The new equation to protect Australia's critical infrastructure

February 2022

Digitisation has transformed our lives and the way we work. It provides boundless economic and social benefits to Australians but it also exposes our nation and our critical infrastructure to unprecedented and increasing risks created by cyber criminals. No critical service exists today that does not rely on digitisation, making us all vulnerable.

Although efforts are underway to increase our cybersecurity through regulations and government assistance, no overarching strategy currently exists. If we can cut through the myriad of conflicting guidance, and directly address this challenge, Australia has the opportunity to become a global leader in setting standards and frameworks.

The pressing need to address cyber risks was highlighted in PwC's 2021 Global Digital Trust Insights Survey of more than 3,200 businesses which reveals 60% of C-suite executives anticipate cyber crime will increase in 2022.

The impact of that crime on business will be far reaching. While more than 50% of those Australian's surveyed in our recent Community Attitudes survey said they had confidence in the ability of essential service providers (water, telecommunications, banking, electricity and major logistics facilities) to stand up to cyber threats, 80% said they would stop using a supplier if their data was stolen or provided without their consent, for example during a ransomware attack.

Overwhelmingly, Australians want greater certainty and trust. Close to one in three individuals surveyed said they would not trust a foreign entity to act responsibly with their data, and were concerned about non-Australian-owned businesses operating essential services.

The challenge for government, industry and our community is to manage the risk posed to critical infrastructure to improve collective security with minimal impact on an already burdened set of industry sectors.

60% of executives anticipate cyber crime will increase in 2022, while

80% of Australians will stop using a supplier if their data is stolen

Rising threat level

Geopolitically, Australia is operating in an increasingly rough neighbourhood. Cyber attacks, including those instigated by state-backed actors are a primary source of concern.

According to the latest Australian Cyber Security Centre (ACSC) Cyber Threat Report[1], an attack was reported every eight minutes in 2020-21, a 13% increase in just one year. These attacks were estimated to cost Australian businesses over $33 billion a year.

Attacks to Australian businesses result in loss of income, personal data and sometimes intellectual property and as such they represent a burden to the Australian economy. Arguably more serious - with the ability to present a threat to life is the threat to our critical infrastructure operators who provide our essential services - water, energy, transport, food and grocery and health services amongst others. The vulnerability of Australia's critical infrastructure is a pressing concern for the Department of Home Affairs.

Operators on the frontline of these attacks have seen their annual cybersecurity spend increase by 500% in some instances, spending in the magnitude of $20 million to reduce their risk rating from catastrophic to medium. Highly regulated industries will recoup these costs from the government. But at the end of the day, consumers will pay.

In October 2021, bipartisan support allowed the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (SLACI 2021) to be fast-tracked through parliament and enacted in December 2021. This legislation allows the Federal government to take control of critical infrastructure in the event of a cyber attack that poses a threat to national security.

A second bill, the Exposure Draft Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022, to be tabled in Parliament in February 2022 proposes a number of requirements for security practices by critical infrastructure operators. This approach will be led by a risk management program which will call for critical infrastructure entities to produce a board-level attestation of their risk management planning currency.

[1] Australian Cyber Security Centre Annual Cyber Threat Report 2020-21

Rising threats to critical infrastructure

For the first time, many sectors are converging their information technology (IT) systems with operational technology (OT) systems[2] meaning an attack on a billing system can take an oil pipeline offline.

We are nowhere near as resilient as we need to be. Implementing the latest cybersecurity standards in a 25-year-old plant or ageing technology system is immensely challenging.

While cyber threats have increased exponentially, the COVID-19 pandemic has exposed supply chain vulnerabilities. For example, an attack on a transport operator can impact food and medical supplies or even disrupt a nation's defence capability.

As the ACSC report states, the pandemic has been a boon for cyber criminals. The rapid digitisation of government services, work, shopping and education has encouraged the illegal activities of both state actors and a new breed of cybercriminal lured by the opportunity to make relatively easy money out of extortion-based cyber-crime. Using readily available cybercrime services, these criminals are often based in regions suffering severe economic downturn.

[2] Building cyber resilience in critical infrastructure, PwC Australia, 2021

Legislation, complexity and compliance

The government's awareness of these risks prompted the recent move to amend existing legislation. SLACI 2021 and the attendant legislation currently in development, introduce security obligations for finance, communications, data storage and processing, defence, education and research, food and grocery, health, space, and transport. This is a first for many sectors and they will need to move quickly to achieve the level of protocols and systems that banks have achieved over the past two decades.

Although the government is adopting a principles-based approach, compliance doesn't equal security, and there are inherent risks in being too prescriptive and punitive. **An overly prescriptive model could potentially push companies into a position where they can not comply, do not want to wear the liability, can not afford to improve their risk management practices, and so stop reporting attacks.**

However, in order to cut through ambiguity and standardise reporting, there remains a need to be prescriptive about critical infrastructure related threats or incidents. Even then, the identification and categorisation of an incident is likely to vary from company to company and even asset to asset. Even where there may be no adverse impact on a business operations, there may still be a threat.

Complicating this issue is the significant complexity in defining and reporting an incident.

Determining what constitutes a cyber event is not straight forward. There may be many interpretations of what constitutes such an incident or evidence of an incident. A central issue is adverse impact. If, for example, a company does not experience a detrimental impact, it may not consider it is dealing with a cyber incident. Yet many actors may use an entity as an access point and not cause damage. Examples are already emerging of entities using loopholes around the definition of evidence, or the ability to find it, to avoid reporting cyber breaches.

How regulators respond to breaches and treat reported data will have a big impact on industries' confidence to have transparent conversations. This in turn will impact the ability of policymakers and regulators to obtain feedback on which rules are based. Where the aim is to make organisations more resilient to attacks, there is a lot to be gained by regulators showing preference for constructive discussion rather than resorting immediately to litigation or threats of litigation.

A major drawback of the new legislation is how light it is on detail. This makes it difficult to ascertain what the specific ask is of industry, and has led to widespread concern about how to comply. **PwC's 2022 Global Digital Trust Insights Survey[3] found regulatory compliance rates are the second highest priority for Australian CEOs in the design of their cyber strategies. Their global counterparts rank it last.**

While directors and executives sort through whether SLACI applies to them, and how it will be applied, they are increasingly concerned about how it intersects with parallel guidance on cybersecurity from authorities and regulatory bodies.

[3] PwC's 2022 Global Digital Trust Insights Survey

Decluttering regulation

The Australian Competition and Consumer Commission is using its powers to get more bullish in this space, while the Australian Prudential Regulation Authority has flagged increased audit activity. All eyes are on the Australian Securities and Investments Commission's current litigation activity to see whether it takes a more consistently litigious approach to dealing with cyber breaches.

Labelling for digital products and services that hold manufacturers accountable for a reasonable level of embedded cybersecurity has been tabled as an option. And there is ongoing debate about whether the Corporations Act should explicitly call out cybersecurity or if the definition of a fiducially responsible director and reasonable preventative steps, sufficiently incorporates it.

There are at least 26 pieces of regulation governing cybersecurity, from global mandates such as the EU's General Data Protection Regulation, to national, state and industry specific rules.

All this points to an opportunity to de-clutter, align and simplify requirements and expectations.

The business community needs a framework of operation in which government and regulators come together and agree on how they intend to triage their various expectations in line with activities already taking place. There is an opportunity to build a simplified process that chief information security officers, executives and boards can plan for - the result being not just increased compliance, but improved security and greater resilience.

The decision to split the bill and undertake further engagement is a positive indicator, as the ability to foster strong and responsive collaboration between industry, government, academia and the not-for-profit sectors through vehicles such as the Joint Cyber Security Centres is one of, if not the single most powerful weapon in the nation's defence against cyber risks.

Working together: Government + Business

Regulation is a starting point for government protection of critical infrastructure from cyber attacks. Beyond this, it has an expansive role to support these vital areas:

- intelligence gathering
- information sharing
- threat detection
- network monitoring
- real-world scenario testing

These capabilities represent a continuum of options for government to gently or more assertively act to help industry protect critical infrastructure. **Importantly, these efforts are cost prohibitive for private sector operators but don't constitute an unreasonably large expense in the context of a national budget where some of these capabilities are already matured. Removing these costly activities from a company's balance sheet, helps build goodwill and cooperation, and ultimately higher levels of protection.**

We can also learn from our global counterparts. Two key areas where the government can provide support is in the resumption of a service after an attack, and in the protection of data.

Facilities such as Israel's Security Operation Centre, which monitors dozens of critical infrastructure facilities in near-real time and alerts operators to attacks, demonstrate that heavy infrastructure assets operate on set-ups that are conducive to centralised monitoring.

Although a company's natural inclination is to avoid the need for government intervention, the clout wielded by a national government can certainly benefit commercial operators. For example, helping in negotiations with global product vendors that threaten to void warranties if sensors are installed in their systems. In a similar vein, Australia's critical infrastructure operators are concerned about liabilities to customers and suppliers arising from the government's new powers to take control of their facilities if a cyber attack threatens national security. **One solution would be for the government to offer liability protection to ease these concerns.**

Resilience testing is another area where governments are best placed to facilitate. Although nothing can stop a determined cyber superpower hacking into a system, resilience training exercises help to build a better understanding of risks and hone skills in executing "bare metal rebuilds". Restoring critical systems from ground zero without being able to count on lights, phones or computer networks is both difficult and time consuming.

Every six months, the United States' Defence Advanced Research Projects Agency runs exercises in jumpstarting a dead electricity grid while warding off a series of cyber threats on Plum Island, near New York. It is virtually impossible for commercial operators to make this type of investment. It is much better undertaken by a government, as is the case in Israel where the government has invested nearly USD10 million in a national laboratory due to open early in 2022. This centre, designed, developed and operated by PwC, will be used to help companies, technology manufacturers, academics and government run cyber attack simulations on for example, power stations, desalination plants and building management systems, free of charge.

Together, government and industry also have a role to play in equipping the community with the right information and tools to make good decisions. Australia's ageing demographic is especially vulnerable to this threat. Support and outreach for this sector needs to be done in a way that is meaningful and effective.

Ultimately, awareness is the single biggest lever at our disposal to make a difference in protecting critical infrastructure from cyber attacks. Unfortunately, after spending hundreds of millions of dollars on public awareness campaigns, the US has also learned that this is one of the hardest nuts to crack, leaving a substantial gap between individuals' expectations of the protections they should have, and their behaviour.

In the international arena, governments must continue to hold robust discussions about cybersecurity values and clearly outline expectations. A number of countries including Australia collaborated to create the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. This work sought to establish rules of engagement for cyber operations and demonstrates how governments can effectively work together on cybersecurity.

If the government does the heavy lifting on threat intelligence, monitoring, and testing, business can focus on cybersecurity alongside any other risk that needs to be strategically managed. Executives and boards can focus on internal risk policies, compliance with international and national standards, ensuring systems are robust and have a degree of separation, and pulling together a team that can adequately respond to attacks.

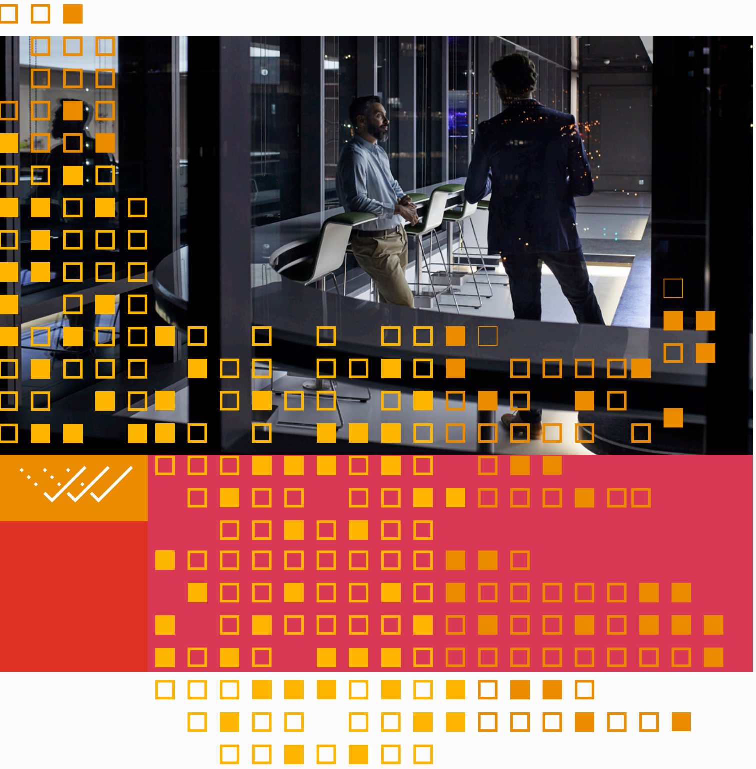
Industry should weigh-up its obligations to consumers using products or services in a data and cybersecurity sense and clearly articulate the consequences.

Unlike energy, sectors captured by the expanded scope of SLACI will not have three years to warm up to new rules, as was the case with the voluntary Australian Energy Sector Cyber Security Framework, which was developed in collaboration with its major players, including the market operator. Newly impacted sectors will only have three to six months to demonstrate progression towards compliance.

Avoiding costly mistakes

Given the need for accelerated adoption, there is an opportunity to leverage lessons from parallel industries that are further up the maturity curve, taking into account the variability in resources between affected organisations. Using Risk Management Planning to take an all-hazards approach to your enterprise will improve resilience, identify scenarios where unanticipated costs could arise, and potentially uncover opportunities for security practice efficiencies. As these reforms mature, collectively maturing risk management should reduce cost across supply chains. There is an opportunity to determine what learnings can be adopted and from where, then press fast-forward.

The easiest way to stretch a cybersecurity budget is not to repeat others' mistakes. Tapping into well-established networks of security practitioners, including the Financial Services Information Security Association, Trusted Information Sharing Network for Critical Infrastructure Resilience and Joint Cyber Security Centres, can help in this regard. These forums are populated by professionals who are happy to share their insights and experience.



Most industry sectors share information and can alert their peers to real-time threats. These forums are useful for trading insights into issues such as cyber insurance – what constitutes a quality scheme, how to call upon it, under what circumstances, levels of coverage, the ability to call on a third party well-versed in responding to incidents, and gaps in a policy that the government might be able to fill.

One of the most common mistakes in cyber risk mitigation strategies is neglecting to test backup plans. It is preceded only by the failure of training and awareness programs that were designed to stop people clicking on malicious emails in the first place.

The only way to know if a backup works is to test it. Under a best practice scenario, an incoming chief information security officer needs to map scenarios on paper and be running live scenarios involving executives and the board, within their first 12 months.

Cyber is just another business risk that organisations need to manage, one that is less regulated and less mature compared to others such as fraud. Industries do not yet have generational learning, and cybersecurity is not yet embedded in processes and procedures. Fortunately, most critical infrastructure providers have mature processes for dealing with other types of hazards covered under critical infrastructure legislation including physical attacks, personnel risks, espionage from trusted insiders, and even supply chain disruption.

Industries and organisations with highly evolved safety cultures can tie cyber risks to safety as the quickest and easiest way to embed best practice into processes. Employees need to understand that it is no different than a trip hazard on a worksite.

New tools, tax incentives and talent pool

A new equation is needed to battle cybersecurity risks, and keep Australia's critical infrastructure protected. No one body or business can solve for this risk; the many component parts of the challenge means our community must work together - bringing expertise and driving change across upskilling, economic policy, regulation, governance and more.

There is a dire shortage of cyber specialists worldwide. Competing for the same resources is not only inefficient, it is unsustainable. With this in mind, there is an opportunity and a need to create a centralised pool of high-quality cyber professionals, co-funded by industry and government, to which organisations demonstrating progression towards compliance, have priority access. Innovators in this space will take opportunities to collectively secure a supply chain and consumer ecosystem - they will reduce costs, share burdens and improve security and risk management processes through a co-operative model.

Australia's education framework needs to produce more cybersecurity specialists. In Israel for example, talented youngsters are encouraged to develop their exceptional skills early, and are fast-tracked through high school and military training. Building our nation's skills means developing a pipeline of engineers, robotic and software designers with the ability to build cyber defences into products and services.

Collective uplift across small and medium enterprises are essential to achieving the cyber equivalent of herd immunity. Entities covered by SLACI amendments only account for 3% of gross domestic product. The biggest companies take services from the smallest and the majority don't have a handle on their third-party cyber risks[4] – risks obscured by the complexity of their business relationships and vendor/supplier networks.

[4] PwC 2022 Global Digital Trust Insights

Imposing industry standards that are built into procurement contracts can have a positive knock-on effect in ensuring supply chain hygiene. In much the same way that modern slavery laws have imposed minimum requirements on suppliers, voluntary standards for cybersecurity could too.

Tax incentives should be considered for investments in cyber technologies, including moving data and software systems to more secure cloud services. This is already putting additional onus on providers of cloud-based software to increase not just the security of their systems, but the basic education of people using them. The surge in hybrid working during COVID-19 saw Google announce a new cybersecurity action taskforce and resilience framework in October 2021, alongside security enhancements to its Workspace productivity and collaboration software.

There is more scope for initiatives such as the AusCyber capability development and innovation hub, which has been very effective in other jurisdictions in giving rise to an ecosystem of security start-ups, technology and talent. Big businesses, such as NAB and Telstra are stepping up to support small and medium enterprises with practical cybersecurity guides and toolkits, although there is still room for improvement.

Models of stewardships, such as the Australian Prudential Regulation Authority, provide a springboard for similar collaborations in cybersecurity. This initiative aims to reduce the spread of harmful online misinformation to Australians, and Adobe, Apple, Facebook, Google, Microsoft, Redbubble, TikTok and Twitter are all signatories.

Technology vendors have a rich appreciation of collaborative inter-dependency but critical infrastructure providers have not yet reached this level of maturity.

Protecting critical infrastructure from cyber attacks is vitally important. The challenge is that no single entity or individual owns it. We are collectively responsible, and all have a role to play. Within this ecosystem there is significant scope for all players to do better.

Every time a hole in the net is patched, it becomes harder for cyber criminals to profit from Australian organisations and individuals. This benefits communities that will experience fewer attacks and losses, and Australian businesses will be sought after as service providers if we develop a reputation as a cyber resilient nation.

Key contacts

Robert Di Pietro

Partner
Cybersecurity & Digital Trust
+61 3 8603 2391
robert.di.pietro@pwc.com

Garry Bentlin

Partner
Cybersecurity & Digital Trust
+61 409 573 636
garry.bentlin@pwc.com

Zoe Thompson

Director
Cybersecurity & Digital Trust
+61 472675510
zoe.thompson@pwc.com

Special thanks to

Rafael Maman (IL)

Partner
Cybersecurity & Privacy Leader
PwC Israel
+972 52 3589008
rafael.maman@pwc.com

PwC refers to the Australia member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. Liability limited by a scheme approved under Professional Standards Legislation.

At PwC Australia our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 250,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.au.

WLTP0102828