paloalto NETWORKS® | Forbes

NAVIGATING THE DIGITAL AGE

THE DEFINITIVE CYBERSECURITY GUIDE FOR DIRECTORS AND OFFICERS

AUSTRALIA

NAVIGATING THE DIGITAL AGE

THE DEFINITIVE CYBERSECURITY GUIDE FOR DIRECTORS AND OFFICERS

AUSTRALIA

Published by

Forbes

Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers – Australia

Printing and Binding: Timesprinters

Navigating the Digital Age:
The Definitive Cybersecurity Guide for Directors and Officers – Australia

is published by:
Forbes Media
499 Washington Blvd.
Jersey City, NJ 07310 USA
First published: 2016

Cover illustration by Tim Heraldo

DISCLAIMER

Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers (the Guide) contains summary information about legal and regulatory aspects of cybersecurity governance and is current as of the date of its initial publication (September 2016). Although the Guide may be revised and updated at some time in the future, the publishers and authors do not have a duty to update the information contained in the Guide, and will not be liable for any failure to update such information. The publishers and authors make no representation as to the completeness or accuracy of any information contained in the Guide.

This guide is written as a general guide only. It should not be relied upon as a substitute for specific professional advice. Professional advice should always be sought before taking any action based on the information provided. Every effort has been made to ensure that the information in this guide is correct at the time of publication. The views expressed in this guide are those of the authors. The publishers and authors do not accept responsibility for any errors or omissions contained herein. It is your responsibility to verify any information contained in the Guide before relying upon it.

Introduction

Forbes Media – Bruce H. Rogers, Chief Insights Officer and Head of the CMO Practice

Cybersecurity is at the top of the agenda today in many boardrooms and executive suites. In a 2016 Forbes Insights and KPMG survey of 1,200 global chief executives, cybersecurity was named as the top enterprise risk—a dramatic shift from the previous year. What was once an IT problem is now recognized as a strategic, operational, and enterprise risk that can threaten brand value, share price, and safety, not to mention lost revenue and productivity. Part of it is personal. In the wake of the most high-profile cyber breaches of recent years, heads at the very top have rolled.

Beyond the headlines, cyber targets continue to expand. It's not just the theft of credit card data and other easy-to-exploit financial information; intellectual property is a key target for cyber espionage. A competitor, nation state, or someone who just doesn't like you might also arrange to remotely sabotage your quality control—or worse. Even hospitals have been subject to ransomware attacks, with criminals demanding payment to restore access to the systems that control records and hospital equipment. Nor are all attacks aiming for a financial payout. Some are engineered to embarrass an organization or individual. Some seek to gather intelligence quietly and invisibly. And some go for the jugular to outright destroy systems or equipment.

Bad actors can now find a way into a system through the most obscure and innocent means: a click-through on an emailed photo of your daughter's soccer match, the billing system of a trusted vendor—even systems that were not meant to be connected to the public Internet, such as an industrial control system or an MRI machine. And there is more to protect every day. For many organisations, the first and sometimes only point of contact with their users is digital. Every day, more sensors and devices are connected

to one another, and more corporate processes are automated and interdependent. Meanwhile, the spread of cloud services is blurring the boundaries of what is inside and what is outside of the network, as will the full advent of cognitive computing.

Within every large organisation, there is a trade-off between accessibility and security. There will always be a healthy tension between those who want to keep operating and data systems open, accessible, fast—and potentially vulnerable—and those who seek to protect valuable assets by limiting access and adding layers of security that can challenge patience and risk slowing productivity—or worse. Not everything warrants the same level of protection. Who cares if someone hacks the cafeteria menu? But at some firms, those everyday internal assets are better protected than the intellectual property being shared with a third- or fourth-party manufacturer overseas.

At the same time, there are far more sophisticated means to protect, identify, and defend against cyber threats than simply restricting access. That is why cybersecurity decisions are best made with a plan and a purpose about what to protect, how much to invest in security, and what to do in case of a cyber event. For boards and C-suites, it is a question of finding the right balance between accessibility and protection, and determining where cyber risk fits in the organisation's overall risk strategy.

Bad actors may seem to have the advantage, but it is possible to shape an organisation's culture around cyber awareness and to build security into every product, service, and investment by design. This takes a good plan, the right expertise, and leadership from the top. In the essays that follow, a distinguished group of Australian authorities share their expertise and insights about the levers of control that boards and executives can exercise when it comes to cyber risk. They also share their practical advice on how organisations can cut through the hype, prioritise what to protect, build cyber intelligence through greater cooperation and make their organisations more resilient.

We hope you learn as much from them as we have.

Introduction: The Importance of Cybersecurity for Executives in Australia

Palo Alto Networks – Sean Duca, Vice President, Regional Chief Security Officer

Anti-malware solution? Check. Firewall? Check. Intrusion prevention? Check.

For years, organisations have been spending valuable capital on check-box cybersecurity products that focus on narrow cyber risks or the specific 'threat-du-jour'. Their IT departments cobble together products and services from one legacy vendor to the next with little strategic planning or thought about what the business core risks are. And they hope that their mountain of legacy technology is updated often enough to provide some defence against the fear, uncertainty, and doubt being spread about cyber threats in the daily headlines.

However, with the number and severity of breaches on the rise around the world, this approach to cybersecurity clearly isn't working today. What may seem like fear-mongering is in fact a new reality: the falling price of computing power has allowed cybercriminals to launch low-cost, low-risk attacks yielding high returns. Hacker toolkits—easy-to-use, highly effective malware that's growing in popularity—enable novices with minimal technical knowledge to understand your digital environment better than you do, and breach your increasingly expensive and complex legacy cyber defences.

The traditional answer to these challenges has us stacking legacy technologies one on top of another, requiring more human operation to function because these point products were never designed to interoperate or share information. Rather than protecting us, these additional layers force organisations to feed threat information into individual tools, analyse what is happening, and then take action—slowing down the ability to keep up with attackers as they go deeper into our networks.

With the rise in successful cyberattacks, cybersecurity is becoming an increasingly strategic concern that threatens the foundations of enterprise value for business lead-

ers in Australia and the Asia Pacific region. Australia is a significant target for a range of cyber adversaries because of the country's prominent role in the region, its dependence on information communication technologies, and its expertise in research, manufacturing, and technology—factors that will only increase in the future. In fact, a recent report[1] by the Australian Cyber Security Centre predicts that cybercrime activity will continue to increase over the next five years, despite efforts by many governments and security organisations to combat these criminals. No leader wants their organisation to be splashed on the front page of a newspaper due to a cybersecurity breach, hurting their reputations and profitability, and undermining their business model, but this is the reality we face today.

It's time for a new approach to security. In order to beat the attackers, we have to move beyond technical point product solutions, towards shifting the economics of attackers. By deploying defences to protect what is of most value to companies (and attackers) and increasing the speed and integration of our defence, we can slow down and potentially deter attackers by reducing their profit motive. A recent study[2] conducted by the Ponemon Institute[3], a privacy, data protection, and information security policy think tank, revealed that two-thirds of the threat experts surveyed say that attackers go after the easiest targets first, quitting if the organisation has a strong defence. This suggests most hackers are looking for a quick payday. The data also shows that if a firm can hold off a breach for less than two days (40 hours), the majority of hackers will move on to another target.

How then can you forestall and thwart an attack?

Lessons from abroad

Many companies—particularly those in Australia—have a laissez-faire attitude when it comes to cybersecurity. The current people, processes, and technologies in place aren't perfect, but they seem as if they are good enough, and many companies are confident that any problem will right itself eventually. Some may even naively believe that a major breach could never happen to them—that such breaches impact only large enterprises, the government, or companies in the United States and Europe. However, history, and the range of stolen data available online, has shown that any company, irrespective of size and location, is vulnerable.

What may be contributing to this perception is the lack of mandatory data breach disclosure laws in Asia Pacific. Because no regulation in Australia forces public disclosure of data breaches—and the public discussion that usually follows disclosure—companies, consumers, and regulators may underestimate the full scope of the threat and damage. Breaches hit the news only when someone outside the organisation discovers and exposes them. Though no regulation is a panacea, organisations in Australia and elsewhere in Asia Pacific should consider what they can learn from other countries that have explored mandatory data breach reporting and notification if personal data is compromised, such as in the United States, which has multiple state-level data breach notification laws, and the European Union.

Not all lessons from abroad are mandates, however. There also are newly emerging, well-regarded voluntary approaches that help entities manage their cybersecurity risks. With many voluntary standards and methodologies already in use globally, Australian organisations should not try to reinvent the wheel. To help guide executive management and boards of directors, they should consider using the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which was developed in an open, collaborative partnership in the United States between NIST, a US federal agency, and the private sector. The framework, which points to globally accepted, voluntary, industry-driven standards for risk management, provides a common language and benchmarks for cyber resilience across an organisation (from boardroom to IT analyst), when dealing with stakeholders and third parties, or when operating across

borders. It enables organisations to manage or complement how they deal with cybersecurity risks by building public and private trust, establishing a common lexicon and framework for accountability, and quantifying their risk from end to end in order to plan, prevent, and respond to cybersecurity risks. Regardless of how executives and boards structure their approach, any strategy must encompass the entire cyberattack lifecycle—the sequence of events that adversaries go through to infiltrate a network and to extract confidential and sensitive data. More broadly, frameworks and strategies for managing cybersecurity risk should not be merely lists of technology check boxes, but rather should be solution agnostic and interoperable among different systems.

Three investments a security program should make to mitigate risk

There is no doubt cybersecurity provides longevity to a business and can help differentiate it from its competitors—for both good and not so good reasons. The Australian government is taking important steps to help raise Australia's cyber resilience with the release of its Cyber Security Strategy in April 2016.[4] Australia recognises that strong cybersecurity is fundamental to the growth and prosperity of all organisations in the public and private sector, to make the country's online systems and networks more resilient, and to provide trust and confidence to citizens, businesses and customers alike.

Toward that end, instead of chasing after a silver-bullet security product, organisations in Australia should target investment in three areas to reduce cybersecurity risk:

- ***Strong cyber defences.*** Companies should practice good cyber hygiene to protect and maintain their systems and devices appropriately, ensuring they are up to date. By taking an inventory of your environment and applications, you can ferret out gaps or deficiencies and note where you lack visibility in your network. Some problems are easily fixed, such as rolling out current patches for operating systems. Organisations should conduct regular health checks around where and how their data is secured, what applications are in use in their network, who are the users, and what do they have access to—as well as the threats traversing the network—to reduce the organisation's overall risk exposure.
- ***A well-trained workforce.*** According to the 2014 IBM Chief Information Security Officer Assessment,[5] human-related errors lead to nearly 95% of all security issues. Companies should therefore educate employees on how to identify and protect their organisations from threats such as phishing, when hackers pretend to be a legitimate entity in an email. Cybercriminals may search online for an employee's interests and hobbies to craft an attack, in the hopes of luring the worker into opening an infected attachment. Organisations should look to move beyond a compliance check for this training and see how they can invoke change to better defend themselves. Businesses should encourage users to protect their data and their systems at home, as this will naturally flow into the workplace.
- ***Integrated platform.*** Organisations should seek out technology that acts seamlessly behind the scenes, on a platform smart enough to take actions on your behalf, with a minimum of manual effort by your security professionals. The only way to deal with adversaries using automated tools is to automate your defences as well.

The elements of your security should be part of an ecosystem—a community of interacting devices, networks, hardware and software vendors, consultants, academics, people, and organisations—sharing threat information constantly and in real time. For example, if malware has been communicating with ten websites a certain way, and the traffic indicates a threat, your site should learn to ward it off. Organisations who share threat intelligence among their peers can thwart nearly four out of every ten hacks.[6]

These three elements can also make security efforts more efficient. You may have seen reports of shortages of cybersecurity talent, with millions of jobs unfilled worldwide. One way we can start to alleviate this shortfall may in fact be through re-alignment. If organisations establish basic cyber hygiene, and if the people, processes, and technology all work together, then companies can make better use of the resources they already have. If you leave your proverbial keys in the front door, attackers will come straight in, requiring manual response activity that is costly in both time and money. By changing your approach to cybersecurity to emphasise preventing as many attacks as possible, your team can focus on protecting your core business value.

Prevent and respond

In Australia and beyond, the prevailing perception is that cyber threats are becoming so advanced that companies can't keep up. The logic goes that if getting compromised is inevitable, efforts should be focused on clean-up after a data breach. Yet isn't an ounce of prevention worth a pound of the best cure? We should all lead with a prevention-first mindset, as this is the outcome worth striving for. This doesn't mean that you must expect to be 100% perfect all the time, but with a sound prevention strategy, attackers would need to design and develop unique tools every single time they want to attack an organisation.

Defeatist thinking is due in part to our over-reliance on siloed legacy security products. Companies are forced to chase after each problem coming in, treating every intrusion at the same level of risk and potentially allowing the gravest ones to slip through the net. In this stacked security model, products such as legacy firewalls, intrusion prevention systems, antivirus software, and the like are purchased in isolation from different vendors. Piled on top of each other, the pieces fail to tie together, and it's easy to lose visibility on potential threats.

Complexity is the enemy of any security program. Ironically, the more technologies deployed in an organisation, the more complex they become to manage, and the less secure you become. The more complex a system, the more room there is to overlook gaps or miss critical alerts, making it more likely an adversary will discover a way to bypass it.

A containment strategy is also critical. A perimeter breach isn't the end of the game—it's the start of the clock. From that point on, how can you limit your attackers' ability to move around your network and reach their objective? That objective could be to steal intellectual property or to undermine the integrity of the data held by your organisation. After gaining entry on one computer, adversaries go low and wide in a lateral movement, mapping out a route to the servers that store your organisation's crown jewels. They install remote administration tools onto machines in order to command and control them from afar. Cybercriminals then hide or encrypt your data before stealing back out. Blocking the hacker at any stage of this attack lifecycle could protect your organisation and stop the attackers from reaching their objective.

Adversaries, with their finite resources, do not invent new ways to attack each new target. Instead, they rely on an established set of techniques that they adapt for specific situations. When they launch their campaigns against specific targets, they leave threat indicators behind in their wake. These indicators serve as forensic artefacts that describe an attacker's methodology, similar to digital footprints left behind. Over time, threat researchers, security vendors, and government intelligence agencies discover through observation new threat indicators. Kept informed, organisations can develop prevention controls to disrupt the attack lifecycle and prevent a negative material impact from a cyber incident.

A strong security strategy and architecture, therefore, integrates three key elements: threat prevention, threat detection, and threat eradication.

- ***Threat prevention*** uses known threat indicators to thwart campaigns at each

phase of the attack lifecycle. Because of the adversaries' propensity to reuse the playbooks against multiple targets, many organisations are aware of these clues. However, if organisations prevent only known behaviour, they will likely miss an adversary's attacks employing the newest hacking techniques.

- ***Threat detection*** automatically hunts for known threat indicators throughout the enterprise at each phase of the attack lifecycle, investigates unknown anomalous behaviour wherever it is found, and takes the appropriate actions. Detection uncovers attacks that security controls did not initially block, and also brings to light previously unknown malicious activity that organisations must eradicate or minimise.

- ***Threat eradication*** blocks future malicious activity by analysing the new criminal attacks and installing additional countermeasures. In this two-pronged-strategy, organisations must first use newly discovered signs of threat indicators to protect their networks. Second, they must understand the adversary's objectives to determine what else they can do to prevent the attack from succeeding.

While similar, all three of these essential tasks are important in their own right, but individually they are not sufficient to prevent material damage. With a strong security architecture in place, businesses will be positioned to prevent every threat that is known, discover new and unknown threats as they emerge, and quickly deploy countermeasures to prevent adversaries from reaching their objective.

Each of these tasks should be automated as much as possible. However, this is incredibly difficult to pull off with multiple security solutions that were never designed to work together or share threat intelligence. One way to address this is by having security professionals work to make strategic investments across an integrated platform that automatically correlates intelligence collection and the deployment of prevention controls for their organisation.

Conclusion

Like any business risk, cyber threats are evolving—and so should your organisation's response. Security risk should be a top concern of executive management and the board of directors in order to protect your business and your customers. Too often, business leaders view security as a matter of compliance and control, which can set up a clash between the needs to protect assets and to foster productivity.

However, cybersecurity can support the goals of senior executives to keep the company running and profitable. Executive leadership must set organisational strategy that builds cybersecurity considerations into the business planning process. Adopting a framework of standards and accountability will help organisations develop a plan that spells out who is responsible for responding to cyber incidents from a technical, legal, and executive standpoint. Toward that goal, technical and non-technical personnel should enter into a common lexicon to discuss cyber risk.

The chief information officer (CIO) and chief technology officer (CTO) are always looking for new ways to innovate and differentiate the company in the marketplace. By working closely with the chief security officer (CSO) or chief information security officer (CISO), they can achieve that innovation in a secure manner that mitigates cyber risks. Leaders can also learn from one another. By joining communities such as the Security Roundtable,[7] they can stay up to date with best practices from peers and experts in the cyber arena. The criminal underground shares the latest techniques to launch their attacks, so it only makes sense that we as defenders should share our lessons learned as well. The more we share, the better we can defend ourselves by driving up the cost of a successful cyberattack exponentially.

Armed with the expert insights in this practical guide, organisations can meet this global cybersecurity challenge. Security is

sport best played as a team, and the steps we take now will have a significant and long-lasting impact on the Australian economy now and in the future.

The insights in this guide include advice and best practices from Australian thought leaders who are chief executive officers (CEOs), CISOs, lawyers, consultants, and former government officials. At the heart of every business should be effective risk management, a thorough understanding of the risks as well as pragmatic solutions, which include better training and awareness. In cybersecurity, knowledge is the key to prevention. And knowledge starts right here.

Works Cited

1. https://www.acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf
2. http://www.ponemon.org/library/flipping-the-economics-of-attacks
3. http://researchcenter.paloaltonetworks.com/2016/02/for-cyberattackers-time-is-the-enemy/
4. https://cybersecuritystrategy.dpmc.gov.au
5. "Fortifying for the Future" - Insights from the 2014 IBM Chief Information Security Officer Assessment
6. http://www.ponemon.org/library/flipping-the-economics-of-attacks
7. https://www.securityroundtable.org

Foreword

Australian Government – The Hon Dan Tehan MP, Minister Assisting the Prime Minister for Cyber Security

The Internet has and will continue to transform our world. Digital services are now central to every aspect of our lives—work, social, and financial. The opportunities associated with this digital transformation are immense.

Unfortunately, so are the risks. Every year, millions of Australians suffer the consequences of poor cyber security. Australian businesses, small and large, are losing hard-won earnings and intellectual property—and these costs are continuing to rise.

Successfully meeting this challenge requires cultural change as well as technological expertise. Leaders and managers need to develop a prevention mindset and understand that good cyber security is built in, not bolted on. Cyber security must become a routine and legitimate subject of Australian boardroom discussions if we are to seize our future as a modern, digital economy.

I have no doubt that *Navigating the Digital Age* will play a key role in making this happen. I commend the Guide's contributors, and Palo Alto Networks, for producing this important document that will help Australians safely unlock the potential of the digital age.

TABLE OF CONTENTS

Navigating the Digital Age

1

Opportunities and Pitfalls in the Asia-Pacific Digital Economy

Australian Strategic Policy Institute – Tobias Feakin, Director, International Cyber Policy Centre

For any business looking to grow its capital income, the Asia-Pacific region offers perhaps the most vibrant global market in which to invest. Whilst the region's economic growth is easing, the region's economy will still grow by an estimated 6.3% in 2016 and will account for one-third of total global growth—twice the combined contribution of all other developing regions. This means that investors and businesses will continue to turn to the Asia-Pacific region as a driving force for growth.

As home to some of the world's largest and most dynamic economies as well as some of the least developed, the region offers a diverse range of opportunities and challenges in the digital realm. Businesses region-wide are looking to use the digital economy to enhance productivity and diversify their business practices.

Growth in the digital economy will play an increasingly important part in the overall economic development of the region. The Australian government defines the digital economy as "the global network of economic and social activities that are enabled by information and communications technologies, such as the Internet, mobile and sensor networks."[i] McKinsey estimates that the region's digital economies, fuelled by disruptive business models and the technologies that enable them (such as big data analytics, mobile Internet, the Internet of Things, and the cloud), will be worth US$220 billion to US$625 billion by 2030, composing 4% to 12% of the region's total projected GDP.[ii]

Cybersecurity must underpin these advancements if they are to reach their potential. Without consumer confidence in online services, products, and the terabytes of personal and financial data that fuel them, the potential will be left untapped. The challenges that cybercrime is creating in the region pose serious problems for the continued growth of this market. So do the region's patchy

legal and regulatory models, which aren't keeping pace with the rate of technological change. Perhaps the most fundamental challenge is simply staffing the new jobs that are opening in this field. Addressing the regional skills gap is going to be essential in the years ahead.

Opportunities in the region – how are nations performing?

With more than half the total world population (over 4 billion people) and presently only 41% of that population online (1.65 billion), there is clearly a great deal of scope to grow the digital economies of Asia-Pacific nations.[iii] However, the disparity in Internet penetration within the region is vast. Asia is home to some of the most connected countries on the planet, such as Japan, with 91% of its population having access to the Internet. For South Korea and Australia, access is at 85%. At the opposite end of the scale are some of the least-connected countries, such as Papua New Guinea with only 9% and Myanmar with 2% of its population connected to the Internet. The digital divide is self-evident, and whilst a problem to overcome, it is also a golden opportunity to build the foundations of a strong new economic future from the ground up.

On the whole there are no surprises as to the economies that are capitalising most on the digital economy. Advanced markets in Australia, Singapore, Japan, the United States, and South Korea—where infrastructure, legislation, and regulatory frameworks are mature and allow for confidence in those markets—all offer solid if unspectacular investment opportunities. Japan's e-commerce revenue grew by 7.1% in 2014–15, to US$114 billion.[iv] With strong support for further expansion in this sector from recent government ICT growth strategies, this means the future is looking bright for further capital investment. In the recent World Economic Forum Global Information Technology Report 2015, Singapore rated number one for its ability to harness ICT. That ranking is further supported by Singapore's ambitious Smart Nation Programme, which seeks to harness the potential of the Internet of Things into the heart of all it does.

Some Asia-Pacific states are seeking to expand aggressively into the new business models that the digital economy makes possible. ICT firms account for 16% of Malaysia's GDP, and Kuala Lumpur has put in place plans and policies, such as its Digital Malaysia Programme, to support and expand this part of the economy out to 2020, making this an attractive market for potential large gains.

Other countries are also embracing digital opportunities. Vietnam is seeing a rapid uptick in technology start-up firms, and in its e-commerce. This is supported by its National E-Commerce Development Program 2014–2020 and tighter laws that facilitate secure e-transactions. The Philippines has capitalised on delivering online services to the extent that by the end of 2016 it is projected that the IT and Business Process Outsourcing industry will gross US$25 billion and employ 1.3 million workers directly. This would account for a 15% share of the global outsourcing market and make up 8% of the total GDP of the country.[v]

Despite lower oil prices in 2014–15 benefiting the poorest states in the region, such as Cambodia, Laos and the Pacific island countries, there are question marks over the ability of those states to invest and develop adequate infrastructure to harness the potential of the digital economy. These countries are struggling to develop a mature connected platform for their digital economies to take off. Despite this slow growth, there are still market opportunities as these nations come online. In Cambodia, for example, the digital economy is estimated to be worth US$800 million and growing, as are the country's e-commerce outlets.[vi]

Some of the least-connected countries may discover they have an advantage; the absence of legacy physical infrastructure and technologies could allow them to more easily adopt disruptive business models in a way that more established economies can't. This is especially true for Internet access via

mobile platforms. Mobile phones have provided online access to a new generation in the region, and it's been taken up with gusto. In 2005, only 23 of every 100 inhabitants in the Asia-Pacific region had mobile Internet access; in 2014, the number had risen 387% to 89 in every 100.[vii]

Australia's cybersecurity opportunity

"This is about supporting our local cyber businesses to expand and grow. It will create more opportunities for our businesses to commercialise and export innovative and secure Australian products.…Cybersecurity and the security of the cyber sphere, ensuring this digital world…people talk about the digital economy and the digital world, the reality is our economy is digital.… There is no longer a separation—this is not a new media or a new technology—this is where we are today. This is the modern world. It is central to everything we do and hope to achieve."[viii]

At the launch of the Australia Cybersecurity Strategy in April 2016, Prime Minister Malcolm Turnbull focused extensively on the opportunities that building a strong cybersecurity industry in Australia would offer, as did the strategy itself.

In Australia, the digital economy contributes AUD$79 billion and accounts for 5.1% of GDP, making it a bigger contributor to the overall economy than both agriculture and the retail industry. It is predicted that by 2020 this could grow to as much as AUD$139 billion (7.3% of GDP). This is in large part due to increasing connectivity, the surge in mobile phone markets, and the take-up of cloud services.

Domestically, there have been multiple measures announced to encourage the maturity and innovation of Australia's technology and cybersecurity industry. Most of these were announced as part of the broader National Innovation and Science Agenda, launched in December 2015. A Cybersecurity Growth Centre has been funded with $30 million in an attempt to create clearer opportunities for Australian business. The centre will also have responsibility to coordinate research and innovation, in the hope that it will allow for Australia to become a global leader in cybersecurity solutions and services. It has to be noted that it will take some time to reap rewards. Australia isn't starting from the same kind of base that exists in the United States or the UK. The UK has established a cybersecurity export industry worth £2 billion per year, and Australia has some way to go before reaching that level.

The start-up industry is being supported in various ways through an Incubator Support Program, and through an early stage innovation fund to assist with the commercialisation of research. There are additional tax incentives for those investing in the tech industry and an enhanced visa system to attract high-quality entrepreneurial talent and skills to Australia.[ix] Domestically, there are now a range of programs in place to assist in growing Australia's cybersecurity industry, and it makes this market more attractive to industry. However, true success will be measured by the creation of a cybersecurity start-up culture that has longevity through a committed investment in money and sound policymaking.

Another key aim of the new cyber strategy is supporting Australian business to expand and collaborate in the region to capitalise on the economic potential that exists. Ben Heyes, chief information security and trust officer at Commonwealth Bank, has stated that 'there's an opportunity for Australia to reposition its economy to leverage cybersecurity as a capability into Asia.'[x] This is a position that's shared by both the policy and technology industry community, especially as Australia has the right ingredients to succeed—namely, a regulated environment, a healthy economy, a culture of innovation, early adoption of technology, and relative political stability. But in order to succeed in the Asia-Pacific region, Australia needs to craft its cybersecurity offering before it begins to export abroad.

A $36 million investment has been made over five years in a Global Innovation Strategy to improve Australia's broader international innovation and science collaboration. One of the key avenues for delivering this broader collaboration will be

through five 'Landing Pads'. These will be based in key global locations, such as Silicon Valley and Israel. The landing pads are intended be a space where Australian start-ups can access entrepreneurial talent, mentors, and investors, with the intent of growing Australia's share of a cybersecurity market, a global market estimated to be worth US$75 billion in 2015, and US$170 billion by 2020.[xi]

Inhibitors to growth

Whilst there are highly attractive opportunities in the cyber sphere in the Asia-Pacific region, there are some serious challenges to growth, which need to be addressed. A lack of connectivity in some countries; insufficient levels of cybersecurity and permissive environments for cybercrime, both of which affect consumer confidence; a shortfall in those with sufficient cybersecurity skills to meet demands; and policy frameworks that obstruct new business all must be addressed.

How effectively a country combats financial cybercrime will directly affect business confidence in that jurisdiction. Without reliable and safe online environments in which to do business, companies are unlikely to invest. Substantial numbers of first-time users are coming online in the Asia-Pacific, but cyber-hygiene awareness and practice are very low, so there are easy pickings for criminals. The rapid take-up of mobile online access creates new opportunities for data and identity theft. Online crime and a lack of harmonised legal structures and capacity are shared challenges in the region. Severe vulnerabilities result from some countries' high use of unlicensed software. For example, 84% of all software in Indonesia and 81% in Vietnam is pirated, creating opportunities for criminals to exploit. Vietnam is currently the ninth largest global botnet command and control centre. (The United States ranks first in this category). Legal frameworks in the region compound the situation. In many countries, there are very few prosecutions for cybercrime. The Asia-Pacific region urgently needs to address shortfalls in combating financial cybercrime if it's to fulfil its undoubted potential.

There is a global shortfall in those with suitable skills for the high-tech industry, and this becomes more pronounced in emerging economies. Recent research suggests that there will be a global shortfall of approximately 1.5 million information security professionals by 2020[xii], and this will impact the ability of countries in the region to recruit and retain sufficient staff to deal with cyber risks they are facing.[xiii] Australia will be affected as much as any other nation. The government expects positions for computer security experts to increase by more than 20% over the next five years.[xiv] The increased focus from universities and tertiary-education providers on cybersecurity skills will pay off in the next five years, but doesn't address current shortfalls, and this urgently needs addressing.

China's policy decisions are noteworthy for their potential to shape the market going forward. Beijing is increasing the nationalisation of its ICT base and creating an environment that pushes China to the forefront of technological advancements and gives its companies an advantage over foreign enterprises. China's Cybersecurity Law is getting closer to being adopted. The proposed law legislates for content control. It allows the Chinese authorities to cut Internet access during public security emergencies and set up alert systems and emergency-response measures. Furthermore, it calls for technology that supports crucial sectors to be "secure and controllable", which lends itself easily to requirements for companies to build in back doors allowing third-party access to systems, provide encryption keys or hand over source code.[xv] This will have a significant economic impact on international companies and investors seeking to capitalise on China's growth in this area. Additionally, as China looks to assist developing economies with their cybersecurity policies and support infrastructure, there is a concern that this approach to policy will be adopted by those nations.

Whilst the Asia-Pacific has enormous potential to reap the rewards of a vibrant digital economy, there are clearly problems that need to be addressed so the opportunity isn't stifled. Most important will be bridging the digital divide that exists in the region. Addressing these problems will require a joint effort among both the industries that are investing in the growing technology sector in the region and the Asia-Pacific states that are undoubtedly benefitting. Increased cooperation on policy, infrastructure development, harmonised frameworks for digital trade, enhanced measures for lowering cybercrime, and raising standards of cybersecurity will allow for this market to reach its potential.

Works Cited

i https://www.alrc.gov.au/publications/3-policy-context-inquiry/concept-digital-economy#_ftn1
ii http://www.mckinsey.com/global-themes/asia-pacific/three-paths-to-sustained-economic-growth-in-southeast-asia
iii http://www.internetworldstats.com/stats.htm
iv https://www.aspi.org.au/publications/cyber-maturity-in-the-asia-pacific-region-2015/Cyber-Maturity-2015.pdf
v http://gpm.com.ph/index.php/general-info/philippine-economy/
vi http://www.phnompenhpost.com/business/ict-federation-overhauled
vii https://www.aspi.org.au/publications/cyber-maturity-in-the-asia-pacific-region-2015/Cyber-Maturity-2015.pdf
viii http://www.malcolmturnbull.com.au/media/launch-of-australias-cyber-security-strategy
ix https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf
x http://www.cio.com.au/article/569942/australia-could-become-asian-cyber-security-base-says-cba-security-chief/
xi http://www.theaustralian.com.au/business/financial-services/cba-calls-for-strong-cybersecurity-strategy/news-story/ba59b4a40876cab074791e6effeb2ffa
xii https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf
xiii http://www.aspistrategist.org.au/australias-cyber-smart-workforce/
xiv http://www.abc.net.au/news/2015-08-27/global-skills-shortage-for-cyber-security-experts2c-says-commo/6730034
xv http://www.aspistrategist.org.au/cyber-capacity-building-through-the-lens-of-techno-nationalism-2/

2

The Connectivity Conundrum

Business Council of Australia – Jennifer Westacott, Chief Executive of the Business Council of Australia

Introduction

Businesses globally are in a state of transition.

Business models are being redesigned, and goods and services are being delivered seamlessly across borders, often over digital platforms, in response to the demands of the empowered consumer. Companies that effectively leverage technology will accrete commercial advantage over others that do not. New technology platforms will drive greater collaboration and sharing of information. But greater collaboration and digitisation will also increase the potential for cyberattack and cyber-theft.

Systems and data provided by these technologies need to be secure and robust, to ensure service continuity, protect commercial secrets, and, most importantly, maintain the trust of consumers. Much of the discussion and debate to date on cybersecurity has been through the lens of technology rather than the consumer. But advances in technology are not the only drivers of cybersecurity innovation. The influence of the empowered consumer is critical to cybersecurity.

Consumers want the benefits of greater connectivity and accessibility, but they also expect data protection and integrity. Failure to adequately protect systems from denial-of-service attacks and cyber intrusions will be judged harshly by consumers. Cybersecurity is a matter of trust, and anything that affects trust can affect reputation and value. For companies, cybersecurity thus becomes a source of competitive advantage.

This is the connectivity conundrum, and companies need to be prepared to deliver both service and security to survive in a globally competitive and connected world.

Empowered consumers

McKinsey describes empowered consumers as 'expert in their use of tools and information [so] that they can call

the shots, hunting down what they want when they want it and getting it delivered to their doorsteps at a rock-bottom price.[1]'

The growth of empowered consumers is happening at the same time as millions of consumers in China and other parts of Asia shift into the middle class. Consumers are benefiting from much greater competition and wider service offerings because transaction costs are reduced significantly by technology.

Australian consumers are among the world's fastest adopters of technology. In 2014, Australians were second behind the UK in terms of online purchases. Almost 90% of Australian households have Internet access. Access to the Internet means consumers can easily compare offerings from local and overseas providers. At the same time, new providers can reach millions of potential consumers simply by setting up a website.

Company reputation and trust are critical enablers of any online transaction. Real-time feedback on reputation and trust—positive or negative—is now easily available through online platforms like social media or crowdsourcing applications. Companies can receive immediate feedback and adjust their services accordingly, like deregistering Uber drivers based on consistent poor performance. Consumer power is strengthened by consumers interacting directly with one another, comparing notes, and acting in concert.

Localised markets are more globally exposed as their goods and services are internationally traded. Old business models that have long existed to facilitate exchange—particularly those that intermediate between buyers and sellers such as real estate, banks, travel agents, retail, and wholesale—are being challenged, and those businesses that do not adapt will become redundant.

Business models that rely on government regulations rather than competitiveness to maintain returns will find their customer base increasingly eroded as consumers simply bypass them. In this sense, consumers are becoming the regulators—demonstrating their preferences and appetite for risk, using data-driven platforms to deliver their preferences instantaneously.

Connectivity conundrum

Businesses have always had to work hard to understand their consumers. In the 1920s, market research was pioneered through media like radio to identify consumer preferences. But advancements in technology now make greater digitisation possible, and more data is available about consumers. This information allows companies to build better insights about consumers' demands and preferences.

At the same time, the lower barriers to entry created by globalisation are driving businesses to redesign the way goods and services are delivered, particularly across digital platforms. Established businesses will face greater competition from a rise in globally oriented, customer-focused business models.

Consumer sovereignty has always been an essential element of competitive markets, but increasing globalisation, digitisation, and the greater availability of information are delivering a step change in the manner in which businesses are interacting with their consumers.

Greater use of data can generate significant benefits for consumers, such as:

- ***lower prices.*** Efficiency and productivity improvements enabled by data mean lower production costs for companies and lower prices to consumers.
- ***access to benefits at no monetary cost.*** Companies want the economic advantages of data, so they offer customers increased benefits in return for more detailed information.
- ***more convenience.*** Greater automation reduces the manual tasks required by consumers. For example, storing address details in an e-commerce website means consumers enter that data only once.
- ***greater personalisation to receive higher-quality services.***
- ***reduced information asymmetry.*** This is arguably the most significant factor in delivering a step change in empowering

consumers. The Internet reduces the amount of time consumers use to assess competing products and services, and provides consumers the capacity to make a better-informed decision.

On the other hand, greater use of data brings new risks.

For businesses to effectively use data, customers need to have trust that firms are judiciously handling personal data and that it is protected and secured. Some data about consumers may have privacy implications. Companies need to use personal data in a way that unlocks the benefits of that data, but that also preserves consumer confidence that their data is managed and protected appropriately. The aggregation of information across a spectrum of platforms creates a more accurate picture of each consumer, but with each new shared platform, there can also be greater vulnerability to cyber risk.

This is the connectivity conundrum: with greater connectivity comes an increased risk of undermining consumer confidence and trust.

Great expectations

Customers expect companies to deliver them world-class and uninterrupted service, while guaranteeing their personal data remains safe and secure. Thus cybersecurity is a competitive strength in a connected world.

Greater interconnectivity and broader distribution of technology mean businesses and their collaborating parties need to consider whether cybersecurity measures are adequate. As businesses adopt new digital technologies to customise their services for users, information protection, reputation, and trust will be the cornerstones of new business models.

As companies leverage their services on new collaboration platforms and deliver more convenient and cheaper services to customers, these advancements need to proceed in lockstep with enhancements to ensure systems are not vulnerable to cyber-attack. Companies that derive major benefit from online platforms have a strong natural discipline and incentive to ensure these systems are robust and protected.

Failure to adequately protect systems from denial-of-service attacks and cyber intrusions will be judged harshly by consumers. Cybersecurity is a matter of trust, and anything that affects trust can affect reputation and value. Degraded service or major data leaks stemming from inadequate cybersecurity erode consumer trust and confidence and, ultimately, the company's commercial value.

Consumer-driven regulation

Discussions on cybersecurity to date have largely focused on technology. But the fundamental driver is the need for businesses to meet their consumers' expectations. Consumers expect more connected and convenient services, but they also expect these services to be delivered in a safe and secure cyber environment.

Businesses will need to respond to these needs and invest in greater technology to be ahead of the risks of connectedness. To date, technology has largely stayed ahead of threats, because private-sector-led solutions respond directly to consumer needs, including consumer and privacy protection.

Regulating cyberspace in this dynamic environment is complex and fraught with difficulty. The cyber environment is non-centralised, crosses national boundaries and is characterised by consumers creating and distributing data instantaneously. This environment presents a complex challenge to government, and existing models for regulation are not fit for purpose. Governments need to consider new paradigms, working with and empowering industry to achieve a secure cyber environment. In Australia, the government has promoted self-regulatory/voluntary approaches to personal data protection.

In 2008 the then Office of the Privacy Commissioner (OPC) released *A guide to handling personal information security breaches (Data Breach Guide).* The Data Breach Guide encouraged companies to voluntarily notify the Privacy Commissioner of data breaches that satisfied the 'real risk of serious harm' test.

The voluntary scheme has been adopted by many companies, and notifications increased by 250%, from 44 in 2009 to 110 in 2015. The scheme is operating well and provides companies with flexibility to investigate data breaches as they occur and notify authorities where there is a 'real risk of serious harm'. Some high-profile examples of voluntary reporting include:

- In June 2014, Optus reported three separate data breaches in which the security of the personal information of over 300,000 of its customers was compromised.

- In September 2015, retailers Kmart Australia and David Jones disclosed that their online stores experienced data breaches compromising names, email and postal addresses, and order details of some customers. Both retailers publicly announced the breaches, voluntarily notified the Australian Federal Police, the Office of the Australian Information Commissioner (OAIC), and affected individuals, and engaged expert information technology security advice. In both cases the OAIC stated it would await further information from the retailers and praised the voluntary notification of the breaches.

The Ponemon Institute and IBM assessed that a series of 26 government and non-government data breaches in Australia last year resulted in an average total cost of $2.64 million per business and a cost of $142 per lost or stolen record.[2] The cost of a data breach is significant and provides companies with the necessary incentive to invest in stronger cybersecurity measures to protect their business and customers.

As a principle, systems should be designed to unlock innovation rather than hinder it. Companies already have incentives to invest in cybersecurity measures that are robust, reactive, and real-time. Consumers in a globally competitive marketplace already judge harshly any company that does not invest in innovation or does not respond appropriately to cyber risk.

What does business need to do?

In a data driven, technologically interconnected and globalised world, competitive markets will be increasingly shaped by the consumer. The impact of their purchasing decisions will be instantaneous, and their judgement will mean only the most competitive companies thrive.

Businesses need to respond with agility to these changes and invest in technologies and services that assist them in understanding their customers better, while also investing in security measures to protect customer data, privacy, and preferences.

When data breaches occur, businesses need to be proactive and timely in disclosing information. Businesses need to invest in resources to secure potential vulnerabilities and address issues promptly. Companies need to communicate any information about material data breaches to consumers as soon as practicable, and deliver solutions and advice to customers to minimise adverse exposure to an unintended data breach.

Business models based on instantaneous customer feedback give those businesses substantial incentives to protect their customers' data and respond in a prompt manner. Where breaches occur, companies have a great incentive to remedy the situation and help their customers minimise the impact of the breach.

What does government need to do?

Government needs to be acutely aware of the dynamic business environment and avoid overly prescriptive regulation. Business models and technology will change faster than regulation is able to adapt, and excessive regulation will slow our ability to deliver benefits to consumers and manage cyber-related risk.

Mandatory reporting of serious data breaches is not a replacement for strong cyber security that minimises the risk of cyber breaches in the first place. Government should be cautious about rushing to regulate this area. Instead, it should continue to encourage voluntary disclosure and adopt measures that encourage collaboration

between government and businesses to deal with cyber incidents, including the prompt establishment of a cyber threat sharing centre, an online cyber threat sharing portal, adoption of governance health checks, and development of national good practice guidelines.

In this dynamic and customer-driven environment, business-led solutions are the key to unlocking greater innovation. Government regulation needs to keep up with change and ensure it supports rather than impedes innovation.

Otherwise, it is at risk of regulating this century's challenges with last century's solutions.

Works Cited

1. David Edelman & Marc Singer, Competing on Customer Journeys Harvard business review 93(11):90-100 · November 2015
2. 2016 Cost of a Data Breach Study: Australia, Ponemon Institute for IBM, https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03094auen/SEL03094AUEN.PDF

3

Cybersecurity and the Law

King & Wood Mallesons – Cheng Lim, Partner

Introduction

Day by day, breach by breach, it is becoming clearer that cybersecurity is the business risk issue of the decade. Unlike Y2K, there is no end date by which the threat will either be addressed or will result in widespread disaster and chaos. Cyber risks are here to stay, and are likely to grow exponentially with the growth in Internet usage, connectivity, and the Internet of Things. The thought of 21 billion connected and potentially compromised devices by 2020 is almost too frightening to contemplate.

Government and regulatory bodies have begun to make cybersecurity a key focus of their activities. The Australian Securities and Investments Commission (ASIC) released its cyber resilience health check in 2015 and completed its first cyber resilience assessment on market operators ASX and Chi-X in 2016,[1] while the Australian Government's Cyber Security Strategy was finally released in April 2016.[2]

Governance

It is now beyond doubt that cybersecurity is not simply an IT issue but is a governance issue for all organisations, and for the nation. ASIC has made it clear that it expects Australian companies to address cyber risks as part of their legal and compliance obligations under the *Corporations Act 2001* (Cth) (**Corporations Act**). In addition, the broad common law duty imposed on directors to act with care, diligence, and skill is likely to require them to take reasonable steps to ensure that their companies adequately address and manage cybersecurity risks.

We expect boards to engage actively with management on cybersecurity issues to ensure that their companies have undertaken appropriate and comprehensive audits and reviews of their governance structures, processes and procedures, IT systems, and information holdings, to be able to assess their cybersecurity maturity. While the use of cybersecurity risk assessment

frameworks such as the NIST Cyber Security Framework (recommended by ASIC) or ISO 27001 can be useful in this regard, it is important to ensure that cybersecurity audits and reviews are not merely 'tick-the-box' compliance exercises, but a real analysis of the risks and threats faced by organisations. Board members should be sufficiently educated in the language of cybersecurity to ask relevant and informed questions in risk and audit committees to enable them to satisfy themselves that management has taken adequate steps to protect their organisations from cyber risks, and to recover and respond should a cyber incident occur. Asking questions such as those posed by Telstra's "Five Knows of Cybersecurity" can be extremely useful in helping board members think about the risks that their organisations face, and the adequacy of the measures taken to address those risks.

Disclosure and other regulatory issues

Unlike some other countries, Australia has not enacted, nor does it propose to enact, any laws that specifically address cybersecurity audits, risks or information sharing. However, the occurrence of a cybersecurity breach would give rise to rights or obligations under a variety of Australian laws.

First, Australian ASX-listed companies are under continuous disclosure obligations under the *Corporations Act 2001* (Cth) and the ASX Listing Rules. These obligations require listed corporations to disclose information that would reasonably be expected to have a material effect on the price or value of their securities. For example, following the TalkTalk data breach in October 2015, the company's shares fell by 10.7%. Two weeks later, analysts halved their forecasts of the company's full-year customer growth, resulting in another 7% drop in share price. This sharp drop in share price following the data breach clearly indicates the potential for cybersecurity to have a material impact on share price, particularly when a breach has an impact on market share or customer retention.

In addition, investors and regulators expect to see board engagement reflected in a company's publicly disclosed information. In its cyber resilience health check report, ASIC identified cybersecurity issues as matters that may be of significant impact to the company's operations and set out its expectation that disclosure of these issues would be required in annual director's reports, and in a company's share prospectus or offer information statement in the event of a share issue.[3]

Interestingly, to date, companies that have addressed cyber and data security in their shareholder communications have been the exception rather than the rule. For example, a spot check of 55 annual reports from 2014 conducted by AMP Capital in September 2015 found that only seven made reference to cyber risks.[4] However, given the classification of cybersecurity as a material risk by businesses themselves, it is likely that such gaps in reporting will not continue going forward. In an ideal world, reporting would be consistent within the same industry and across different reporting periods, so that investors are able to establish whether there are any improving trends, and how a company compares with other players in the industry.[5]

Second, there are proposed amendments to the *Privacy Act 1988* (Cth) (Privacy Act) that, when passed, would require organisations to make disclosures of data breaches to affected individuals and to the Office of the Information Commissioner (OAIC) when the data breach may result in a 'real risk of serious harm' to the individuals affected.[6]

Even leaving aside those amendments, the *Privacy Act* currently requires organisations to take reasonable steps to protect personal information in their possession from misuse, interference, and loss, and from unauthorised access, use, modification, or disclosure. A cyber breach that results in the loss or unauthorised disclosure of personal information will in all likelihood give rise to an investigation by the OAIC under its investigatory powers, which were significantly strengthened in 2012. The OAIC can now impose penalties of up to

AUD $1.8 million for serious and repeated privacy breaches.[7]

Third, entities whose activities are regulated under specific legislation (such as banks, insurance companies, financial-market participants, and electricity-industry participants) may well have specific regulatory obligations to ensure the security of systems they operate, or the information or data they control. For example, under the National Electricity Rules, responsible persons (generally electricity distributors at the moment, but in the future, 'metering coordinators') for electricity meters must ensure that they are secure and that associated information storage and processing systems are protected by security mechanisms acceptable to the Australian Energy Market Operator.

Finally, further assistance on cybersecurity governance and clarification of what regulatory bodies expect will also be provided through the cyber guidance for financial market industry providers that ASIC proposes to develop with the RBA,[8] as well as the voluntary national cybersecurity guidelines that will be co-designed by the public and private sectors under the Australian Government's Cyber Security Strategy.[9] Listed companies should also be prepared for closer scrutiny by ASIC, which has stated that its formal review of financial market infrastructure providers is only the first of the formal cyber resilience reviews that it proposes to undertake.[10]

Risk management

The risk management activities that organisations will need to undertake will generally follow from the risk assessments they undertake in relation to their cybersecurity maturity. Nonetheless, there are a number of risk management activities that are of general application to all companies and organisations, regardless of industry or maturity.

The first arises out of the fact that instigators of cyberattacks will seek out and exploit the weakest link in the system. This means that companies will need to consider not only the resilience of their own systems, but also the security of their entire supply chain. For example, it was recently reported that U.S. law firms have been targeted by hackers who are seeking to infiltrate their networks, use keywords to locate drafts of merger agreements, letters of intent, and confidentiality agreements, and to use the information obtained to execute algorithmic insider trading.[11] As can be imagined, the undertaking of due diligence into the cyber maturity of the myriad of contractors and service providers to an organisation is not a trivial exercise and—unless it is carefully planned, scoped, and implemented—can result in a very expensive form-filling exercise with possibly very little gain.

In addition, cyber threat sharing will be an important risk mitigation strategy for many companies, to enable them to get timely information on threats that are being seen by other companies or government in the same or different industry sectors. It will be important for companies to participate in these threat-sharing forums (such as the proposed online cyber threat-sharing portal proposed to be co-developed by the Australian government and the private sector). A question remains as to whether or not that portal framework will be sufficient, or whether the private sector and government will need to develop frameworks that better support threat-intelligence sharing between and across industry sectors without fear of adverse consequences.

Looking more broadly at the spectrum of corporate activities, cybersecurity due diligence in M&A transactions is also an essential exercise in third-party risk management that should not be overlooked. While the outcome of the due diligence may not necessarily change a decision to undertake an acquisition, or the value of the acquisition, it may well support the negotiation of a specific risk-allocation regime in relation to cybersecurity risks, or the provision of optionality in relation to a decision whether or not to proceed with an acquisition. It also enables acquirers to focus post-acquisition integration actions on cybersecurity if it is considered to be a deficiency in the target.[12]

Moreover, given the likelihood that, despite all the efforts that companies may take, a cybersecurity breach is likely to happen at some stage, it is critical for them to have well-developed incident management plans. Incident management is an art in itself and, among other things, requires companies to ensure that they identify what assets and systems need to be protected, establish an incident-management committee with well-understood roles and responsibilities, have the capability to detect and contain the impact of the incident, and have a communications strategy to deal with customers, regulators, and other stakeholders. Of course, it is not enough just to have a plan—it is important to simulate the occurrence of a breach to test the robustness and adequacy of the plan.

Finally, companies should consider the appropriateness of obtaining cybersecurity insurance, not only to cover third-party liability (for which some companies may already be covered under their professional-indemnity insurance) but also to cover first-party loss and expenses (that is the cost to the company of dealing with a cyber breach, such as data restoration and systems remediation). These costs can be substantive. For example, Target has disclosed that its 2013 data breach resulted in it incurring some USD $252 million in costs, USD $90 million of which was covered by insurance.

Conclusion

In some ways, cybersecurity is just another risk that all organisations have to manage in their day-to-day business. However, the difference is the volume, variety, and velocity of the attacks, the increasingly interconnected nature of our world, and the vast quantities of data that can be compromised through a cybersecurity breach.

This requires organisations to move faster and to be more prepared than ever to deal with risks, issues, and incidents. It requires a new mindset around collaboration and information sharing between industries and competitors. The risk is not just that one organisation is adversely affected, but that trust in systems or industries could be compromised in a way that results in a loss of value to everyone. Government undoubtedly has a role to play in fostering this trust and collaboration and in setting up frameworks to enable that trust and collaboration to occur. The new Cyber Security Strategy will be an important first step in doing so.

Works Cited

1. ASIC, *Report 429 ('Cyber resilience: Health check'); ASIC, Report 468 ('Cyber resilience assessment report: ASX Group and Chi-X Australia Pty Ltd').*
2. Department of the Prime Minister and Cabinet, *Australia's Cyber Security Strategy.*
3. *ASIC, Report 429 ('Cyber resilience: Health check')*, pp 49-57. See also Cathie Armour (ASIC Commissioner), 'Cyber Security and Directors' (1 April 2015) *Company Director* http://www.companydirectors.com.au/director-resource-centre/publications/company-director-magazine/2015-back-editions/april/the-regulator-serve-and-protect.
4. AMP Capital, *Corporate Governance Report: ESG insights & proxy voting*, p 6.
5. AMP *Capital, Corporate Governance Report: ESG insights & proxy voting*, p 12.
6. Exposure draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015.
7. Sections 13G and 80W of the Privacy Act allows the OAIC to impose civil penalties of up to 10,000 civil penalty units for interferences with privacy by corporations. One penalty unit is currently equivalent to AUD $180.
8. *Report 468 ('Cyber resilience assessment report: ASX Group and Chi-X Australia Pty Ltd')*, pp 12-13.
9. Department of the Prime Minister and Cabinet, *Australia's Cyber Security Strategy*, p 35.
10. ASIC, Report 468 *('Cyber resilience assessment report: ASX Group and Chi-X Australia Pty Ltd')*, p 4; ASIC, *Corporate Plan 2015-2015 to 2017-2018*, p 19; *Policy*

and Markets Brief (April 2016) <http://asic.gov.au/regulatory-resources/markets/resources-on-markets/markets-articles-by-asic/embedding-cyber-resilience-within-company-culture/>..

11. See e.g. Nicole Hong and Robin Sidel, 'Hackers Breach Law Firms, including Cravath and Weil Gotshal', *Wall Street Journal* (online), 29 March 2016 http://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504; Chloe Smith, 'M&A Hack Attack on 48 Elite Law Firms' (4 April 2016) *UK Law Society Gazette* <http://www.lawgazette.co.uk/practice/ma-hack-attack-on-48-elite-law-firms/5054524.fullarticle>.
12. Cheng Lim and James Walsh, *'The Importance of Cyber Due Diligence in M&A Transactions'*, pp 36-7.

4

Cybersecurity Leadership: Cutting Through the Hype and Distractions and Knowing What Questions to Ask

Telstra Corporation Limited—
Rachael Falk, Former Head of Cyber Influence, and
Mike Burgess, CISO, Telstra Corporation Limited

Cybersecurity isn't a mysterious risk

Boards and leadership teams have long been well versed in dealing with unfamiliar subjects such as complex legal liability, financial transactions, strategic planning and expenditure, just to name a few. And they are used to ensuring that they understand the corporate governance obligations that go with disclosing and balancing those risks.

It is therefore interesting that cybersecurity has taken on a veneer of mystery when it comes to board and leadership discussions. Too often we hear it described as complex and technical and that boards should consider having someone sitting with them who has particular cybersecurity expertise—someone who can help them navigate the technically complex, choppy cybersecurity seas.

While there is no doubt that boards may call upon specialist, niche skills from time to time, much of the hype around cybersecurity is unfounded and distracting. And this hype has arisen largely because cybersecurity has been seen as an IT issue or driven by the murky and exciting world of espionage.

Worse still, boards and leadership teams are often told that the solution to the thorny issue of cybersecurity is for them to simply authorise more spending on technologically advanced solutions or compliance with some security standard or framework. And once these miracle cybersecurity solutions are in place, they will ensure that compliance frameworks are met and all will be well in the world of cybersecurity.

The reality is a little different. The cyber threat cannot be eliminated; rather, cyber risk must be managed.[1] What is needed at the board and CEO level to better understand the cyber threat and the attendant risk is clear advice about what questions they should be asking to get the right mix of technical and people controls in place.

Importantly—and this will differ depending upon the risk appetite of each company—every board and CEO must know and understand what good looks like in cybersecurity and their acceptable level of cyber risk. Flowing from that, they will need to ensure that their organisation is well placed on that path to good.

Cybersecurity is a business risk and can no longer be regarded as solely an IT risk. Successful companies already know how to manage significant risks—boards and senior leaders are well versed in dealing with risk. What is needed are trusted advisors who can cut through the hype and not be distracted, providing boards and senior leaders with impartial advice.

Most CEOs don't stay awake at night worrying about data breaches. They are more likely to be concerned with whether their company has identified and is effectively managing the risk. They also want to be assured that they have tested plans and capabilities to respond when a cyber incident does happen. In essence, cyber-crime is just crime, cyber espionage is just espionage, and hacktivism is protest. It is connectivity that means that all these things can occur at a pace, scale, and reach that is unprecedented.

Cybersecurity distractions in the boardroom

The main distractions that boards and leadership teams often have to contend with include threat, attribution and compliance distraction. These may be relevant when managing cybersecurity risk, but they should not be allowed to dominate boardroom discussions.

Threat distraction: This is where the escalating hype about the increased threat level and threats becoming more 'persistent' or 'sophisticated' drowns out sensible discussion about the reality of the threats out there.

> The threat environment is a given. Make sure your organisation has a deep understanding of the threat and how this is relevant to your organisation, but don't allow the hype to unduly influence spending on the next new technical solution or compliance program. Focus on what your organisation can do to counter that threat and constantly look for ways to improve your mitigation strategies.

Attribution distraction: One of the hardest parts of cybersecurity is working out the source of a threat or compromise. Cyber space is not like the real world, where there can be a perfect DNA match with the perpetrator. In cyber space, identities are fluid and can be manipulated and spoofed. In the heat of a breach, the focus for any business must be on remediating the incident and making sure that any risk to customers and company data has been contained. Attribution is an important part of any data breach investigation, but it should not dominate incident management.

> It is important that boards and leadership teams focus on remediation and recovery and not look to blame someone publicly. Attribution and root cause is important but not in the heat of an incident.

Compliance distraction: Compliance does not equal security. Boards and leadership teams should not be distracted into believing that investing in large-scale compliance activities means that there are effective security controls in place. There are many compliance frameworks out there, but it is important to question how many of them will actually result in effective security outcomes for your organisation.

Boardroom discussions about cybersecurity

Any CISO of a large organisation must be able to explain to the board and leadership team, in clear language, the cybersecurity challenge and the unique risks to the organisation. Just as it is the role of a group general counsel to break down even the most complex of legal concepts in accessible language, articulating the risk, so a competent executive-level CISO must be able to do the same thing.

Tackling the challenge of cybersecurity requires leadership from the top, driving the discussion so that all parts of the organisation understand the risk and what they are doing to manage the risk effectively.

> Compliance does not equal security. Make sure any compliance program actually results in effective security outcomes for your organisation.

Five things all organisations can do to assess their cybersecurity risk:

1. *Know the value of your data*—not only the data that is valuable for your organisation but what would be valuable to a competitor as well as what would cause your organisation pain if you were to lose it or be denied access.
2. *Know who has access to that valuable data.* Who within the organisation and supply chain has access, and do they need to have access to it?
3. *Know where that data is*—both in the organisation and across the globe.
4. *Know who is protecting that data*—within your organisation as well as any outsourced data.
5. *Know how well it is protected.* Are the right controls in place? Would you know if there is a breach? Is it being monitored 24/7?

It is only when these five questions can be answered and gaps have been remediated—**and solid cybersecurity capabilities (like security controls, threat analysis and an awareness-raising capability) are in place—** that a board or leadership can truly assess how they are managing cyber risk.

While the board and leadership team must satisfy themselves as to the answers to the 'Five Knows', they must also make sure that they get satisfactory answers and look for assurance on the three questions below.

Three cybersecurity questions the board and leadership team should ask:

1. Have we identified the right risks for our company and customers?
2. Are we managing those risks effectively (**keeping in mind** that compliance and more spending on security does not equal security)?
3. Do we have plans and capabilities in place to respond swiftly to an incident? Do we regularly test those plans?

Finding what good looks like for any organisation

There is no inherent magic in the answer to 'what good looks like' in the context of cybersecurity. However, taking the time to **move through the Five Knows review** and asking the right questions can help. What is most important is that relevant cyber risks are identified and managed effectively. Achieving or maintaining 'good' will always be a dynamic challenge because the cyber criminals and hacktivists are always looking for different ways to steal or disrupt. Good also means an organisation can comfortably complete the Five Knows exercise along with the three key questions about risk and capabilities. Good also means having effective mitigation strategies so that distractions are minimised.

It is only then that any board and leadership team can assess their organisation's cyber risk and whether they are well placed to continuously manage this risk.

Works Cited

1. Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, James R Clapper, Director of National Intelligence, February 26 2015

5

Four Questions Executives and Directors Should Ask About Cybersecurity

Stephen Day, Major General, former Head of Cyber at the Australian Signals Directorate and the Inaugural Head of the Australian Cyber Security Centre

Corporate directors and executives have asked me many questions about cyber risk. Of all those questions there are four that usefully sum up what these busy folks really want to know about cyber risk:

- Why should I care?
- What can I do about it?
- This could cost plenty, so what should I invest in?
- What does good look like?

What follows are some thoughts and answers to these questions.

Why should I care?

Chances are, while you read this brief chapter, there will have been thousands of attempts by cyber criminals to penetrate Australia's banking and retail sectors, perhaps even your own business. And foreign intelligence services will have made several attempts to penetrate the networks of some of the nation's biggest companies, as well as the government.

Australia is not at the head of the list of countries most subjected to intrusive cyber activity—the United States probably owns that spot. But Australia is attractive to malicious cyber actors for a number of reasons.

- We are, relatively speaking, a wealthy people who do a substantial amount of our business online.
- We have valuable intellectual property in some specific areas of research.
- We have strategically important resources.
- We have some significant bilateral relationships and alliances.

There are three groups who pose a threat, including organised crime, foreign intelligence services, and issues-motivated groups. Sometimes the foreign intelligence

service is aided by an insider. Sometimes the criminal or the issues-motivated group is an insider.

Organised crime is lucrative and operates globally. Long before most governments and businesses realized the value of their data, cyber criminals worked out that personal information and company data are commodities from which you can make money. For the moment, Eastern Europe is the centre of gravity for global cybercrime. It is the most sophisticated and prolific region. But cyber criminals there are selling their tools and techniques to criminals from around the world. Their knowledge is migrating to the broader criminal community.

In late 2013, cyber criminals attacked a US retailer, Target. They stole around 70 million records that included the names, phone numbers, and personal addresses of Target customers. The details of around 40 million payment card numbers were also stolen. This led to the reissue of 21.8 million credit cards at a cost of around US$200 million. Several banks that incurred the cost of the reissue are pursuing legal action to recover their loss. The criminals, meanwhile, generated an estimated US$53 million from the sale of stolen credit card details. Target's profits were down 46% from the same quarter of the previous year. The company's CEO and the CIO left the company.

Foreign intelligence services are the most sophisticated and best-resourced cyber actors. They do what spies have been doing for centuries: acquire sensitive diplomatic and national security information from other governments for strategic advantage. They also target industry. In fact, their attempts against industry in Australia are more numerous than against the government. They are trying to obtain intellectual property, R&D information, as well as sensitive insider information about board decisions such as negotiating positions. They do this primarily for economic advantage, but there are other motivations as well.

In late 2014, Sony Pictures was subject to a cyber-attack allegedly conducted by the North Korean state. Evidently the North Koreans were angered by a film produced by Sony, intended as a comedy, about a plot to assassinate a North Korean dictator. In the cyber-attack, important intellectual property was stolen and some of it selectively posted to the Internet, including the script for a not-yet-released James Bond film. Sensitive company data as well as personal emails of executives and clients, with confidential and embarrassing information, were leaked. The attack included a destructive element that disrupted the Sony network for several weeks. The co-chairman of the film side of the business was invited to leave the company. As of last year, costs to repair the damage were in the tens of millions of dollars.

Issues-motivated groups seek to embarrass their target or attract publicity for themselves, or both. They do not need much sophistication to be successful. Perhaps the best known, ironically, is Anonymous. But there are plenty of others out there, and it is common for them to work from within an organisation or to be helped by insiders.

The most publicised action by an issues-motivated group was the 2015 breach of the 'why-don't-you-have-an-affair' site, Ashley Madison, by some morally offended by the business. Costs will take a while to become clear, but the CEO was invited to leave the company. (You may be picking up a trend here.) Evidently he believed that executives should try their own products. The legal fraternity have rolled up their sleeves for suits alleging breach of contract and negligence.

Five points are worth noting from the threat:

- There are real costs to companies from these compromises, costs associated with disruption, forensic efforts, lost revenue, reputation, and loss of executive and other valuable staff.
- It is clear that a cyber incident is 'reasonably foreseeable'—an important conclusion for legal proceedings.

- It is not just about theft of data. The attack on Sony included a destructive element. If you can penetrate to steal, you can penetrate to destroy.
- Nation states are prepared to target industry to achieve strategic ends.
- None of the examples cited are from Australian business or government, and it is not because there are not any examples. There are plenty. There remains a reluctance to speak publicly about cyber incidents in many countries, including Australia. This needs to change. The nation needs to have an open dialogue to raise awareness of the threat and to swap notes on the best ways to deal with it.

The threat through cyber is present now. It is persistent, and it has real consequences.

If the functioning of your business rests on a reliable IT system, if you care about whether your customers can trust you with their information, if you care about your organisation's reputation, if you believe in the competitive advantage that IP and R&D can deliver, then you need to care about cybersecurity. Moreover, if you believe that safe, secure, and trusted networks are fundamental to the nation's social and economic wellbeing and national security interests, then you need to care about cybersecurity.

Okay, now I care, what can I do about it?

The 'what to do question' is best tackled in several parts: three framing ideas, some questions to ask, and what to invest in.

Three framing ideas

- **First**, dealing with risk of the cyber threat is senior leader business. This is not something that should be left to your IT folks to sort out. The solution is, in part, about technology. But it is primarily about risk management, culture, policy, and resource allocation. These levers are usually controlled by the board and the executive. So, effective cybersecurity requires senior leadership attention.
- **Second**, cybersecurity is a team sport. To be successful against this threat requires an enterprise-wide approach. It is no good if every department has the right approach, but the HR team, for example, do not; they will be the vulnerable point through which access to the enterprise can be achieved. And there needs to be a partnership between businesses. Businesses with similar information holdings will experience similar targeting by malicious actors. Partnerships enable the exchange of information on developing threats and ideas on how to defend against it. If a successful attack is prosecuted against online banking, then consumers' trust in that form of business will degrade for both the victim bank as well as the broader online banking community. Cybersecurity should not be a source of competitive advantage; it is too important for that.
- **Third**, cybersecurity is a process, not a product. There is no silver bullet that will make this problem go away, nor is there a one-size solution. While there are some fundamental steps that everyone could usefully take—and all solutions should involve people, process, and technology—most organisations have unique circumstances with different risk profiles that are best addressed by tailored solutions. Those solutions need review and adjustment to keep ahead of the evolving threat.

Some questions to ask

As you consider what you should be doing to deal with cyber risk, you might like to ask some questions:

- How are the executive and the board informed about the current level of cyber risk and its potential impact on our organisation?
- What data is genuinely valuable and needs protecting? You may find that only a part of your holdings matter and that is where your resources should be focused. I would suggest customer records are a data set worth protecting.
- Where is our data stored? Is it in the servers in the basement—the same place

we have had it for a decade—or is it now in the cloud? If it is in the cloud, have we satisfied ourselves with the physical and cybersecurity arrangements there?

- Who has access to our systems? In particular, who has the authority to access the entire network? The more people with this level of access, the greater the risk to an organisation. Foreign intelligence services, and organised criminals, specifically look to steal the login details of users with network-wide access. Once they have those credentials, they can move unfettered over a system to steal or change the data.
- And what of former employees? Do any still have access to our systems? Do we have a protocol— and is it being enforced—to remove access for employees as they leave the company?
- Do we have in place a mechanism to spot the early indications of a potential breach? Can we detect an intrusion if it occurs? The average time from intrusion to detection is typically 200 days. A lot of damage can be done in 200 days.
- Do we have a cyber incident response plan? If we have a response plan, have we exercised it?
- If you work for a public company, you might want to ask what your continuous disclosure obligations are in the event of a cyber compromise.

This could cost plenty, so what should I invest in?

If you had only one dollar left to spend on cybersecurity, you should spend it on awareness. Today, in Australia, there are still more people, businesses, and organisations who neither know about, nor understand, the cyber risk. And if they are not aware of the risk, they cannot be expected to mitigate it. Awareness is the pre-condition for doing something about the challenge.

Most organisations have developed their IT systems in fits and starts over many years. Many systems look like the IT equivalent of a rambling mansion. If you have never conducted a review of your network, or it has been many years since the last one, then you should invest in one. At its conclusion, your organisation should understand your system better than anyone else. This gives you the defender's advantage.

That done, you should implement the Australian Cyber Security Centre's Top Four mitigation strategies.[1] If you do nothing else, you will have met the standard the Australian government has imposed on its departments and agencies. The Top Four will mitigate at least 85% of all cyber intrusions.

If you have more to invest, then you should consider a vulnerability assessment. Bring in an external assessor who will work with you to understand your network(s), conduct a cybersecurity audit and then make recommendations on how to address the vulnerabilities.

With your preventative measures established and more capacity to invest, you could look to a monitor-and-detect capability. It is worth noting that the substantial majority of these capabilities look for known problems. This is fine because most attempted cyber intrusions still use known capabilities. But malicious cyber actors are increasingly using hitherto unknown means (known as 'zero-day exploits' in the industry) for cyber intrusions. If you are looking only for known problems, then you will not detect zero-day exploits. In response to this challenge, some detection capabilities have been developed that use anomalous behaviour indicators to identify cyber intrusions, the theory being that any unusual activity should be detected, regardless of whether the intrusion was achieved by a known, or zero-day, exploit. The market for these capabilities is growing and shows much promise, but it is not yet mature.

Larger organisations may find benefit in a threat-intelligence service. You should seek a service that will provide you with an analysis of the threats specific to your industry, which should, in turn, give a pointer to more-targeted mitigation strategies. Beyond these investments is a range of services, from insurance to cyber emergency response teams, that can help mitigate costs and speed recovery from an incident. No security is

100%, but investing in a strong plan at the outset is the most effective way to reduce your cyber risk.

What does good look like?

So what are the signs that you have a mature cybersecurity capability in your organisation? What does good look like?

Look for five signs:

1) That the cybersecurity arrangements are driven from the top. That means from the board and the executive team. Indicators that this is occurring might include the fact that cybersecurity is a standing item for the board or for meetings of the audit/risk committee. Or, that there is a mechanism in place for the chief information security officer, or equivalent, to report regularly and directly to the chief executive.

2) You know that an organisation is on top of its game when conversations are characterised by clear and plain English so that everyone can understand, participate, and contribute. This is particularly important in cyber, where many people struggle with the concept, let alone the details.

3) An organisation is in the right place if it understands that cybersecurity is more a human problem than a technical one. There was a time when a black box or an anti-virus program was sufficient to provide for cybersecurity, but that was a long time ago. The solution is about technology, but it is also about people, policy, and culture.

4) The existence of a response plan. Now, response plans can be—and should be—brief. But it is not enough just to have one on the shelf. It should be tested and subjected to regular exercise. The first time a response plan is put to use should not be for the real thing.

5) Perhaps the most significant indicator that cybersecurity is embedded in an organisation's culture is whether it features in the early conversations about a new product or venture. If cybersecurity is factored in from the beginning of new endeavours, then the organisation has moved from reactive, which describes most, to proactive, which describes very few.

A cautionary note

A risk to the reputation of the cybersecurity industry looms. Into the atmosphere of heightened concern over cyber threats there are emerging some less than honourable businesses and practices.

Trusted networks are important to Australia's social wellbeing, its economic prosperity, and its national security interests. The cybersecurity industry has an important role in helping to deliver those trusted networks. But if the industry is not trusted, then it will be eschewed, and if that happens, then our networks will be more vulnerable and more easily compromised. It follows that a damaged cybersecurity industry reputation is in no one's interest. Boards and executives can help the cybersecurity industry be a trusted one.

Demand that the service being offered be explained in plain English. If the vendor's staff cannot do this, then they do not know enough about their product, and so neither will you.

Some cybersecurity vendors are offering silver-bullet solutions. There are none. A single product is fine, as long as it is understood that it will work best if it is part of a larger plan. If you are engaged with a cybersecurity vendor who insists it has a single-product solution to the cyber threat, show that vendor the door.

Boards and executives have a role to play to ensure that the cybersecurity industry matures with its reputation intact.

Works Cited

1. Available on their website: acsc.gov.au

6

Cyber Resilience—A Whole-of-Enterprise Approach

Australian Cyber Security Research Institute—David Irvine, Chairman

For the past 30 years, governments, business enterprises, and private citizens have been galloping down the path of digitisation. So far Australia has coped well with digital disruption; we have adjusted our lives and our economy to the new technology. There is no doubt about its benefits to society and our economy, but not without some huge adjustment challenges into the future.

In the rush for bigger, better, faster, and more efficient digital technology, only in the last few years have we realized the need for safer, more secure, digital technology. We can no longer get by in the hope that cyber crime and cyber attacks happen to other people, not to us. Today, we are inundated by reports about malicious activity exploiting the vulnerabilities created by our growing dependence upon cyber technology.

Governments have had to devote increased resources to protecting their secrets and our critical infrastructure from vulnerability to espionage and sabotage by cyber means. They have had to invest both in cyber productivity and in cyber resilience, hardening their systems not only to protect information relating to national security and the efficient operation of essential services, but also to protect the intimate personal details of all Australians.

While government systems can be threatened by state and non-state cyber actors alike, by far the largest proportion of cyber attacks has been within the private sector. Cyber crime against commercial enterprises includes the theft of funds, intellectual property, and commercially sensitive information as well as disclosure and exploitation of confidential information about clients, not to mention industrial sabotage and malicious disruption of operations. The global cost of cyber crime is estimated to rise from $400 billion in 2015 (more than $2 billion in Australia) to over $2 trillion in 2019.[1] Every company and every individual is a potential target.

So ubiquitous is the threat, and so serious the potential consequences, no company director or CEO can afford to neglect it. The challenge is to understand the nature of the threat, how it can rapidly mutate and very suddenly endanger the viability of a long-proven business model—not to mention the bottom line. Cybersecurity must now feature in every business model, as well as in our personal take-up of digital technology, including the mobile technology we carry in our pockets and on our wrists.

Corporate cyber resilience

For companies there is no one solution, no single "firewall" panacea. To be successful companies need to embrace a concept of **holistic cyber resilience**, which improves their chances of resisting threats from both internal and external sources and managing those risks effectively. My own checklist for cyber resilience has 10 elements.

1. Understand risk

Cyber resilience must be a primary focus of boards and senior management. It is not something that can be left solely to the chief information officer. Nor is it simply a question of ensuring cybersecurity features on the company Register of Risk. As strategic risk managers, board members need to take personal legal, ethical, and fiduciary responsibility for the company's exposure to cyber compromise, regularly addressing the risk of cyber failure, and ensuring that cyber resilience is built into all aspects of their business and operating models.

2. Understand consequences

We can all comprehend how a prolonged breakdown of cybersecurity in the telecommunication sector, the banking industry, or an airline could be catastrophic on a national scale. At the small and medium-size business level, cyber disruption could be equally disastrous both for the business and for the customers who had placed their trust in it. For any enterprise, the failure or disruption of operating systems or the compromise of intellectual property, commercially sensitive information, or data held in trust for customers (such as personal and credit card details) will be reflected in the company's reputation, credibility, and, ultimately, its profitability.

3. Understand systems and data

Accurate assessment of risk and the consequences of failure is facilitated by a clear understanding of a company's IT systems and the data it holds. Telstra has done us a great service by succinctly summarizing this point into its "Five Knows" (discussed elsewhere in this volume). If boards and senior management understand the value of their data to those of malicious intent, if they know where that data is, how it is protected, and who has access to it, then they are in a stronger position to implement a cyber resilient business model.

Telstra's "Five Knows" are equally relevant in respect to **cloud computing**. Service providers of cloud-based systems and data storage are proliferating. The security, stability, and reliability of these systems, which promise great efficiency and cost benefits, need to be assessed carefully, according to a company's specific operating needs.

4. Regular cyber hygiene

The Australian Cyber Security Centre has drawn up a list of 35 strategies to enhance cyber resilience. While some are complicated and need the support of technical specialists, just four strategies (regular proprietary patching of software, as well as of operating systems; minimising the number of systems administrators with privileged access; and application white-listing) will help mitigate about 85% of the current panoply of malicious intrusions.

5. Redundancy, backup systems and response plans

There have been enough publicised instances of malicious destruction of data, or denial of access to data (as with ransomware), not to mention human errors causing system failure or data loss, to make it axiomatic that companies build in system redundancy and regular real-time backing up of data and records.

Redundancy and backup systems will be essential to recovery after a successful attack. Boards also need to ensure that their enterprise war-games and **regularly exercised response plans** can be implemented immediately if an attempted attack is detected. Boards need to be proactive in ensuring these elementary measures are implemented assiduously.

6. Proprietary malware protection systems

There is a growing range of off-the-shelf proprietary anti-malware systems available to the ordinary cyber consumer. Cybersecurity technology companies are developing solutions that have moved beyond the concept of ever-higher digital firewalls, necessary as those are, into exciting new realms of predictive and intuitive digital analysis, providing deeper layers of security. Major consulting companies now promote one-stop-shop cybersecurity management packages tailored to the needs of a particular enterprise.

7. Access professional expertise

Cybersecurity technology is now so complex that few companies can afford the expertise and resources to achieve cyber resilience on a solely in-house basis.

Access to regular, independent, professional advice on cybersecurity is essential, as attack methodologies proliferate in depth and breadth. Increasingly niche cyber security providers, in addition to the larger business consulting firms, have the expertise and access to sophisticated protective cyber security systems that will assist boards to support their CIOs with professional advice and customised software solutions.

What can never be outsourced, however, is ultimate responsibility for cyber security within an enterprise.

8. Continuous investment

The tools of cyber offence are developing so rapidly that the tools of defence are constantly struggling to keep up. For this reason, investment in cyber security can never be a one-off activity. Effective cyber resilience requires continuous investment in the upgrading and refining of protective systems as a normal cost of business.

9. The human factor

While the vast majority of cyber attacks emanate from outside the enterprise, human error within the organization, including through a lack of security awareness, is an important contributor to security breaches. Cyber resilience requires the active participation not simply of the company's systems administrators, but of all staff who access the system and who, as normal human beings, are tempted to click on spam or open unverified email attachments. Without regular staff training and security skills upgrading, company expenditures on the most sophisticated protection systems will be less effective.

A strong culture of cybersecurity resilience, including an informed and committed staff, creates an environment where peer behaviour reinforces positive security practices. In my experience, staff react positively to examples-based cybersecurity training. They lap up the narrative of cybersecurity incidents. They are intrigued by the technology of cyber offence and defence, and they respond well to being included as partners within the enterprise's cybersecurity effort. Cybersecurity can be professionally rewarding—and fun.

For some, however, it is more than fun. Another source of cyber attack is the trusted insider—a person who uses access to the company IT system either to steal proprietary information or to vent a grievance by disrupting or disabling the system. A combination of strong security controls, including access and usage monitoring, together with sound staff management practices, can help mitigate this threat.

10. Report breaches

While it is up to stock exchanges and governments to set rules for company reporting of significant cybersecurity breaches, it is important that anti-malware service providers and government cybersecurity agencies (e.g., CERT Australia) be informed of the nature

and extent of cyber attacks. Timely reporting assists the anti-hackers to develop and deliver new solutions to manage and neutralise malicious intrusions. In this sense, breach reporting is both an act of self-help and an important element of cyber resilience.

Cybersecurity: Here to stay

It has sadly proved a truism that the cyber attacker has managed so far to keep a step or more ahead of the cyber defender. No protection system or cybersecurity culture can guarantee absolute protection. But the adoption of the concept of holistic cyber resilience, which entails paying systematic and expert attention to cybersecurity, will substantially improve a company's chances of managing cyber risks and reducing the damage to a company's reputation, credibility, and the bottom line.

Responsibility and leadership: The sine qua non

Cyber attack is now a major strategic business risk, a constantly lurking vulnerability. Firms cannot rely on blind luck to avoid serious failures or disruptions of their systems caused by this new 21st-century phenomenon. Active strategic leadership by boards and CEOs, in close partnership with their CIOs, is the essential ingredient in the effective protection of the now ubiquitous, Internet-based, digitally reliant business model.

Strategies and technology are constantly evolving to detect, prevent, mitigate, or recover from potentially catastrophic cyber attack. It is the responsibility of boards and CEOs to proactively identify the risks and implement the most appropriate defence strategies. These strategies must focus not only on technology, but also, increasingly holistically, on the essence of an enterprise's culture, people, and processes.

To do otherwise would be derelict—and costly.

Works Cited

1. Juniper Research, 12 May 2015, Hampshire

7

Cyber Incident Management: Let the Data Tell the Story

Rachael Falk, Cyber Security Expert

Most companies already have a strategy for dealing with a crisis and, importantly, how communication with customers, regulators, and government should be handled. All CEOs and leadership teams are very familiar with dealing with ambiguity and making quick and considered decisions.

In cyberspace, the world is open for business 24/7, 365 days a year. Just as your business enjoys all the opportunities and ease of being connected, this also means that cybercrime, cyber activism, and cyber espionage can happen at a pace, scale, and reach that is unprecedented. Your organisation can have data stolen, disrupted, or destroyed in a matter of minutes.

There are many challenges in the minutes, hours, and days after a cyber incident. Companies now rely on supply chains to deliver their services, and this means that untangling a cyber incident can be complex. You may not have immediate access to the information needed, and may have to work across several time zones in order to understand the breadth of the incident. The impact of an incident can also be long lasting, and you may not know who has access to your valuable data, where it is, or what has been done with it until days, months, or even years later.

However, while the impact of a breach, disruption, hack, or attack may be severe, determining the root cause is something that's best done when all the data and evidence is available. Unfortunately, the availability of that evidence isn't always at the speed of cyber. It requires careful analysis and review, often by a team of incident responders and experts all working together behind closed doors.

It is entirely understandable to want to explain the nature of the breach or incident and what is being done or will be done to remediate the issue, but when it comes to any cyber-related breach, it is important to think about the need to balance notifying your customers and the market with making sure your statements are accurate.

For listed companies there are continuous disclosure obligations under the Corporations Act 2001 (Cth) and the ASX Listing rules, which mean that ASX-listed companies are required to disclose information that would reasonably be expected to have a material effect on the price or value of the securities (and that is a matter for the company to decide at the time in conjunction with its legal advisors). All companies must ensure that their statements are true and correct, and not just made in good faith. In any subsequent regulatory or legal investigation, all statements made by a company are required to be given as part of a submission of evidence, and they will be scrutinised by others, in the cold light of day, who will not be concerned with the tension and pressure that was felt by all in the actual Incident Management Room during those early hours/days.

To that end, rushing to get any explanation in a media release or TV interview because you believe that's what the market will demand—or that you need to fill the void with your narrative before the media makes one up—is a risky strategy. You will need to say something, but there is a difference between filling the void and acknowledging the incident. Eventually, you will need to acknowledge what has happened and what you are doing to understand what has happened.

There's no perfect timeframe to tell the world the full story (or a more detailed explanation), and there may well be operational security or other considerations that will mean you have been advised not to disclose details of the breach. But don't assume customers, regulators, or the world at large will simply forget about your incident. Full disclosure, once all the facts are known and you have gathered all the data you need, should happen as soon as possible.

However, the very nature of cyber means that guiding principles are necessary when determining how to inform all your stakeholders about a breach, but also how to inform them as more data is analysed and tells the story.

Some tips to keep in mind when setting the public strategy:

1. **It is fine to not know everything:** in fact, you will not know all the facts in the first 24 hours. Being comfortable with this ambiguity is important. Cyber incidents by their very nature are complex. Keep the pressure on your team but don't let the media cycle dictate what you say and how you say it.

2. **The truth is the best cover story:** there is no shame in admitting that your organisation does not know the root cause or extent of what has happened but will update customers and the market as soon as more information is available. You will preserve goodwill by being frank yet careful.

3. **Have someone in the room who is the detractor:** someone must play the role of questioning the story, the timeline, and asking 'why?'. This person plays a vital role in ensuring that the CEO—or whoever is the public face of the story—is comfortable and can explain the story in a cogent manner. Better you face challenges behind closed doors rather than provide a response under the pressure of media glare that you may then have to retract. This will undermine your personal and organisational credibility down the track.

4. **Have an executive lead the communications approval from a subject matter perspective:** and also decide who will be the media spokesperson. These may be different people. This should be an appropriate senior executive, but that person must be able to understand and verify the response. Importantly, this executive should not be approving anything that they can't explain, in plain English, to the CEO or the board of directors. This person can be the bridge between the technical Incident Responder team and the leadership team. You need to understand the who, what, when, where, and why in accessible English. That is the role of both the responsible executive and a good communications team.

5. You cannot control the narrative, but you can keep your core narrative consistent: the media will not always interpret and report in a way that you want, but that is their role. By being transparent and clear in all public-facing statements, you can keep your core narrative consistent. Expect questions and answer them in a considered way. Avoid putting an executive in front of the camera to read a prepared statement who then refuses to take questions. You will find that not only the incident but how you handled the incident becomes the story.

6. Resist the pressure to approve any statements because you are advised that you need to say 'something' about the incident: avoid statements or being drawn into questions about attribution and who might be behind the incident. This requires analysis done in slow time. Everyone loves the idea of a villain, but jumping to conclusions about a nation state or a hacker group does not achieve anything other than taking up valuable time. Remember, time will be in short supply.

7. Let the data tell the story, and don't fill the void with words like 'attack', 'hack' or 'cyber theft' until you know this is actually what happened: everyone gets very interested when these words are used. They are even more interested if it looks like you can't work out what exactly happened.

8. Correct inaccuracy in reporting or things that are just plain wrong: this is important so that you are not focused on having to go over something that is a red herring or a non-issue. Time is a currency you cannot afford to waste on cyber red herrings. Down the track in any litigation or regulatory investigation, it may mean you are forced to waste time and resources explaining why you didn't correct the record at the time.

9. Prepare for the breach now: have your team gather the media releases for the last 12 months from listed companies that had a breach, hack, disruption, or attack-style incident. Learn from what they did well and what you think could have been done better. Decide how you want your company to be perceived in the heat of crisis, and whether that perception is consistent with your company's values.

10. Have a good Crisis Management Plan and exercise it often: constantly rehearse this plan. There is a role for simulations or exercises, and you should practice different types of simulations. You must deliberately inject uncertainty into your simulation, as this will closely resemble what a realistic incident will be like. Equally important is making sure that you have the right team in your simulation. Nominate a leader and deputy, and ensure that the chain of command is in place to approve and manage your narrative when the world is moving at the speed of cyber. Make sure that the core team members have capable deputies who can step in during times of annual leave or illness. You want a solid, cohesive team managing the incident.

Conclusion

There is no perfect textbook way to manage a cyber incident, and you will, with certainty, never be able to please all your stakeholders as you move through managing and remediating an incident. However, controlling your core narrative in a way that is consistent with your company values, is honest and transparent but acknowledges the complex nature of cyber incidents, will allow you to maintain corporate credibility and focus on letting the data tell the story at a time when this matters most.

8

Activating Security Thinking Across the Enterprise

Commonwealth Bank of Australia — Ben Heyes, Chief Information Security & Trust Officer

During a recent visit to a security operations centre in Australia, my attention was drawn to a handwritten sign pinned on the wall.

> DAYS SINCE LAST INCIDENT: ~~30~~ 35

Was it a KPI? A morale booster for the incident responders? Or somebody's idea of Dilbertesque humour? I settled on the latter.

Organisations usually take somewhere between 100 and 200 days before they detect a network intrusion, according to the Ponemon Institute. So, while it might be 30 days since the last major incident about which this organisation knew, it could well be 130 days, and they just don't know it yet.

The discipline of cybersecurity is often characterised by attempts to conjure up something definitive in an environment plagued with uncertainty. Traditionally, the approach of securing the perimeter—or keeping the bad guys out—provided some satisfaction. A CISO could say for certain, when reading the logs, that a definitive number of malicious emails or web requests were blocked at the front door. But this gave no assurance of what was missed.

Organisations today operate in an environment that features a higher volume and severity of cyberattacks. In recent years, large organisations with well-established information security practices have been compromised by nation states (consider attacks on the Office of Personnel Management in the United States or Ukrainian power utilities), organised criminals (consider attacks on Target and J.P. Morgan), and hacktivists (consider the attack on TV5Monde).

Organisations themselves have also evolved such that the traditional network perimeter has all but dissolved. Commercial practices—including use of third parties such as cloud service providers—have blurred the boundary between what is inside an organisation's network and what is outside. It is no longer sufficient to frame the pri-

mary security objective as 'making sure bad guys don't get in'.

In this new and challenging environment, a CISO must do more than provide a strategic view of how best to protect the organisation. The role of the CISO is to activate security thinking across the enterprise.

So how do you transform an organisation with a 'good enough' information security function into one with a proactive, organisation-wide cybersecurity culture? While it's a task difficult to break down into a repeatable framework, these are some of the key ingredients:

Engage your leaders

The volume and scale of major data breaches has motivated boards and senior executives to seek stronger oversight of cybersecurity issues. This interest provides an unprecedented opportunity to advocate for an organisation-wide security culture.

In an environment where most organisations' interactions with customers are digital, cybersecurity is best presented to business leaders as an enabler of trust and brand. Security directly impacts how confidently customers engage with the organisation's services.

Boards and C-level executives, by their nature, are well grounded in how to measure complex and unpredictable risks. Further, they are each likely to have a broad range of prior experience drawn from a variety of disciplines from which cybersecurity problems can be considered. Sociology and psychology, for example, are as applicable to the cybersecurity issues of today as a deep knowledge of technology.

A CISO should be looking to frame conversations with these business leaders using a narrative that unlocks their individual interests and perspectives. With such a narrative established, the CISO can define a framework within which business leaders can actively relate to, digest, and own security decisions.

A threat-based approach

There are comprehensive cybersecurity frameworks available that can provide an exhaustive view of controls against cyber risks. Useful as they are, I have observed that wholesale adoption of these frameworks can lead to a 'one-of-everything' mentality that adds cost and complexity and commits your resources to dealing with relatively insignificant risks. Prioritisation of controls is markedly easier when thinking like an attacker.

Modern cybersecurity operations endeavour to be intelligence driven. This prioritises efforts and controls against recently encountered threats, as well as over-the-horizon threats the cyber intelligence function anticipates. While an intelligence-driven operation is far from a mature science in the corporate sector, it presents a useful approach to decision making.

A threat-based approach can address some of the aforementioned biases of information security towards protective technical controls. For instance, by recognising that attackers seeking to execute a network intrusion typically capitalise on an employee's lapse of judgment, we now pursue programs to enhance staff awareness, including running simulated social engineering or phishing attacks. Likewise, recognising the burgeoning grey market for vulnerabilities and exploits, we engage in penetration testing, objective-based testing, and application-security programs to provide assurance above and beyond patching processes.

Organisation-wide accountability

Central to driving organisation-wide accountability for security is having all parts of an organisation recognise their role in addressing cybersecurity risks. Establishing a mandatory baseline of security controls that apply to all critical systems in the organisation is an effective way to do this. (A critical system might be one that is Internet-facing or hosts customer data). It's vital that the business units that are accountable for these systems are also accountable for implementing these non-negotiable controls and for remedying any gaps or risks. This accountability can be driven by a board or executive mandate.

Ultimately, business units make better security decisions when they genuinely own the risk of non-compliance. Their buy-in is improved when they are provided incentives,

such as formalised access to security funding to remedy identified gaps, and discretion, such as owning the residual risk of non-compliance when circumstances permit (e.g., for systems due for imminent retirement, or for test systems that hold no customer data).

A security-conscious culture, where staff actively recognise their own responsibility for mitigating cyber threats, is equally critical. This is typically pursued via mandated cyber hygiene education, simulated phishing exercises, and a set of clearly articulated IT security policies. As we learn more about cybersecurity from behavioural sciences, I expect that security awareness programs will evolve significantly in years to come.

The extended enterprise

The connected nature of the Internet means that the fate of any one provider of digital services is intrinsically tied to the cyber capabilities of others. For instance, organisations with lax security whose websites are infected by malware designed to further infect the devices of any future visitors to the site are a risk to all other digital providers in the same market.

An organisation's supply chain is likely to exhibit an even greater degree of interconnectedness. Digital services offered to customers more than likely rely on Internet-hosted services supplied by third parties. It can also be practical for suppliers and partners to grant each other's staff authenticated access to assets within the network of the other. This can be a path to compromise. The startling breach of customer data from Target in the United States, for example, arrived via the compromise of an air-conditioning system supplied to Target by a third party, which was connected to Target's retail network for ease of billing. Similarly, breaches of U.S. government contractors ultimately handed attackers the credentials required to breach the U.S. Office of Personnel Management in 2015.

A CISO's focus thus needs to extend to influencing the security practices of suppliers and partners—whether by a direct set of minimum requirements asked of them in contractual negotiations, or indirectly through efforts to advocate for their own uplift in security capability via the sharing of knowledge, threat intelligence, or other resources.

Motivated and on a mission

Cybersecurity is maturing from point-in-time investments on perimeter security to the developing of operational teams in areas like assurance, awareness, and response. This cultural shift isn't possible without highly skilled and highly motivated staff. That's a challenge for many organisations, for two reasons.

First, we compete in a market where key technical talent has a choice of employers. And the task at hand requires the thinking of a broader set of people that haven't typically been employed in our sector: behavioural scientists, communicators, and creatives. A cybersecurity strategy needs to anticipate the needs of talent. It cannot afford to exclude the view of groups typically underrepresented by the information security discipline, or to sap the talent's creativity with undue process.

Also, top talent isn't always motivated by salaries alone. The ability to keep learning, or to impart their knowledge to others as educators or advocates, can also be a strong driver, as is providing them a strong sense of mission. There is more work to be done to refine operational models and build career pathways that account for and support these diverse needs.

Winning

The design of the Internet favours an attacker. The asymmetry between the cost of waging an attack and the cost of successfully defending an organisation has grown exponentially as attack surfaces grow larger and the tools available to an attacker become more sophisticated, affordable, and accessible.

In this landscape, the cybersecurity team doesn't get to enjoy a lot of easy wins. So it's important to celebrate those wins when they come along. It's equally important to champion new ideas—especially the radical ones—that challenge our preconceptions on how best to solve these problems.

Only then will we have a lot more to shout about than counting the days since the last incident.

SECURITY RESPONSIBILITIES – THE EXTENDED ENTERPRISE

GOVERNMENT & REGULATORS

- Recognition of shared responsibility for digital trust.
- Law enforcement.
- Investment in user awareness and skills development programs.
- Setting (voluntary) best practice frameworks.

SUPPLIER GOVERNANCE PROGRAMS

SUPPLIERS

- Contractual obligation to comply with cyber security requirements, particularly for systems or processes that store or transmit sensitive data.

BOARD AND EXECUTIVE	• Governance of security projects and policies based on risk management framework. • Cross-disciplinary guidance on cyber security challenges
CISO	• Activate 'security thinking' across the extended enterprise. • Define a framework through which the board and executive can relate to, digest and own security decisions. • Establish a mandatory baseline of security controls for cyber-critical systems
BUSINESS AND SYSTEM OWNERS	• Accountability for system compliance with mandatory baseline of security controls for cyber-critical systems, and mitigation of gaps.
STAFF	• Awareness and responsibility for personal cyber hygiene including use of organisation-owned systems and handling of customer data.

COMMUNITY OUTREACH PROGRAMS

CUSTOMERS

- Recognition of their role in a broader ecosystem of digital trust.

SUBSIDIARIES

9

Bridging the Cybersecurity Skills Gap

Australian Information Security Association
— Arno Brok, Chief Executive Officer

Almost every day, the media covers another massive data breach or cybersecurity incident. The reality is that cybercrime is now a $400 billion industry, and it's in hyper growth. Nevertheless, cyberattacks are becoming more and more sophisticated, yet we see sites being compromised because their owners didn't have even the basic security controls in place. Is this because of a lack of understanding, a shortage of experienced cybersecurity professionals, a lack of training, or a lack of funding? This chapter explores each of these interconnected issues, suggesting some means to tackle the problem nationally and internationally.

There are clear connections at play here. The need for increased security means that security specialists are more in demand, which in turn results in a skills shortage that directly impacts those organisations with the least ability to recruit and retain expensive professionals.

The issues involved are complex. We need to ensure that all of the stakeholders in the Australian economy (industry, government, and education) take appropriate security measures and contribute to the development of the information-security profession. Furthermore, we need to make sure that Australia has appropriate cyber defences, supported by a sufficiently experienced cyber workforce with the appropriate skills.

Cybersecurity skills shortage

The shortage of skilled and experienced cybersecurity professionals has been raised as a concern both internationally and within Australia. It is an issue that has been identified by the Australian government's new Cyber Security Strategy and raised independently by a number of key organisations in Australia. According to the Australian Department of Prime Minister and Cabinet, demand is expected to grow by 21% nationally by 2020, totalling around 9,100 cybersecurity jobs across the country.

The reality is that the cybersecurity industry has been aware of the shortage of security professionals for many years, but nothing has been done to fully quantify and address the problem. To remedy this, the Australian Information Security Association (AISA) has initiated a research project to better understand the extent of the problem in Australia and determine if it's related more to knowledge or to experience. We've tasked the research team to investigate whether there is a broad skills shortage or whether the focus should be on a particular demographic of the security community, such as senior management or risk specialists. Do all of Australia's states and territories have the same cybersecurity skills problems? We already know that some of these problems make the cybersecurity skills issue hard to quantify and, hence, difficult to address.

Cybersecurity career guide

A key finding of one of last year's studies was related to the lack of widely understood job roles within the cybersecurity workforce. As an example, analysis of a job seeking website, seek.com.au, showed that six jobs were advertised with six different titles, yet each of the hiring organisations was after the same skill set: i.e., a penetration tester. The lack of consistency in job-role definitions makes it difficult for employers to express clearly what they need applicants to be able to do, especially in terms of aligning skill sets and experience with what their organisation needs. The upshot is that employers continually complain about the number of job applications they receive for positions where the applicant doesn't have the necessary qualifications, skills or experience required to take up the role. Another consequence of this confusion is the lack of clear career paths for existing cybersecurity professionals. The security workforce doesn't have a clear guide illuminating how to progress from one level to another in their career, nor what their next role might be, nor the skills required for that position.

One of the first steps in solving these issues is to begin with defining the cybersecurity career landscape appropriate for Australia. Not all cybersecurity professionals want to be a chief information security officer (CISO), nor is CISO the only executive position; there are those who are considered peers, at the same level, with the titles of chief scientist or chief security architect. The important thing is that the career map fits the individual and recognises him or her as a senior member of the cybersecurity team.

Another way to help improve clarity around career paths in cybersecurity is for us to develop a professionalization programme for the industry. This is an area that has been identified as vital in solving the cybersecurity skills shortage and is key to the success of Australia's new Cybersecurity Strategy. It is critical to establish educational and support programmes as the basis for the national cybersecurity profession and to ensure solutions are provided for real problems that are fully understood.

The top of the pile

More often than not, hiring managers hold off for the perfect candidate. This panacea is almost always a pipe dream, and the position will go unfilled. As in most professions, there are superstars who are the leaders in their field, commanding superstar salaries and often spending their professional life on the conference circuit and in the media. The cybersecurity profession needs to ensure that we identify, nurture, and grow our superstars, offering our people challenging problems to solve in rewarding environments. Cybersecurity should be seen as an attractive career option for school leavers and college graduates so that it will be considered as 'cool' as (or cooler than) engineering, architecture, or the arts.

Rather than building a home-grown capability, many organisations poach from others. This creates a shuffling of the deck chairs across organisations without attracting new people. So, the question remains as to how we can be more innovative in meeting the growing demand for cybersecurity jobs? Why are we not adopting systems such as mentoring and job introduction that have worked in other industries for decades? For

example, if you want to become a medical specialist, you need to complete an internship, working alongside qualified professionals after you leave the university before you can practise on your own.[1] Cybersecurity should follow that same principle. Several organisations have strong graduate programmes, but they are more the exception than the rule.

Cybersecurity salaries

Salaries are another area with a marked divergence between the expectations of employers and those of cybersecurity professionals. With many in the security field aiming for the top 1% of professional roles—and the highest salaries in cybersecurity—AISA members have said they are not seeing attractive compensation packages from employers consistently across the market. Neither have we seen recruitment agencies head-hunting from overseas to fill Australian cybersecurity roles.

Cybersecurity is still not on the list for skilled migrants.[2] Being on the doorstep of Asia, with a large supply of skilled cybersecurity workers, this seems illogical. In recent years, Australia has lost cybersecurity experts to other countries, mainly the United States, where cybersecurity superstars can earn stratospheric salaries. If Australia wants to become the digital economy of Asia, we need to change tack. We need to make it attractive for our home-grown superstars to stay here, with effective incentives to attract overseas professionals to migrate to Australia, as well as incentivise the lower ranks of professionals to remain in the game and strive for greatness.

Workforce 2020

If we accept that there is a cybersecurity skills shortage in at least some demographics in Australia, we need to know what the country's future requirements look like before we can address the issues and devise a plan to solve them. Developing people with the knowledge, skills, and experience required to address the shortfall takes time and investment—possibly more than five years. This is one of the reasons the country is currently suffering a shortfall. At the moment, we don't know how many cybersecurity professionals we might need or what skills will be most important for the Australian economy by 2020. There are many global estimates, but none has been focused on the Australian market. We believe that further research in this area will help set realistic goals for policy makers to better understand recruitment requirements.

Convincing a lagging industry

A recent UK study, *Security Breaches Survey*,[3] showed that 87% of businesses experienced a cybersecurity breach in the past year. This is a rise of 10% from the previous year. One of the main issues is that small to medium-size businesses (SMBs) don't see cybersecurity as their problem. There is a disparity between the perception and the reality of security preparedness. Many SMBs believe that their security processes are optimised and their security tools are effective, while only their security preparations for managing incidents likely need improvement.

Mandating basic cybersecurity hygiene is essential to the success and longevity of these companies and to ensuring they can help drive an effective and efficient digital economy for everyone.

For basic cybersecurity hygiene, we refer to initiatives like the Cyber Essentials Scheme, which was developed by the UK government and industry to fulfil two functions:

- Provide a clear statement of the basic controls all organisations should implement to mitigate the risk from common Internet-based threats within the context of ten practical steps to cybersecurity; and
- An assurance framework that offers a mechanism for organisations to demonstrate to customers, investors, insurers, and others that they have taken these essential precautions.

Cyber Essentials offers a sound foundation of basic hygiene measures that all types of organisations can implement and build upon. Initiating similar measures in Australia could significantly reduce an organisation's vulnerability.

However, it does not offer a silver bullet to remove all cybersecurity risk, i.e., it is not designed to address more advanced, targeted attacks. Organisations facing these threats will need to implement additional measures as part of their security strategy. What Cyber Essentials does is define a focused set of controls that provide cost-effective, basic cybersecurity for organisations of all sizes.

Helping small businesses

AISA understands that implementing even basic security controls can be a major challenge for SMBs. We believe that the top end of the market will take on a significant portion of these trained workers. However, the majority should be deployed at SMBs with one clear objective: make Australia a Cyber Smart Nation. Australia's 200,000 small and medium enterprises[4] are the engine of the economy. We need to get them on board.

Organisations that provide cybersecurity services (consulting, security testing, and design) understand the importance of taking on cybersecurity trainees, as well as mentoring them for several years to transform them into well-rounded cyber professionals. They all understand that building cybersecurity capabilities needs to happen from the ground up. But many businesses are all too aware of the costs and risks of losing their well-trained cybersecurity professionals once they've learned the tricks of the trade. The phenomenon of lateral hiring is still prevalent and makes smaller organisations wary of the time and effort they are willing to invest in a trainee.

This is a big threat to developing a stronger trainee pipeline. If SMBs don't hire these workers to improve their cybersecurity capability, efforts to grow the trainee pipeline are doomed to fail.

Educating the young

We strongly believe that we can't start early enough with educating children in cybersecurity. Not only will this make them more aware of the Internet's security risks, but it will also lead them to consider career opportunities in cybersecurity the norm at a very early age. As an industry, we will jointly have to develop material that speaks a language that both parents and children understand.

Conclusion

Without consensus and collaboration, the onslaught of breaches at corporations and threats to critical infrastructure will continue to escalate. If current trends continue, it is likely we won't have the right sort of cybersecurity professionals by 2020. The cybersecurity skills shortage will become more visible and more problematic than many seem to realise. To keep pace, we need to mature the cybersecurity profession into a proactive, not reactive, model.

For AISA, it is very clear that this challenge cannot be solved by one single entity. It must be an industry-wide collaboration. AISA believes that bringing together key stakeholders from the public and private sectors around Australia is imperative to finding a common solution for this shared problem.

AISA is Australia's primary information security professional body, representing a member base of over 3,000 cybersecurity professionals from a diverse set of business, government and academic markets.

Works Cited

1. https://ama.com.au/careers/becoming-a-doctor#five
2. http://www.border.gov.au/Trav/Work/Work/Skills-assessment-and-assessing-authorities/skilled-occupations-lists/SOL
3. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/191671/bis-13-p184es-2013-information-security-breaches-survey-executive-summary.pdf
4. From: In June 2015, 61% of actively trading businesses in Australia had no employees, 28% had 1-4, 9% had 5-19, 2% had 20-199, and less than 1% had 200 or more. In June 2015, the number of actively trading businesses in the market sector was 2,121,235

10

Decoding Tomorrow's Economy: Cybersecurity, the Internet of Things (IoT), and the Fourth Industrial Revolution

Data61 – Adrian Turner, CEO

Innovation potential

We are moving quickly to a world where everything with a circuit board and power supply will connect to the network. Some estimates suggest there will be as many as 200 billion connected devices by 2020,[1] with the goal of creating new services, economic structures, and operational efficiencies. The Internet of Things (IoT) is a term used to describe previously non-connected devices, like fuel gauges and elevator control systems, being fitted with data transmitters to enable control from anywhere on the local network or even the global Internet. IoT is here today and is being used to create sustained competitive advantage as its economic impact begins to take shape. The so-called 'fourth industrial revolution' will place information systems and automation at the centre of productive output—from driverless cars to robotic process automation.

For individual corporations, new avenues for growth are at stake with IoT, but along with this opportunity comes new risks and responsibilities—and new security challenges. Company executives and board members who don't take the time to review and understand this current shift towards their industries being connected and data-driven risk obsolescence. Those who do so have the potential to achieve extraordinary shareholder returns.

The IoT security imperative

According to a recent report published by the World Economic Forum (WEF),[2] executives list cybersecurity breaches as their primary IoT concern, followed by personal data breaches. Security considerations for IoT systems are very different than for other IT systems. Where IT refers to information technology systems, IoT systems are supported by OT, or 'operations technology'. IT systems are composed of servers, storage, and software, which run business information processes. OT systems are industrial components designed for managing operational

processes like temperature and pressure settings and material production flow. IT systems are mission critical; OT systems are often life critical.

Rod Beckstrom, former director of the National Cyber Security Center (within the United States Department of Homeland Security), published a law related to IoT security that brings the need for IOT security into focus. Simply stated:

1. Anything attached to a network can be hacked;
2. Everything is being attached to networks, therefore:
3. Everything is vulnerable.

Enormous value can be created through connectivity, but it has to be done with the understanding that no connected systems are completely secure today.

Due to the scale of IoT deployments, to realise the benefits of connectivity, automation is fundamental. And automation cannot occur if the underlying data can't be trusted—cybersecurity now underpins the ability to automate. In this sense security is not an IT or OT issue, it is a business continuity issue.

In an industrial context, cybersecurity also translates to safety issues. If a function of a device is compromised, it has the potential to malfunction. This was the case in Germany, where industrial equipment was compromised in a steel factory, causing a fast shutdown of a furnace and resulting in extensive damage. It is unusual for such systems to be directly connected to the Internet, but it does happen, and IoT is set to make this much more common. These incidents ultimately highlight the need for greater emphasis on data security and data integrity in the IoT economy.

Key IoT security considerations for company boards

Below is a checklist of considerations and questions for company boards to help members capitalise on the massive emerging opportunities around IoT while minimising the risk of cybersecurity breaches.

1. Recognise there is a real and present threat

Company boards need to recognize that the threats are real and they are present today. Business drivers will mean more connected devices, but there are already documented cases of breaches causing physical damage, in addition to economic and reputational damage. And just because there is no evidence of a breach, that does not mean your systems are secure. The threat landscape is evolving exponentially, and it is important to understand the motives of external actors and recognise that the majority of incidents still come from errors by internal teams. The full spectrum of threats and disruptions include: unauthorized access; technology failure; malicious attacks; espionage; sabotage; criminal activity; natural disasters; and human error. Any connected device has potential to be an attack vector—including seemingly innocuous devices like printers.

2. Elevate the discussion to the board level

IoT security should be discussed with the board. While the technologies might be complex, the principles are not—in a network, the whole system is only as strong as the weakest link. This could be the people, the network, or the individual devices. Discuss corporate cybersecurity communications methodologies and cadence with the board, and stay on top of current IT security trends. One way to look at this is by redefining the chief information security officer (CISO) role. Create a reporting structure whereby the CISO oversees both IT and OT security. Also, create an exchange program across the functional teams in the organisation and frame both functions as business functions first, equally fundamental to business continuity. Recognise that in a networked world trust is the most valuable currency. Have the CISO also own trust, as it relates to trustworthy devices, customer and partner interactions, and the organisation's brand. The board will then have an understanding of the importance of IoT security and a 'go-to person' for regular updates.

3. Take a holistic approach

While IT and OT are very separate functions today, they will converge. Emphasis needs to be placed not just on trying to prevent breaches with cyber hygiene, but also on risk management and resilience. Review the device topology of the corporation; the risk profile and the context of the connected equipment; the networks devices connect to; the people who use them; and the value of the data collected and systems that protect it. Then there will be a more unified approach to security and less finger-pointing in the event of a problem.

4. Communicate a business continuity plan

Breaches will happen, so be prepared for them, both internally and across your value chain. Be clear on disclosure policies and practices, and have a communication plan prepared now. Also, have a business continuity plan for employees, partners, and customers to minimise the impact of a breach.

5. Understand business context and risk tolerance

Discuss and agree on the risk profile and tolerances of the organisation as it relates to both IT and OT relative to the wider business requirements. Openly discuss the type of devices connected to the network and the data being collected and shared, including who has access to what data. This should be an ongoing process resulting in identification of the risks and the steps to mitigate them.

6. Create a strong security model for connected devices

Ensure that all IT and OT systems are properly patched. In the world of IoT, patching tends to be spotty at best. There can be underlying concerns that patches might disrupt the operation of the connected device or system; however, this is short-sighted. Ensure connected devices have hardware-based roots of trust wherever possible and certificate-based authentication for device identity. Some devices still ship with the same hard-coded crypto keys or passwords, introducing a known vulnerability. In addition, ensure the remote management interface to devices is secure, and access to the devices and associated data is controlled.

7. Monitoring for rapid response and recovery

Ensure the mechanisms are in place for ongoing monitoring of OT environments for rapid response when breaches occur. It is best to assume there will be breaches, and that these can be difficult to detect, given some IoT devices don't have visual displays and are not designed for direct human interaction. Don't underinvest in response systems. Participate in government and community cybersecurity auditing programs like the ASIC cyber resilience check program in Australia.

8. Focus on data protection and privacy

With IT systems, data confidentiality, integrity, and authentication are most important—in that order. With IoT systems, the importance is reversed to be authentication, integrity, and confidentiality. There will also be an increased emphasis on data authentication and integrity, as it is fundamental to automation. There will also be a move to allow more granular access controls to device data. Understand how data is collected and where it is stored, either locally or in the cloud. If data is stored in the cloud, ensure it is compliant with regional requirements for in-country data storage where applicable. Instil a privacy-first culture to become a strong custodian of the data you collect and not overreach with data-access policies.

9. Supply-chain integrity, information, and risk sharing

Global supply and value chains are increasingly demanding that participants be secure. Many multinationals are already forcing security audits of partners in order to collaborate, transact, and share data. For connected equipment, understanding the provenance of the hardware and software is important. It is also important to understand—and have common mechanisms for—reporting on the protective provisions in the license agreements for cybersecurity products and services that connect to your network, as well as for the components that are licensed into the connected products and services that you sell. Be aware that these protective provisions are often not as robust

as expected; you may have large exposures that you are currently unaware of.

10. Join government collaboration networks

The Australian government recently announced the creation of a Cyber Security Growth Centre, a new program that will be Australia's peak industry-led cybersecurity body. It will take the form of a national network and drive alignment among industry, government, and academia to help create a vibrant domestic cybersecurity sector. All Australian companies who are concerned about cybersecurity should consider participating in this network. It will include programs like the development of a cybersecurity curriculum for company directors.

Cybersecurity key to connected economy

Every Australian company will be competing with IoT platforms and applications in the near future, and the best will proactively seek to create them for themselves. There's no escaping the reality that these emerging platforms will include connectivity of people and devices, with different security priorities from today's IT systems, including an increased emphasis on operations technology. OT security is becoming an imperative if organizations are to survive and thrive through this digital transition.

For Australian companies and directors, this means they must move quickly to understand the dynamics described in this chapter and to ensure their organisations have the right security posture, processes, and controls that align to its risk profile. Platforms can scale quickly, but at their core is trust, which can be eroded equally fast. If Australian companies are to participate in the global digital economy, connected to many third-party platforms and ecosystem participants, strong and compliant security will be a prerequisite. Take the time to consider the items outlined here to help protect your business and capitalise on the opportunities presented by IoT. This list should be the start of a comprehensive cybersecurity risk and compliance program, overseen at the board level.

Works Cited

1. Intel: http://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html
2. WEF: Unleashing the Internet of Things Report

Contributor Profiles

Forbes

Forbes Media

BRUCE H. ROGERS

Chief Insights Officer and Head of the CMO Practice

Bruce Rogers is the Chief Insights Officer for Forbes Media, responsible for managing the Insights division, which creates and distributes thought-leadership, research-based content for blue-chip customers such as IBM, Google, KPMG, SAP, CIT, and Deloitte. Bruce also oversees the Forbes Insights content channel on Forbes.com, and writes a column for Forbes where he profiles thought leaders changing the business landscape.

Bruce is also the Head of Forbes' CMO Practice, overseeing the group's creation of content through the Forbes CMO Network section of Forbes.com, and events such as the annual Forbes CMO Summit. Under his guidance, the CMO Practice recently released an in-depth report entitled, "Publish or Perish: A CMO Roadmap to Managing, Systematizing and Optimizing the Marketing Content Supply Chain".

Prior to this role, Bruce was the Chief Brand Officer, responsible for all integrated marketing, brand communication, research, and sales support activities for Forbes Media.

From March 2000 to October 2008, Bruce was the Vice President of Marketing for Forbes.com. In this position, he was responsible for developing and implementing marketing strategies and programs to build the Forbes.com brand, drive consumer traffic, create customer acquisition and retention programs, as well as initiate research and promotions in support of advertising sales. During his tenure, Forbes.com grew from under 500,000 to 20 million unique monthly visitors.

From 1992 until March 2000, Bruce served as Vice President, Worldwide Marketing Communications for Forbes Inc. In this capacity, he oversaw brand building for the company. He directed marketing efforts for Forbes' growing publishing assets and was directly responsible for Forbes.com's and Forbes magazine's advertising campaigns. In this role, he inaugurated Forbes' signature "CEO Profiles" ad series, which in 1995 won a Gold EFFIE award from the American Marketing Association.

Bruce serves as the President of the Business Marketing Association of New York and is a board member of the Media Ratings Council and the advisory boards for SBV Capital, Adtech, and BPA (Business Publishers Association).

He is the co-author of "Profitable Brilliance: How Professional Services Firms Become Thought Leaders" as well as the previously published, "In the Line of Money: Branding Yourself Strategically to the Financial Elite".

He has a BA in Human Communication from Rutgers University and resides in Waldwick, New Jersey, with his wife and their two children.

Palo Alto Networks Inc.

SEAN DUCA

Vice President, Regional Chief Security Officer

Sean is the Regional Chief Security Officer for Asia Pacific at Palo Alto Networks, where he works on the development of thought leadership, threat intelligence, and security best practices for the cybersecurity community and business executives.

With more than 18 years of experience in the IT security industry, he acts as a trusted advisor to organisations across the region, helping them improve their security postures and align security strategically with business initiatives.

Prior to joining Palo Alto Networks, he spent 15 years in a variety of roles at Intel Security, with his last position as the Chief Technology Officer for Asia Pacific. Before this, Sean was involved in software development, technical support, and consulting services for a range of Internet security solutions.

Sean actively discusses security issues in mainstream media, including television, radio, print, and security-related broadcasts. He regularly participates in forums, conferences, and panels, and provides intelligence on cybersecurity matters to the public and private sector.

Australian Government

THE HON DAN TEHAN MP

Minister Assisting the Prime Minister for Cyber Security

The Hon Dan Tehan MP is the Member for Wannon in Victoria. He became the Minister for Veterans' Affairs, Minister for Defence Personnel, Minister Assisting the Prime Minister for Cyber Security, and Minister Assisting the Prime Minister for the Centenary of Anzac on 27 July, 2016.

He previously served as Minister for Veterans' Affairs, Minister for Defence Materiel, and Minister Assisting the Prime Minister for the Centenary of Anzac from 18 February, 2016.

Mr Tehan was elected to Federal Parliament in 2010 and has held positions as the Chair of the Parliamentary Joint Committee on Intelligence and Security; Chair of the Victorian Consultative Panel for the Black Spot Programme; Chair of the Coalition Policy Committee on Economics and Finance; Co-Chair of the Parliamentarians Supporting Cancer Causes; Co-Chair of the Parliamentary Friends of Youth Mental Health; and Chair of the Coalition Friends of Tourism.

Mr Tehan has also held positions on the House of Representatives Standing Committee on Regional Australia; the Standing Committee on Agriculture, Resources, Fisheries and Forestry; and the Joint Human Rights Committee.

Prior to entering Parliament, Mr Tehan worked at senior levels of the Australian Government, including as a Senior Adviser to the Deputy Prime Minister and Chief of Staff to the Minister for Small Business and Tourism. He worked as the Director of Trade Policy and International Affairs at the Australian Chamber of Commerce and Industry, Deputy State Director for the Victorian Liberal Party, and in the Department of Foreign Affairs and Trade, where he held various roles, including as a diplomat at the Australian Embassy in Mexico. Mr Tehan worked in agriculture in Australia and overseas and has Masters Degrees in International Relations and Foreign Affairs and Trade.

Mr Tehan lives with his wife Sarah and their family on a small farm on the outskirts of Hamilton. He is a passionate supporter of the Richmond Football Club and enjoys spending time outdoors with his family and their increasing number of pets.

Australian Cyber Security Research Institute

DAVID IRVINE

Chairman

David Irvine is unique in the history of Australian intelligence, a long-serving diplomat who subsequently became the only person to have served as the head of both Australia's foreign intelligence collection agency and its domestic security agency – positions he held for almost 12 years.

Irvine was Australian High Commissioner to Papua New Guinea during a particularly turbulent period from 1996-1999 and Australian Ambassador to the People's Republic of China between 2000-2003, when he was also concurrently Australian Ambassador to Mongolia and to the People's Democratic Republic of Korea.

David Irvine is a graduate in Arts from the University of Western Australia. He has an honorary Doctorate of Letters from that university and an honorary Doctorate of Science from Edith Cowan University.

He is a member of the Advisory Council of the National Archives of Australia and a member of the Foreign Investment Review Board.

He currently lectures at the National Security College within the Australian National University and is Chair of the Board of the Australian Cyber Security Research Institute.

Irvine has published two books on Indonesian culture.

Australian Information Security Association

ARNO BROK
CEO

Arno is a former AISA Board executive and held the position of AISA National Director from 2013-2015. Arno was vital in defining the strategy for AISA to advance from an association purely for information security professionals to one where all individuals, businesses, and governments are educated in the risks and dangers of cyber-attack and data theft. Arno has been driving the strategy towards a sustainable association and further transforming AISA into the peak body for cyber professionals in Australia, with the objective to grow cyber security capabilities to really become a cyber smart nation.

Arno is an excellent motivator and facilitator. His strengths lie in his ability to communicate complex information security issues with a positive 'can-do' attitude.

As the first appointed CEO of AISA, Arno Brok is committed to delivering value to its members, the community, and the cyber security industry.

Australian Strategic Policy Institute

TOBIAS FEAKIN
Founding Director

Tobias joined ASPI in October 2012. He is Director of National Security Programs, coordinating all of the Institute's work in this space. He examines issues relating to national security policy, cyber security, global counter-terrorism, resilience, and critical infrastructure protection. He established the International Cyber Policy Centre at ASPI in 2013 and is Director of the Centre. In this role he researches how cyberspace is used for nefarious purposes, by state and non-state actors, creating collaborative policy responses, and creating national and international cooperation in cyberspace. His latest research examines Asia-Pacific Cyber Maturity and state responses to cyber incidents.

In 2014 he was appointed by the Australian Prime Minister to be part of the 'Independent Panel of Experts' to the Australian Cyber Security Review. He is an Oxford Martin Associate of the Devising Cyber Policy and Cyber Defence working group at the Oxford University

Global Cyber Security Capacity Centre, and a Research Advisor for the Global Commission on Internet Governance run by Chatham House.

He has worked as a Research Fellow for the Landau Network, Centro-Volta in Italy, and the UK Home Office. He was previously Senior Research Fellow and Director of the National Security and Resilience department at the Royal United Services Institute for Defence and Security Studies, in London, and is still Associate Fellow of RUSI.

Business Council of Australia

JENNIFER WESTACOTT

Chief Executive

The Business Council of Australia is an association of chief executives from many of Australia's leading companies. It was established in 1983 to research and promote economic growth policies for the benefit of the nation and all Australians.

Jennifer Westacott has been Chief Executive of the Business Council of Australia since 2011, bringing extensive policy experience in both the public and private sectors.

For over 20 years Jennifer occupied critical leadership positions in the New South Wales and Victorian governments. She was the Director of Housing and the Secretary of Education in Victoria, and most recently was the Director-General of the New South Wales Department of Infrastructure, Planning and Natural Resources.

From 2005 to 2011 Jennifer was senior partner at KPMG, heading up the firm's Sustainability, Climate Change and Water practice and its NSW State Government practice. Jennifer was also a board director for the firm. During her time at KPMG, Jennifer advised some of Australia's major corporations on climate change and sustainability matters, and provided advice to governments around Australia on major reform priorities.

Jennifer facilitates the contribution of the Business Council of Australia's CEO members across a policy agenda that includes economic policy and competitiveness; regulation; infrastructure and sustainable growth; labour market, skills and education; engagement with Indigenous Australians; global engagement; healthcare policy; and innovation.

Jennifer coordinated the development and release of the BCA's landmark *Action Plan for Enduring Prosperity* in 2013, which is widely recognised as one of the most significant contributions to economic policy debate in Australia in recent years.

Jennifer has a Bachelor of Arts (Honours) from the University of New South Wales, where she is an Adjunct Professor at the City Futures Research Centre. She was a Chevening Scholar at the London School of Economics.

Jennifer is a National Fellow of the Institute of Public Administration Australia and a Fellow of the Australian Institute of Company Directors, and since 2013 has been a Non-Executive Director of Wesfarmers Limited and Chair of the Mental Health Council of Australia.

Commonwealth Bank of Australia

BEN HEYES

Chief Information Security & Trust Officer

Ben is the Chief Information Security and Trust Officer at the Commonwealth Bank of Australia (CBA), which is Australia's leading provider of integrated financial services and is widely recognised for its technology leadership and banking innovation. CBA is also the tenth-largest bank in the world by market capitalisation and has operations in Indonesia, China, Japan, India, Vietnam, New Zealand, Europe, and the United States. In his role, Ben is responsible for ensuring the security of the Group in the face of a rapidly evolving cyber security landscape, for operational risk of the group's technology environments and for digital trust and privacy.

Ben is passionate about the possibilities of technology and their application to societal enhancement and trust in the digital economy. He believes in creativity, innovation, and the application of both art and science.

Prior to CBA, Ben held leadership roles in a number of the world's leading financial service providers, including NAB, Deutsche Bank, and UBS, in a career that saw him work across Europe, Australia, and America. Prior to financial services, Ben spent six years working in various technical and liaison roles in national security and foreign intelligence.

Ben holds a Bachelor of Computing and Computer Science and a Masters of Law in Technology Law. He is also a non-executive director of The Conversation, a media company; and Chairman and non-executive director of CREST Australia, a not-for-profit company focused on defining and ensuring high standards for Ethical Security Testers.

Data61

ADRIAN TURNER

CEO

Adrian Turner is the CEO of Data61 at CSIRO. Data61 is creating our data-driven future.

Adrian is a successful and influential Australian technology entrepreneur who has spent 18 years in Silicon Valley. Most recently he was Managing Director and Co-Founder of Borondi Group, a holding company focused on the intersection of pervasive computing, platform economics, and traditionally conservative industries.

Prior to this, Adrian was co-founder and CEO of smartphone and Internet of Things security company Mocana Corporation, had profit and loss responsibility for Philips Electronics' connected devices infrastructure, and was Chairman of the Board for Australia's expat network, Advance.org. He was recently named Co-Chair of the Cybersecurity Growth Centre, is a member of the Board of the Australian eHealth Research Centre, and is also a member of the UTS: Business School Advisory Board.

He is regarded as a thought leader on entrepreneurialism, the Internet of Things, and the impact of network connectivity on business economics. He authored the eBook *Blue Sky Mining: Building Australia's Next Billion Dollar Industries.*

KING&WOOD
MALLESONS

King & Wood Mallesons

CHENG LIM

Partner

Cheng is the leader of King & Wood Mallesons' Global Cybersecurity team and was instrumental in developing KWM's '7 Pillars of Cyber-Resilience'. He has worked extensively in the field of data security, data breaches, and privacy for the last 20 years.

Cheng specialises in helping clients navigate complex legal, commercial, and regulatory landscapes in telecommunications and technology. In 2014 and 2015, he led the teams advising Telstra on a number of major renegotiations of its landmark agreements with NBN relating to the rollout of the NBN network. In 2015 he was named by Best Lawyers as Telecommunications Lawyer of the Year, while in 2016, he was named by IT as IT Lawyer of the Year.

Telstra Corporation Limited

MIKE BURGESS

Chief Information Security Officer

Mike Burgess is Telstra's Chief Information Security Officer and has led Telstra's Security Operations group since 2013.

Mike is known for his thought leadership and visionary approach to cyber, establishing the unique Discovery and Influence capabilities, which play a critical role in protecting customer and corporate information. Mike is also the co-author of the Five Knows of Cyber Security, a well-recognised and often referenced approach that can be used to effectively manage cyber security risk from the Board down.

Before joining Telstra Mike was the Deputy Director for Cyber & Information Security at the Australian Signals Directorate (ASD), the Commonwealth authority on information security. Mike's leadership was critical in addressing the increasing challenge of securing Government information against unauthorised network intrusions.

During his tenure at ASD, Mike led the establishment of the Cyber Security Operations Centre (CSOC) and oversaw its development into a key cyber capability for Government. The CSOC brought together capabilities from across Government to deliver a greater understanding of the cyber threat against Australian interests, and provided response options for significant cyber events across government and systems of national importance.

Mike's early career established a strong, broad technical base for his more recent leadership roles. Mike worked in private industry before joining the Defence Science and Technology Organisation in the field of imaging radar. He then joined ASD as a collection engineer in 1995 and went on to hold a variety of roles spanning the intelligence, security, capability development, and executive aspects of ASD's business.

RACHAEL FALK
Cyber Security Expert

Former GM, Cyber Influence, Awareness & Threat National Security Advisor, Telstra

Rachael is the co-author of the Five Knows of Cyber Security, a well-recognised and often referenced approach that can be used to effectively manage cyber security risk from the Board down. Most recently, she was the General Manager leading Telstra's Cyber Influence team. This capability is responsible for raising awareness on cyber security issues and ensuring that cyber security is front of mind for all 35,000 Telstra staff.

Prior to making the move into cyber security, Rachael practiced as a lawyer for 15 years both at Telstra and with leading law firms both in Australia and overseas.

Rachael has a keen interest in legislative and policy issues surrounding cyber security and has just completed an Advanced Masters in National Security Policy with the National Security College at the Australian National University (ANU).

Rachael also holds a Bachelor of Arts from the ANU and Bachelor of Laws (Hons) from the University of Technology (Sydney).

Individual Contributor

MAJOR GENERAL STEPHEN DAY (RETIRED)
DSC

General Stephen Day recently transitioned from the government to the private sector after completing his appointment as Head of Cyber at the Department of Defence and as the inaugural Head of the Australian Cyber Security Centre. His principal task was to lead the whole government team responsible for protecting Australia's national security and economic prosperity from the threat through cyber. During his tenure, the success of cyber-attacks against the national government was reduced by 75%. He organised and participated in crisis exercises in Australia and the US to test response plans for a variety of crises triggered by cyber-attack. He briefed the Prime Minister's 2015 summit on cyber security, attended by the Chairs and CEOs of 20 of Australia's leading companies. He is a frequent public speaker on cyber security in Australia as well as in NZ, the UK and the US. He advises Government Departments, boards and executives on the nature of the threat and what to do about it. He is the Chair of the Advisory Board to the University of New South Wales Centre for Cyber Security.

CONTRIBUTORS

- **The Honourable Dan Tehan**
  Member of Parliament
- **Bruce H. Rogers**
  Forbes
- **Sean Duca**
  Palo Alto Networks
- **Mike Burgess**
  Telstra
- **Rachael Falk**
  Cyber Security Expert
- **Jennifer Westacott**
  Business Council of Australia
- **Stephen Day**
  Retired Major General
- **David Irvine**
  Australian Cyber Security Research Institute
- **Arno Brok**
  Australian Information Security Association
- **Ben Heyes**
  Commonwealth Bank of Australia
- **Cheng Lim**
  King & Wood Mallesons
- **Tobias Feakin**
  Australian Strategic Policy Institute
- **Adrian Turner**
  Data61