm they are NIST-compliant – although there is no framework for measurement.

Australian industry representatives would prefer an agreement with US authorities to allow self-certification of compliance to a voluntary scheme to suffice. A two-tier level of certification in the defence industry has been proposed, and discussions with the Attorney-General's Department and the Department of the Prime Minister and Cabinet on using ISO 31000 methodology to assess risk and required measures could be pursued. Although US companies will be required to ensure that international suppliers meet NIST standards by December 2017, senior British figures would also prefer a national scheme with equivalent provisions, and the Americans have expressed no objection in principle to this alternative.

Voluntary measures in other sectors may reduce costs, but they only capture companies which chose to be involved, meaning that companies with problems will avoid them. Firms tend not to commit resources to 'non-productive' activities or employ or train skilled staff if they are not compelled to do so; however, compliance with such schemes can be enforced by tender provisions issued by the government or major companies. A voluntary approach has worked with Defence Export Controls, as membership of the scheme is required to gain contracts.

Co-regulation is also employed in NSW, with the relevant minister retaining broad control, but leaving much of the detail to industry.

IoT Devices

Some Australian consumers, as well as mining, manufacturing and infrastructure companies, are increasingly worried about the vulnerability of IoT devices, such as security cameras or card readers. However, many other users remain blissfully unaware of the vulnerability of the growing swathe of internet-connected devices in their homes and workplaces. The simple firmware of such devices can often be hacked to recruit them into botnets to launch DDoS attacks, for example, while cameras can be intercepted to give hackers views into people's home. Companies show little concern for such issues, if they are not directly affected, but lower insurance costs for properly hardened networks could encourage a greater sense of responsibility.

The announcement in October 2017[52] that the Australian Government is negotiating with the technology industry to label IoT devices with a cyber security consumer rating is welcome and could help consumers make easy but more informed choices.

However, the warning by Dan Tehan, the Minister Assisting the Prime Minister on Cyber Security, that the government is prepared to pass new laws if voluntary codes are not applied is necessary, given the lack of security built into devices today, from fridges and televisions to baby monitors and toys. There could be up to 50 billion such devices in the world by the end of the decade, offering hackers a simple and surreptitious route into family computer and Wi-Fi networks, if they are not properly protected. American baby monitors have already been hacked, for example, and New York's Department of Consumer Affairs warned parents about their use in 2016. Future threats to driverless vehicles, heart pacemakers and automated industrial machinery could prove even more damaging. Taskforce members were therefore prepared to support making compliance for IoT a legal requirement and its extension to all software apps that link IoT devices to the internet.

A cross-party group of US Senators recently introduced a bill that would force companies providing internet-connected equipment to the US government to ensure their products can receive security updates, do not have known security vulnerabilities and have changeable passwords[53]. Such provisions could be adopted by, and harmonised between, major international markets to close loopholes, reduce costs and ensure security.

Carrying out more research on current threats is reactive, rather than proactive, and more effort should be expended on making the internet inherently more secure. There is a need for better 'security by design' across the whole internet, rather than just IoT devices. The entire system must become more robust, rather than holes being plugged and patched when they are discovered.

The Australian Government is not merely sitting back to observe what is rolled out in the USA and UK to deal with vulnerabilities such as the IoT. The ASD works closely with its Five Eyes partners on defensive measures, and up-to-date threat data is vital to success. 'Security by design' will be encouraged by market demand, as well as government mandate, and the government appears willing to give industry and consumers a chance to 'clean their own house', supported by official advice and information, before embarking on more prescriptive measures.

Vulnerabilities in ICT

While accrediting the security of new IoT devices is important, many other IT devices used by SMEs and large companies every day may not have had their safeguards verified. Security issues in all electronic devices should therefore be a concern, whether they are IoT appliances or standard IT hardware. Many devices could run for years without any issues, but lack proper updates and support. If a vulnerability is detected, their owners will not have the proper mechanism and processes in place to ensure that these devices can be fixed.

New ICT devices are constantly being purchased and introduced, but their users often pay little attention to the security mechanisms and 'cryptographic primitives' used to secure the device. Cryptographic primitives are well-established, low-level cryptographic algorithms that are frequently used to build cryptographic protocols for computer security systems. A simple example would be a firewall device which does its job in blocking or filtering specific connections, but also contains a back door affording the manufacturer access which could be exploited at a future point in time.

Outdated software and unfixed bugs are one of the biggest and easiest vulnerabilities that cyber criminals can use to access or subvert computer systems. Vulnerabilities in software are constantly being identified, even for software that has been running for years without a problem. These bugs can be found in the way that software operates or the ways in which the 'cryptographic primitive' was implemented.

A company would need to be aware of such vulnerabilities as well as have the right team to monitor and fix them. In October this year, a vulnerability was detected in the cryptographic implementation of WPA2, which has been in used in WiFi networks since 2004, which means it took 13 years to find the bug. New software from major companies can also have its flaws, with the recent revelation that a generic 'root' user name can be used to gain admin access to any computer running the latest MacOS High Sierra.

Mobile devices play an important role in modern corporate networks, but many companies do not have proper policies or procedures in place to prevent their use as espionage tools. Cyber criminals understand this, and sophisticated techniques combining social engineering and vulnerable apps are now using mobile device as access points to enter internal corporate networks.

Malware, spyware and viruses can be running from the day of purchase of a new device. Pre-installed software has been found to contain spyware and malware, which can be used to transfer sensitive company data to cyber criminals. There are even companies which specialise in creating malware to break through specific security defences and which sell their malware in the open market.

The increasing use of Voice Over Internet Protocol (VoIP) technology for interpersonal interaction has created a host of opportunities for hackers to tap into most corporate communications while data is being transferred over the web, instead of through strictly controlled internal networks.

New attack variables are constantly being developed, from stealing data from air-gapped networks using security cameras to stealing sensitive data using the Bluetooth/non-Bluetooth wireless devices used in the network and logging mobile keystroke while someone enters an email password on a mobile device.

Cryptography

Cryptography plays a vital role in securing networks, devices and communications. It would be fair to say that cryptographers will be the locksmiths of tomorrow.

However, merely enabling encryption in a device or communication portal does not guarantee security. As with any security scenario, a host of other issues may come to the fore, including how 'cryptographic primitives' are implemented, the various cryptographic algorithms and protocols on the market, and approaches chosen to secure a network.

Even the most robust commercially available algorithms are vulnerable if implemented incorrectly. 'Side-channel analysis' can be used to monitor communications and deduce the keys used from the network packets sent, compromising data and passwords. A side-channel attack gains information from the physical implementation of a cryptosystem, utilising information such as timing, power consumption, electromagnetic leaks, or even sounds.

Email is another area where cryptography is often absent or insufficient to guarantee security. The majority of emails are still sent in plain text, and once an email leaves a network heading toward the recipient's address, it bounces unprotected over several servers and networks before reaching its destination. Sensitive data can be readily accessed during its transmission and used by malicious entities monitoring email servers for such messages.

Companies that use encryption devices usually rely on the manufacturer to ensure that their security is watertight. Most manufacturers offer several different encryption options to choose from while setting up the device. This, in effect, moves the responsibility for security to the company buying the device. If data is leaked due to a weakness in the cryptography, a manufacturer can always claim several options were available and the customer chose poorly. A cryptography expert or consultant could provide the necessary information to make the right choice.

Backdoors and data leakage can occur at any point in the development of a device or its software. Choosing the right cryptographic primitives and security mechanism is therefore essential from the outset, because it can change how the software or system works, as well as determine how a system is developed.

Cryptography should therefore be considered at the start of developing devices, software or systems, rather than a final step to assure their security in operation.

Education and Skills

A 'technology first' approach will always leave organisations struggling to meet new threats, as attacks will always evolve and strike before defences are developed. Education is required for all Australians, of all ages and backgrounds, in cyber security, as almost everyone either uses computers and mobile phones, or depends on those who do. While it is usually presented as a technological issue, the human factor is vital in cybercrime. Every breach required an active human intent to cause harm and, all too often, was enabled by mistakes or oversights by the targets of abuse. While the training of more cyber security professionals is clearly important, everyone needs to know how to protect themselves and, just as importantly, to actually do so.

Educating Young People

Even young school children are warned about dangers online, given their increasing access to tablets and computers in their studies and at home, and continuing cyber security education should encourage greater awareness as they enter the workplace.

Education efforts should be based on a set of national standards and best practice, rather than ad-hoc activities, and benchmarked against international activities and outcomes. The renewed emphasis on STEM education in schools should encourage more students to study computing and related subjects, enabling them to enter cyber security careers, and this avenue should be emphasised as a career option, given the outsourcing of less sensitive tasks abroad or their automation. Younger cyber security professionals should also have a greater voice in the cyber security debate, as they are closer to front line developments than their older colleagues in senior management.

Children should be taught about cyber issues at school, with lessons linked to new family versions of online business awareness courses for use by the whole family at home. Young people are often more *au fait* with emerging technology and media than their older peers and can educate their elders in turn. Children could help teach family members about the danger of 'phishing', for example, and the havoc that clicking a rogue email link might cause. Cyber security must become part of 'societal DNA', rather than be reduced to a business issue.

Although some schools do teach children about cyber issues, there is no NSW Department of Education curriculum distributed to shape courses in high schools. Lessons on children's wellbeing in NSW schools discuss the issues around posting private information on social media, but this has not been tied to wider cyber security precautions. The Skills and Economic Development Division of the NSW Department of Industry are working on a cyber strategy for the NSW government which could be linked into schools, and further efforts of this kind are required across the whole country.

Educating Employees

Many employees with computer access are poorly educated about the threat of cybercrime, and penetration testing should address staff behaviour as well as software. While only a handful of technicians may understand the IT system in a firm, any employee can offer a weak point of entry to it.

Any number of system and hardware controls can be put in place, but most security breaches occur at the interface between chair and keyboard. The 'human factor' is increasingly the weakest link in cyber security. It is a human fault, if default passwords are used to safeguard computer systems, rather than a defect in the system itself. Ways to link cyber security frameworks with real-life employee and customer activity must be found to ensure they are effective.

There are many ways to prevent people clinking dangerous links in emails, for example, from staff training to automated scanning, and a range of defensive strategies must be employed to account for the failure of any particular one. However, the failings of companies to secure their data should not be blamed on lowly employees when senior executives have neglected the issue themselves and allowed a lax and under-resourced culture to develop. The new state-based Cyber Security Centres could be asked to reach out and educate the private sector in their regions, but there must be a willingness to engage from the nation's firms.

Different levels of security training are required, given the threats employees may face and the access they have to vulnerable systems. Although attention is concentrated on the need for high-end specialists, many middle managers and lower skilled workers lack compliance training of the most basic kind. Common global frameworks for IT and digital skills, such as FAIR[54], for example, already exist and should be more widely adopted to ensure compliance with international norms and acknowledge the growing importance of cross-border digital communications and trade.

Educating the Public

While the threats to business are always emphasised, members of the public are vulnerable to cybercrimes at home as well as in their companies. Baking cyber security into the social consciousness of everyone would help improve it in companies. Older people as well as the young spend a great deal of time online, and retiring baby boomers[55] are an increasingly important, and vulnerable, section of the population, as their technology skills tend to stagnate after they leave the workforce, leaving them vulnerable to new threats online.

Efforts to educate small and medium-sized enterprises should therefore be applied to the whole population to ensure all Australians remain secure in their day-to-day interactions and are mindful of the personal information they share on social media. Many of the broad concepts which secure businesses apply equally well to private individuals and would buttress education efforts about social engineering breaches and email phishing at work. Well-structured, coordinated public information campaigns, similar to those for driver safety or against smoking, could educate all Australians about cyber safety and be funded at the state or federal level.

While the government does run a *Stay Smart Online* initiative, and *Security, Influence and Trust*[56] (a community of cyber security awareness practitioners backed by Australia Post and other organisations) has promoted online safety recently, better coordination of public information campaigns on cyber security will help raise community awareness that these resources exist.

Cyber Expertise

The Taskforce agreed that a lack of suitably skilled cyber security personnel is a major problem and contributes to poor defensive measures. However, a number of promising developments show that change can be effected. A new ‘CyberGym’ in Melbourne’s Docklands is training technical staff from a variety of organisations in digital defence[57], while the Optus Cyber Security Experience[58] offers online cyber education for secondary schools, TAFE and universities which may encourage students to consider a career in cyber security. AusCyber has been working with leading TAFE institutions to develop a common standard for cyber security graduates, to be revealed in November 2017[59], while ANU has just announced its new interdisciplinary Cyber Institute *“to bring together the required expertise across a range of areas to deal with highly complex issues in the cyber domain”*.[60]

The Taskforce created a Skillset Development Subgroup which agreed on several areas of concern, including the fragmentation of training approaches and content. A revamp of Australian training would reshape registered training organisations and TAFEs, encouraging a more coherent approach by the public and private sector. It would also facilitate global recognition of Australian standards and personnel and facilitate international exchanges.

Progress on cyber security requires enough people with the right skills, and boards would be more confident and show greater leadership if they could rely on qualified personnel in this sector. A national framework for qualifications would help ensure that professionals have the right skills – and character – to be trusted. There are many organisations offering little more than marketing material, but Australia has no accreditation body to regulate their offerings. Accreditation is usually processed by state police departments (although in Queensland it is handled by the business department), and a more comprehensive system is required.

The Subgroup therefore recommended the creation of an accreditation body for cyber skills training, linked to existing licensing or security legislation and encouraging the internationalisation of training content through partnerships and leadership.

There is student demand for more formal courses in cyber security, as its graduates would be constantly employed. Cyber security courses would offer portable skills applicable to a variety of industries, from aviation to banking, which would encourage parents to fund their children's studies. The problem lies in finding suitable lecturers and supervisors, as the subject is still relatively new.

Businesses and agencies struggle to retain skilled staff, given demand for them outstrips supply. Cyber security specialists can hop from job to job in pursuit of greater challenges or pay, but short stays increase the chance of security loopholes. Government departments lose skilled people every month, for example, and should perhaps organise secondments with the private sector to give their cyber security professionals the new experiences they seek, without losing their long-term employment.

A good deal of work is already underway on improving academic and vocational education. The Australian Information Security Association (AISA) is working on course and diploma content with TAFE and universities, for example, to ensure they highlight the skills and outcomes which businesses require. Some high schools are also keen to add cyber security to their curriculum, but receive no guidance from the Department of Education on what to include.

The federal government is working on curriculum content with the Australian Computer Society, but the Academic Centres for Cyber Security Excellence, announced in 2016, have been undermined by poor funding, with typical grants of $200,000 per year wholly inadequate to the task at hand. Demand for master's degrees in cyber security have doubled or tripled in recent years, but universities are not meeting the demand. UNSW, the University of Sydney, Macquarie University and Edith Cowan University offer cyber courses, with the latter hosting a research centre, as well as a computer and security faculty.

Accreditation

The Taskforce agreed that improved standards of education in cyber security and cybercrime prevention will require the development of more standardised and authoritative accreditation schemes. Australia still lacks a central accreditation body to ensure that standards are both set and met. There is no shortage of talented and experienced professionals who could assist in developing such standards, and the creation of a suitable body was flagged as a priority for additional government action.

CONCLUSION

The Australian Government clearly takes the issue of cyber security seriously, but continuing incidents, such as the leak of F35 data by a poorly secured Adelaide contractor, underlines the need for deeds as well as words in both the public and private sector. The 2016 Cyber Security Strategy is a foundation on which to build for the future but important planks, such as CERT Australia's Information Sharing Portal, are still 'under development' months after their original launch date.

Attacks have multiplied over the last twelve months, with 47,000 reported this year, an increase of 15%. Many attacks are not reported to the police, although they constitute a crime, which complicates the development of defences. Attack vectors include business e-mails and insecure IoT devices, demonstrating that current self-regulation is insufficient. Cyber criminals have used social media to profile and impersonate CEOs to claim six-figure invoices from their firms.

Cyber security must therefore be maintained by every individual, manager, firm, agency and employee, and awareness is key to prevention, given the importance of the 'human factor' to technological breaches. Alternative and innovative solutions must be continually developed to match the energy and ingenuity of criminal and hostile state adversaries. This will require a more complete understanding of current and incipient cyber threats and the training of more specialists to counter them through a wider range of properly accredited courses.

While the Commonwealth and commercial companies allocate significant sums towards improving cyber resilience, these resources are still dwarfed by actual and potential losses due to poor security provisions and sloppy real-world practices. Computing and internet connectivity have become so pervasive, that almost everyone is a stakeholder in the issue, but this means efforts are often disjointed, despite the pressing need for a united defensive front. More research is required into the true scope and scale of cybercrime to help government shape policy responses. Many vendors of technology are not complying with acceptable security standards and government inaction about insecure IoT devices creates a difficult situation. Business and community still lack awareness of the risks involved, and better training and accreditation are required for specialist staff.

Modern society itself depends on a safe and reliable online environment. Computing has become the administrative backbone of almost every company, and the internet is the dominant marketplace. The identity and social lives of many younger people is tied almost as much to their social media profiles as to their 'meat space' reality. Cybercrime cannot be allowed to blight personal lives and cripple industry, just as espionage and hostile state actors must be repelled to safeguard our freedom and security.

We all share a responsibility to protect ourselves and each other online, as we do in the rest of our lives, and in the end, we cannot expect the government to bear a burden we refuse to shoulder ourselves. This is especially true for Australian businesses. Companies of every size, sector and vintage are quick to use IT and internet connectivity to reduce costs and boost sales, but they must also invest in security to ensure users trust their services and continue to use them. Cyber security must become an integral part of companies' operations. Customers will not trust businesses which are continually hacked, and long-anticipated innovations such as driverless cars will stall if people fear their physical safety is at risk from cyber vandals or malicious hackers, with no human behind the wheel.

While the Turnbull administration has prioritised cyber security measures, government leadership and responsibilities remain diffused across Foreign Affairs, the Attorney-General's Department, the ASD and other bodies, and the 'cyber tsar', despite his best intentions, is not able to drive reform. The issue of cyber security is important and pervasive enough to be dealt in an integrated way, perhaps through a new home affairs portfolio or a strengthened role for the Attorney General, to provide a more authoritative strategic approach from government. Administrative change is needed, as well as greater commercial and individual awareness, rather than another strategy paper.

Leadership is not only required from government and the IT services sector itself, but from everyone with the power to improve security and encourage change. A collaborative cyber security approach should combine the efforts of government, industry and academia to safeguard society, as the threat of malicious activity grows as quickly as online technology itself. Cyber security must become as agile and multi-faceted as the threats it defends against, encompassing public education, employee training and threat prevention, response, resilience and recovery.

The subject of cyber security can appear too complex to comprehend, and the technological and administrative minutia baffles most non-specialists. However, everyone can understand that any defence is only as strong as its weakest point, and the long list of hacks enabled by negligence of the most basic security procedures means that everyone can play their role. Cyber security, like software or the internet itself, is always in a 'beta' state, subject to constant iteration and improvement, but individual diligence will always be the most important factor.

Stakeholders cannot simply demand action from government or each other, but must take responsibility for ensuring their own cyber security, contribute to education and research, and play an active role in delivering change for the better. As the lines between hardware, software and services blur, technology companies of all size have a duty to design security into the next generation of networks and devices, given their growing ubiquity and importance to society, rather than patching and reacting to incidents as they occur.

ATTACHMENTS

Acknowledgements

Taskforce Membership

Gordon Arbinja, Detective Inspector, Cybercrime Squad, NSW Police Force

Prof Greg Austin, Professor, Australian Centre for Cyber Security, University of NSW

Damien Bailey, Partner, Herbert Smith Freehills

Tony Bates, Deputy Secretary, Governance Policy & Coordination, VIC Department of Premier & Cabinet

Keith Besgrove, Policy Adviser, Energy Consumers Australia; Chair, National Standing Committee on Digital Engagement

Matthew Boyley, Chief Information Officer, Department of Industry, Innovation & Science, Australian Government

Jason Brown, National Security Director, Thales Australia; National Head, Standards Committee for Security & Resilience

Simon Brown, Head of Strategy & Capability, Information Security Group, Westpac

Ian Cameron, Head of Cyber Security Strategy & Governance, IAG

David Campbell, A/g Assistant Secretary CERT Australia

Rod Cowan, Strategic Advisor, Emirates, ECU Centre Dubai (CASS)

Gabrielle Davies, CEO, Rightworkplace

David Fox, VP Security Division, DXC Technology

Peter Fritz AM, Chair, Australian Government Consultative Committee on Knowledge Capital; Group Managing Director, TCG Group; Chairman, Global Access Partners

Catherine Fritz-Kalish, Co-Founder & Managing Director, Global Access Partners

Air Marshall (ret) John Harvey, NSW Defence Advocate

Stephen Hayes MBE, Partner, Gravity Consulting

Jeremy Hulse, General Manager, Cyber Security, Thales Australia

Martin Kaldor, Consultant

Sam Keayes, Vice President of SIX/GTS, Thales Australia

Will Keppel, Content Assessor/Investigator, Office of the Children's eSafety Commissioner

Gabrielle Knowles, Senior Marketing Manager, ANZ, Splunk

Helaine Leggat, Director, Information Legal

Anthony Lu, Information Security Analyst Strategy & Capability, Westpac

Debbie Lutter, Chief Security Officer, DXC Technology

Alastair Milroy AM (*Taskforce Chair*), Consultant

Wayne Plumridge, Detective Sergeant, Cybercrime Squad, NSW Police Force

Stuart Strathdee, Asia Pacific Security Director, Splunk

Tanya Stoianoff, Government Affairs, DXC Technology, Australia & New Zealand

Braham Thiyagalingham, Cyber Consultant, Thales Australia

Aiden Tudehope, Managing Director, Government, Macquarie Telecom

Phil Vasic, Regional Director ANZ, FireEye

Prof Vijay Varadharajan, Microsoft Chair, Professor in Innovation & Computing Director, Advanced Cyber Security Research Centre, Macquarie University

Warwick Watkins, Managing Director, WW & Associates; Chair, National Consultative Committee on Security & Risk

Tim Wellsmore, Director of Threat Intelligence & Consulting, Mandiant International

Nick Wiesener, Policy Advisor, Insurance Council of Australia

Report Production

Olga Bodrova, COO & Director of Research, Global Access Partners

Emma Johnson, Project Manager, Global Access Partners

Nick Mallory, Report Writer & Economics Consultant, Global Access Partners

Endnotes and References

All weblinks listed below were correct and live at the time of publication.

[1] Data from the WEF Executive Opinion Survey conducted between February and June 2017. The question on risks to doing business was answered by 12,411 executives across 136 countries. The full Global Risks report will be published in January 2018; https://www.zurich.com/en/knowledge/articles/2017/09/key-data-points-global-risks-of-highest-concern-for-doing-business-in-2017#country

[2] https://cybersecuritystrategy.pmc.gov.au/

[3] http://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html

[4] http://www.abc.net.au/news/2017-10-11/hacker-stole-data-from-defence-subcontractor/9040906

[5] http://www.smh.com.au/federal-politics/political-news/webconnected-household-devices-to-face-mandatory-rating-over-spying-fears-20171013-gz08jp.html

[6] https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf

[7] https://asd.gov.au/publications/protect/Essential_Eight_Explained.pdf

[8] http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf

[9] https://www.oaic.gov.au/media-and-speeches/statements/mandatory-data-breach-notification

[10] https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams

[11] http://www.zdnet.com/article/iot-alliance-australia-releases-security-guideline-for-iot-development/

[12] http://www.bluemountainsgazette.com.au/story/4987913/web-connected-household-devices-to-face-mandatory-rating-over-spying-fears/?cs=2452

[13] https://www.acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf

[14] As reported by the Attorney General's Department in the 2016-17 budget paper.

[15] https://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/National%20Plan%20to%20Combat%20Cybercrime.pdf

[16] http://www.innovation.gov.au/page/cyber security-growth-centre

[17] https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf

[18] https://www.acsc.gov.au/

[19] http://www.itu.int/en/Pages/default.aspx

[20] https://www.nist.gov/itl/applied-cybersecurity/nice

[21] http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework

[22] https://www.computerworld.com.au/article/455433/australia_signs_up_europe_convention_cybercrime_/

[23] http://au.nec.com/en_AU/solutions/security-and-public-safety/security/cyber security-threats.html

[24] http://www.abc.net.au/news/2017-01-24/turnbull-declares-cyber security-the-new-frontier-of-warfare/8207494

[25] http://www.abc.net.au/news/2016-10-12/bureau-of-meteorology-bom-cyber-hacked-by-foreign-spies/7923770

[26] https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf

[27] https://thehackernews.com/2017/02/cloudflare-vulnerability.html

[28] https://www.theguardian.com/technology/2017/jun/16/wannacry-ransomware-attack-linked-north-korea-lazarus-group

[29] https://www.theverge.com/2017/6/28/15888632/petya-goldeneye-ransomware-cyberattack-ukraine-russia

[30] https://www.reuters.com/article/us-usa-security-kaspersky/israeli-spies-found-russians-using-kaspersky-software-for-hacks-media-idUSKBN1CG05P

[31] https://www.reuters.com/article/us-microsoft-cyber-insight/exclusive-microsoft-responded-quietly-after-detecting-secret-database-hack-in-2013-idUSKBN1CM0D0

[32] https://www.symantec.com/connect/blogs/morpho-profiting-high-level-corporate-attacks

[33] https://www.symantec.com/connect/blogs/android-malware-google-play-adds-devices-botnet-and-performs-ddos-attacks

[34] https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2016

[35] https://www.safeguardingaustraliasummit.org.au/

[36] https://www.itnews.com.au/news/barely-any-progress-made-on-australias-cyber security-strategy-463539?utm_source=feed&utm_medium=rss&utm_campaign=editors_picks

[37] http://www.canberratimes.com.au/national/public-service/aps-compliance-culture-a-risk-to-cyber security-prime-ministers-adviser-says-20170529-gwfd8j.html

[38] http://www.minister.industry.gov.au/ministers/sinodinos/media-releases/plan-boost-australia%E2%80%99s-cyber security-capability

[39] https://industry.gov.au/industry/Industry-Growth-Centres/Pages/Cyber security-Growth-Centre.aspx

[40] https://www.acsc.gov.au/publications/ACSC_Cyber_Security_Survey_2016.pdf

[41] http://www.roymorgan.com/morganpoll/consumer-confidence/roy-morgan-business-confidence

[42] http://www.asx.com.au/documents/investor-relations/ASX-100-Cyber-Health-Check-Report.pdf

[43] http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf

[44] http://www.innovationaus.com/2017/05/Govt-taps-new-cyber-alumni-plan

[45] https://asd.gov.au/publications/protect/Essential_Eight_Explained.pdf

[46] http://www.abc.net.au/news/2017-10-11/hacker-stole-data-from-defence-subcontractor/9040906

[47] http://www.defence.gov.au/ExportControls/DTC.asp

[48] http://dfat.gov.au/international-relations/themes/cyber-affairs/aices/pdf/DFAT%20AICES_AccPDF.pdf

[49] The idea was first mooted by the Australian Law Reform Commission in 2008 but was opposed by commercial interests. Its provisions were also watered down in response to industry submissions. The Privacy Commissioner received 107 voluntary data breach notifications in 2016, and this number is expected to increase significantly, once mandatory notification is enforced.

[50] Centre for Strategic & International Studies (2017), From Awareness to Action: A Cybersecurity Agenda for the 45th President, A report of the CSIS Cyber Policy Task Force, January 2017; https://www.csis.org/analysis/awareness-action

[51] https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework

[52] http://www.innovationaus.com/2017/10/Security-ratings-for-IoT-devices; also http://www.bluemountainsgazette.com.au/story/4987913/web-connected-household-devices-to-face-mandatory-rating-over-spying-fears/?cs=2452

[53] https://uk.reuters.com/article/us-usa-cyber-congress/u-s-senators-to-introduce-bill-to-secure-internet-of-things-idUKKBN1AH474

[54] http://www.fairinstitute.org/frequently-asked-questions

[55] https://www.securitymagazine.com/articles/88390-study-says-baby-boomers-more-concerned-about-cybersecurity-than-millennials

[56] http://news.nab.com.au/security-influence-trust/

[57] http://www.innovationaus.com/2017/05/Israeli-CyberGym-arrives-in-Aust/

[58] http://www.theaustralian.com.au/business/technology/optus-cyber-partnership-brings-security-closer-to-schools/news-story/91d9ee38f91cccc5998f212154a2fee1

[59] http://www.innovationaus.com/2017/10/AustCybers-brand-new-curriculum

[60] http://opengovasia.com/articles/australian-national-university-established-interdisciplinary-institute-to-focus-on-cybersecurity-and-innovation