Building cyber resilience in critical infrastructure

pwc

An increase in attacks on our critical services and infrastructure

The national conversation about the cyber threats faced by Australian governments and businesses is ramping up. In May 2021, Mike Pezzullo, Secretary of the Department of Home Affairs and one of Australia's top national security figures, said cyber attacks against Australia's Critical Infrastructure were his "most pressing and immediate concern" - going so far as to call the threat of a breach that could take down the nation's electricity network "realistic", "credible", and "deeply concerning."[1]

This comes less than a year after Prime Minister Scott Morrison revealed that entities at all levels of government, industry, politics, education, health, and essential services had come under targeted cyber attack by a sophisticated state-based actor.[2]

Australian organisations are no strangers to the consequences of a successful cyber attack though. The system outages, financial loss, and reputational damage resulting from a ransomware infection or data breach are now part of the weekly news cycle.

But what concerns an increasing number of people is the potentially catastrophic impacts of cyber attacks on critical infrastructure. After all, the consequences of such a breach go further than financial loss. They include the potential for prolonged outages of essential services and, subsequently, impacts on health, safety, and even national security.

Recent global incidents include:

The Colonial Pipeline attack

After discovering a cyber intrusion within its IT systems, the operators of the Colonial Pipeline proactively took systems offline to contain the threat, grinding its operations to a halt in the process. As the largest refined oil pipeline system in the United States, the outage resulted in widespread shortages of gasoline, diesel, jet fuel, and heating oil along the south-eastern US coast. Some analysts described the incident as "the most significant, successful attack on energy infrastructure we know of in the United States."[3]

Oldsmar water treatment facility hack

It's suspected hackers gained access to a water treatment facility's computer system near Tampa, Florida, USA, in February 2021. Once inside the system, attackers sought to introduce excessive levels of a dangerous chemical into the water supply.[4] While disaster was averted before the chemical could reach the water supply, the consequences could have been devastating for the town's 15,000 population. It became the first documented attempt to hack into and contaminate a US community's water supply.

Johannesburg electricity ransomware attack

In 2019, a major electricity supplier in South Africa's largest city suffered a ransomware attack that affected a quarter of a million people with power outages.[5] City Power reported that the attack had "encrypted all our databases, applications and network". While attacks like this are on the rise, this is not a new threat. As far back as 2007, the Stuxnet virus reportedly destroyed numerous centrifuges in Iran's Natanz uranium enrichment facility, while in 2015 and 2016 Ukraine's power grid was attacked and partly shut down[6] after a spear-phishing campaign targeting IT staff.

The Transport NSW incident

In late February 2021, the Department of Transport for New South Wales was impacted by the breach of Accellion[7]. Attackers targeted this provider of file transfer software, gaining access to over 300 clients' sensitive data that was stored within the file sharing software. The actor behind this attack, CL0P, is known to conduct ransomware attacks before leaking data (called a double extortion attack), but instead this time went straight to extorting money based on the information stolen.

As cyber threats become more sophisticated and increasingly target operators of critical infrastructure, organisations must urgently assess and uplift their cyber resilience.

Converging IT and OT introduces new risks

Many critical infrastructure entities, particularly those in industrial sectors, are characterised by a growing convergence of their information technology (IT) and operational technology (OT) systems, including business processes and related IT systems. But this convergence comes with a risk. Take the Colonial Pipelines incident[8] for example, where the attack took billing systems offline and effectively made operating the pipeline impossible.

Having traditionally been separated from IT systems - and, therefore, common cyber threats - much of the convergence between IT and OT in critical infrastructure has been driven by demand for more data-driven analysis, decision-making, and automation. Pressure to deliver services more efficiently is increasing due to competition, technological change, reduced government funding, and price regulation[9].Organisations surveyed by ASPI in 2019 forecast a rapid increase in this convergence over the coming years, particularly in the telecommunications, energy, water, and transport sectors.

But this convergence leads to more potential entry points for cyber intruders who want to hold utilities to ransom or disrupt their operations, and can add more complexity to mitigation efforts.

The answer is not to avoid further convergence but to ensure it is implemented securely. While many critical utilities operators have recognised the need for increased focus and investment on IT security, this has not been matched for OT systems.

That ultimately leads to critical vulnerabilities with real-world impact, including the supply of electricity, water, gas, or other essential services.

Progress is being made, but there's more to do

There has been significant progress in the level of cyber maturity across the utilities sector over the past few years. This has been ably shown by the industry's willingness to embrace the Australian Energy Sector Cyber Security Framework (AESCSF), developed jointly by AEMO and PwC in 2018 and applicable to its 270 market participants. Despite being a voluntary framework, participation rates across the sector have been very high, raising awareness of shortcomings around IT and OT security.

Many organisations leveraged this sector-wide initiative to spark board-level discussions about the importance of cyber security and the need for continued investment. Many other industrial sectors are still striving to gain this level of traction at the senior executive level. The step-change in the utilities sector is further evidenced by the growing appointment of CISO positions within larger organisations - a choice that was much less common just five years ago.

The tightening regulatory environment

Despite growing awareness of the risks of IT/OT convergence and the need for investment, efforts to boost security and resilience have not gone far enough. Reasons for this include:

- The level of perceived threat (and therefore investment) was lower until recent attacks on critical infrastructure, both in Australia and internationally.
- Legacy and critical assets with long lifespans can take millions of dollars to re-engineer or re-architect making it costly to secure them.
- There was less regulatory focus on critical infrastructure cybersecurity and resilience, with the majority of focus on physical security and emergency management.

But times are changing. In response to the increasingly dangerous cyber threat landscape, federal and state governments are turning their attention to the challenge of uplifting the cyber resilience and capabilities of Australia's critical infrastructure providers. Upcoming regulatory changes are a direct outcome of this increased focus, with a range of regulations, obligations, and voluntary reporting frameworks already in place, including:

- Protective Security Policy Framework (PSPF)
- Foreign Investment Review Board (FIRB)
- Security of Critical Infrastructure (SOCI) Act 2018
- Australian Energy Sector Cyber Security Framework (AESCSF)
- Notifiable Data Breaches (NDB) scheme 2018.

In particular, the Security of Critical Infrastructure (SOCI) Act 2018 brought welcome focus to the security of essential industries, including electricity, water, gas, and ports. But it quickly became clear that those industries alone were not enough. The Security Legislation Amendment (Critical Infrastructure) Bill 2020 expands the SOCI Act to mandate obligations on companies across a broader range of critical sectors, reflecting the changing security priorities identified in the Australian Cyber Security Strategy 2020.

The enhanced regulatory framework brings additional clarity to the steps required to strengthen cyber resilience, enabling industry and government to work together more effectively. For most organisations the additional SOCI obligations will be simple to implement and will complement activities they're already undertaking. But for others, uplifting cyber capabilities to meet proposed regulatory requirements will involve more significant cost and effort. The Positive Security Obligations and Enhanced Cyber Security Obligations as part of SOCI will drive additional investment in people, process and technologies, as well as an increase in assurance activities to meet board reporting and risk management requirements.

Moving beyond security to build resilience

So, where to start for critical infrastructure providers, including utilities? First, it's important to ensure you're aware of your organisation's obligations under the Security Legislation Amendment (Critical Infrastructure) Bill 2020, as well as other state cybersecurity legislation such as state-based license conditions.

Beyond compliance there's a number of security challenges unique to critical infrastructure operators who rely on both IT and OT. Our deep experience conducting security assessments and penetration tests in industrial environments has highlighted a number of common issues, outlined in our whitepaper describing the most common security vulnerabilities in OT networks[10].

The traditional view that we can isolate critical systems is becoming outdated as businesses increase levels of connectivity and adoption of technologies like cloud and Industrial IoT.

Many organisations are still looking to the Purdue Model[11] as a framework for segregating technology environments, which was developed before the advent of contemporary tech such as cloud and IoT.

At a more granular level, the ISA/IEC 62443 Standard provides more technical guidance on how to securely manage OT environments, and great progress has been made in developing secure coding practices for Programmable Logic Controllers (PLCs)[12] which are core components of many critical infrastructure networks.

Whilst these frameworks and standards can offer a helpful lens through which to develop and assess security capability, adopting them wholesale can be cost prohibitive, and they are just one piece - a technology centric piece - of a bigger puzzle that cannot be solved by technology alone.

As the lines between physical and digital disruption are blurred and attacks become more of an inevitability than a possibility, there is a growing need to shift from a preventative mindset to a more holistic, resiliency-based approach across people, process, and technology.

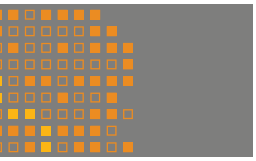
This shift from a security to a resiliency approach focusing on the ability to detect and respond to attacks in a manner that minimises disruption to services is even more urgent in the case of critical infrastructure providers such as utilities, whose provision of services can have health and safety or national security implications.

The key is to make your approach consistent across every aspect of your business in how you identify, detect and respond to disruption, either digital or physical. Consider that the attack on the Colonial Pipeline did not hit the OT or gas pipeline assets themselves, but instead started with a phishing email. As Colonial began to fear the attack would spread and they would lose control of their systems, the business shut the pipeline down themselves. This failure to adequately protect mission critical systems (such as a gas pipeline) from events impacting lower-security environments (such as email systems) is a glaring example of a need for greater resilience.

We as humans regularly take steps to build our own resilience, so that in the event we become ill or catch a cold, we can recover as soon as possible and carry on with our most important tasks. We accept, despite our best efforts, it's not always possible to guarantee prevention and similarly, critical infrastructure organisations must use modern risk management practices to identify, mitigate and control risks within defined business risk appetites. Cyber incidents will occur - an organisation's measure of success isn't stopping them, but how they respond and recover from them.

This is starting to happen in the utilities sector, where the language around cyber security is shifting towards the concept of resiliency. Encouragingly, we now see cyber security being adopted into organisations' "all-hazards" approach to risk management. While some mature organisations have been practising all-hazards resilience for a long time, the pace of digital technology adoption is so fast that many of these strategies are now in need of a refresh.

Where should we focus? A holistic view of resilience requires:

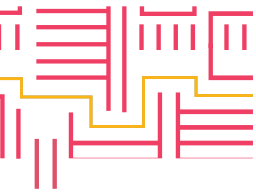


Proactive assurance activities and security testing.

Penetration testing - or hacking your own system - gives you the opportunity to find and fix weaknesses before cyber attackers do. While this has become more popular within critical infrastructure IT environments, often penetration testing is deemed too risky for core OT systems. But it is possible to undertake such testing in a safe and controlled manner with the right specialists involved, utilising a combination of automated (i.e. testing tools) and manual methods (i.e. walkthroughs with process control engineers). Minimising risk depends on being able to ensure effective communication between engineers, operations, health and safety, physical security and technology teams across the organisation. This type of assurance activity is key to a successful risk management program.

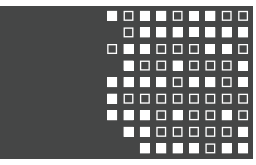
Establish an "OT Cyber Champion" or expanding the role of the CISO.

Having a defined cyber champion helps elevate cyber safety conversations across your engineering and operations workforce. While we have seen a welcome rise in the number of CISOs in critical infrastructure providers, one challenge we still see is that the CISO doesn't always have the mandate or authority over OT as well as IT. More mature organisations are dropping the "I" to create Chief Security Officers responsible across IT, OT, and physical security.



Go beyond natural hazards.

Critical infrastructure providers, including utilities, are used to resilience-based thinking when it comes to natural hazards and emergencies. Continuity plans are in place to define clear responsibilities, limit damage, and restore services fast. Cyber hazards should be treated no differently to supply chain risk, personnel risk, and physical security. Regularly practice cyber crisis response through exercise and drills, leveraging what your organisation may already be applying for emergency management or natural hazards. It is important these are conducted with representation across all key business stakeholders - not just cyber security, but also operations, HR, legal and public relations. The most implausible scenarios are often the ones that need the most practising, and the dependencies and flow-on effects of cyber disruption are sometimes not understood until an incident occurs (as the Colonial incident has demonstrated).



Bolster business continuity plans.

Ensure your business continuity plans (BCP) cover scenarios for ransomware and system unavailability. And don't forget the links between mission critical systems and corporate systems - for example, can you maintain production without corporate email? When was the last time you conducted a full system restore to test backup and continuity capabilities?

Make measurement key.

You can only improve resilience and sustain it if you can measure the success of your work. This requires choosing useful metrics and having access to accurate data. A fundamental starting point is to report on the risk landscape, including how risks are changing based on the steps being taken. Whilst many useful cybersecurity frameworks enable maturity-based measurement, every organisation should be able to clearly translate this into their own risk management language, in line with a defined risk appetite.

Strengthen your cyber resilience today

There is no magic silver bullet in the new world. Utilities and other critical infrastructure providers need to focus on getting the basics right, applying defence in depth strategies, establishing useful metrics, and practicing resilience - including testing and crisis scenarios.

At PwC, our purpose is to build trust in society and solve important problems. Ensuring the critical services Australians rely on every day remain available, secure, and stable sits at the very core of that focus.

We help organisations address cyber IT and OT risk from the technical level on the factory floor all the way to strategic conversations at board level.

PwC has played a pivotal role in advancing critical infrastructure security, working across the industry spectrum. Proof of our expertise is the strength of voice to Government. That includes submissions on the SOCI Amendment Bill, our role overseeing implementation of the Australia 2021 Cyber Strategy through representation on the Industry Advisor Committee, and our position within Engineering Australia's Cyber Security subcommittee to promote the intersection of cyber security and engineering disciplines. PwC Australia were also recognised as Advisory Contributors to Version 2.0 of the C2M2 Cyber Maturity model released in July 2021, which is adopted by many critical infrastructure organisations globally.

This experience across industry and government allows us to bring a deep understanding of the latest legislation and, more importantly, what it means for your organisation in practice.

With experts in cybersecurity, industrial control systems, and business risk, PwC can bridge the gaps in organisation, overcoming the siloes that can impede the building of resilience.

If you or your organisation are looking to strengthen your cyber resilience, get in touch with us today.

Key contacts

Robert Di Pietro
Partner
robert.di.pietro@pwc.com

Mike Younger
Partner
mike.younger@pwc.com

Garry Bentlin
Partner
garry.bentlin@pwc.com

Tom Wentworth
Director
tom.w.wentworth@pwc.com

Zoe Thompson
Senior Manager
zoe.thompson@pwc.com

Footnotes

1. https://www.abc.net.au/news/2021-05-24/cyber-attack-threat-critical-infrastructure-mike-
2. https://www.pm.gov.au/media/statement-malicious-cyber-activity-against-australian-networks
3. https://www.politico.com/news/2021/05/08/colonial-pipeline-cyber-attack-485984
4. https://www.washingtonpost.com/nation/2021/02/09/oldsmar-water-supply-hack-florida/
5. https://www.bbc.com/news/technology-49125853
6. https://www.bbc.com/news/technology-35297464
7. https://www.transport.nsw.gov.au/news-and-events/articles/transport-for-nsw-impacted-by-worldwide-accellion-data-breach
8. https://edition.cnn.com/2021/05/12/politics/colonial-pipeline-ransomware-payment/index.html
9. https://www.aspi.org.au/report/protecting-critical-national-infrastructure-era-it-and-ot-convergence
10. https://www.pwc.com.au/pdf/cyber-savvy-securing-operational-technology-assets.pdf
11. https://www.automationworld.com/factory/iiot/article/21132891/is-the-purdue-model-still-relevant
12. https://www.plc-security.com/

WLT127083042