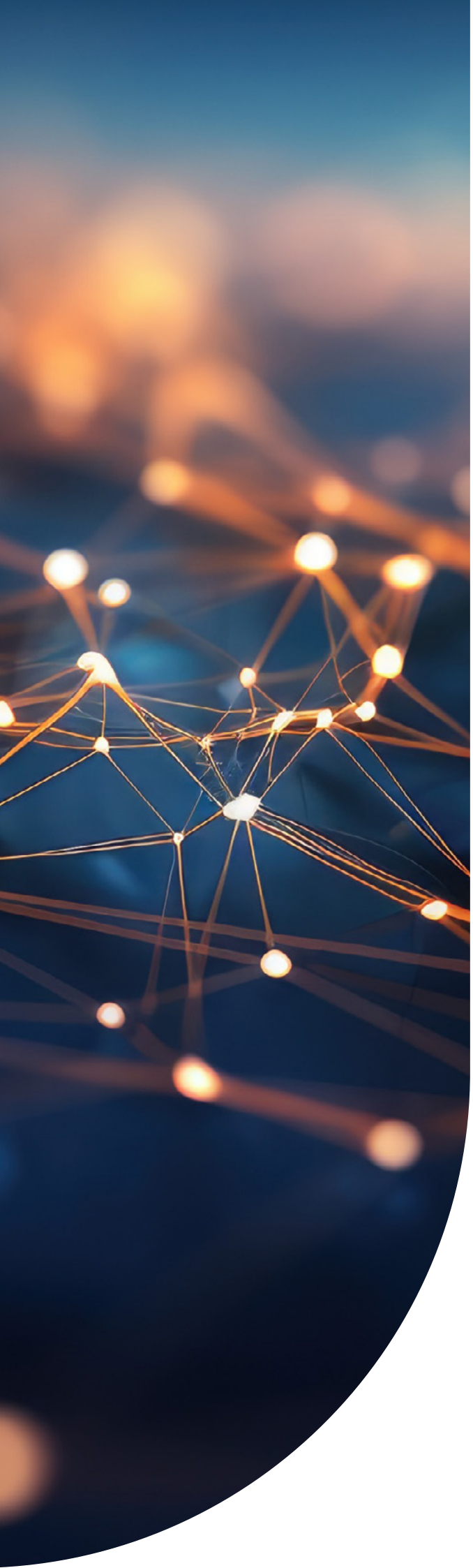
The era of digital complexity in Australian energy, utilities and infrastructure

CLAYTON UTZ



Contents

About this report

The era of digital complexity in Australian energy, utilities and infrastructure is written by Clayton Utz in partnership with The Action Exchange, a thought leadership and stakeholder engagement agency.

This report explores the changing nature of procurement and contracting in increasingly digitally-connected infrastructure, energy and utilities projects. It argues that traditional risk and procurement models fall short in Australia's new era of heightened regulatory demands, governance requirements and sophisticated cyber risks.

This report examines the convergence of these trends through the lens of three overarching complexity drivers —sentience, interoperability and security— to understand how asset owners and operators are grappling with them.

Clayton Utz and The Action Exchange thank the following people who were interviewed for this research:

- Peter Hannam, Director of Asset Management, Infrastructure, **IFM Investors**
- Victoria Moore, Chief Strategy, Development and Legal Officer, **Patrick Terminals**
- Dr Tony Pollock, Chief Technology Officer, **Icon Water**
- Mitch Erickson, Group Manager Digital Engineering, **John Holland**

We acknowledge the Traditional Owners of Country throughout Australia and recognise their continuing connection to land, waters and culture. We pay our respects to their Elders, past and present.

Key Findings

1	Australian infrastructure, energy and utilities are entering a new era of digital complexity	The uptick in complexity of new connected technologies is changing the way that infrastructure equipment and systems are being acquired and managed. Conventional risk and procurement policies often fail to address the unique vulnerabilities and regulatory obligations of high-tech infrastructure developments.
2	Passive assets are giving way to smart systems	Internet-connected equipment and systems are driving operational advances for asset owners and developers, from increased productivity and preventive maintenance to enhanced decision making, reduced emissions and cost savings. Yet, they bring with them new legal, procurement and regulatory issues.
3	New layers of due diligence are emerging in technology outsourcing and procurement	Connected technologies introduce new layers of commercial and legal due diligence into infrastructure projects, making traditional contracting insufficient. Intellectual property, cyber resilience, critical IT systems and data privacy are joining traditional headline due diligence factors in deal considerations such as competition and pricing. Australia's relatively small size in the global technology market can impact local asset owners' bargaining power with 'big tech' suppliers.
4	Interoperability across projects and proponents is becoming the norm	As Australian infrastructure, energy and utilities assets become more technically complex and connected, their data and systems must be interoperable across projects and even whole sectors. The convergence of operational technology and information technology brings with it a tangled web of additional digital risks, in particular third-party exposure to cyber threats. To reduce their risk of a hack or breach many companies are purging their data, but this too poses a risk of missing opportunities and insights. Striking the right balance is crucial.
5	Cyber risk, and Australia's regulatory response to it, is growing	National security threats against internet-connected Australian infrastructure mean whole swathes of asset owners and operators face a growing compliance burden, which is expected to increase in the coming years. In an operating environment awash with cyber threats, investors and asset owners are prioritising recovery and resilience to minimise asset downtime. Implications for investors: Australian regulators are increasing their scrutiny and requirements on foreign investment in critical infrastructure, giving domestic players an advantage.

Introduction

A decade ago, *Wired* magazine declared data 'the new oil of the digital economy'[1]. Getting that data flowing safely through today's 'digital combustion engine' is proving increasingly complex and risky— and nowhere more so than in infrastructure.

Australia's largest industrial, infrastructure and energy projects rest on complex digital backbones. Hard hats and cranes are giving way to data interoperability, cyber resilience and AI governance. Traditional risk and procurement policies often focus on financial and physical factors rather than the unique needs of high-tech infrastructure developments.

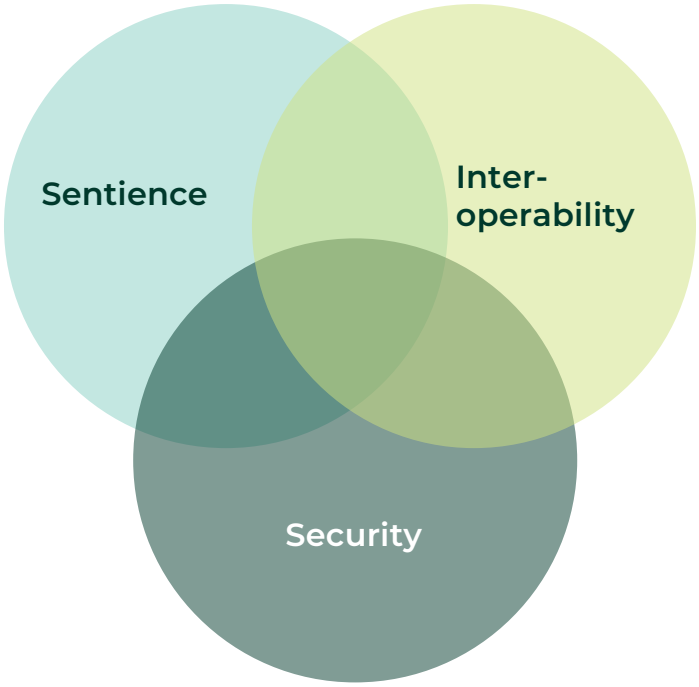
However, today's operating environment is flooded with new and emerging technologies, making risk profiles more nuanced and less understood than conventional industrial technologies.

Volatile macroeconomic conditions are making energy and infrastructure increasingly attractive asset classes among a growing number of investors[2]. But are investors prepared for the uptick in complexity, unique vulnerabilities, regulatory obligations and unorthodox transactions that now typify this sector? From patent 'chokeholds' to governance liabilities and geopolitical cyber-threats, developing and investing in infrastructure has entered a new era of digital complexity.

"... today's operating environment is flooded with new and emerging technologies, making risk profiles more nuanced and less understood than conventional industrial technologies. "

At the same time, businesses are losing confidence in their ability to manage risks. Executives are 20 percent less confident in their procurement team's ability to manage supplier risk in 2024 than they were a year earlier, according to a global survey conducted by Economist Impact[3]. Consult Australia's 2024 survey found almost three-quarters of members, many of whom are involved in delivering infrastructure and engineering, are operating in a higher-risk environment than they were the year before[4].

This report explores the convergence of these trends by examining three overarching complexity drivers —sentience, interoperability and security— and how Australian asset owners and operators are grappling with them.



Complexity Driver 1

Sentience

When ‘dumb’ assets become ‘smart’ systems

Infrastructure, energy and utilities projects are no longer simply passive assets made from concrete and steel. Modern systems increasingly have intelligent and software-reliant technology built into them. Driven by demand for innovation, data insights and operational efficiencies, many asset developers and owners are eagerly adopting - and realising significant benefits from - connected digital technologies. Yet they are also discovering that internet-connected equipment brings with it new legal, procurement and regulatory issues.

The ubiquity of connected digital technologies embedded in infrastructure, energy and utilities projects makes building, owning and investing in these assets more complex and risky than in the past. And, while digital and cyber risks are well known, the new layers of due diligence required to procure and deploy smart systems are less well understood.

“Too often, asset owners buy a complete solution without fully understanding the long-term implications of embedding a piece of IP-laden technology into their infrastructure,” says Lina Fischer, a construction and infrastructure partner at Clayton Utz. “It’s important to consider how the tech will be upgraded, what happens when it becomes obsolete and how modifications will be managed. It’s not uncommon for asset owners to find they don’t have much bargaining power down the track.”

The ubiquity of connected digital technologies embedded in infrastructure, energy and utilities projects makes building, owning and investing in these assets more complex and risky than in the past.

Innovative systems driving operational advances

Smart systems drive productivity and innovation gains across the infrastructure, energy and utilities sectors in various ways: enabling preventive maintenance, reducing asset downtime and driving both enhanced decision making and cost savings.

Icon Water, an Australian Capital Territory-owned company that provides drinking water and wastewater services to the nation's capital and surrounding regions, uses data from the company’s vast sensor network to augment decision-making, including enabling predictive maintenance. The technology reduces both maintenance cycle times and operational costs associated with sourcing water from various dams, says Dr Tony Pollock, the company’s Chief Technology Officer. Using this type of technology to achieve operational efficiency is increasingly ubiquitous among water utilities[5].

Integrating digital technology into infrastructure assets “has a revenue upside as well,” says Peter Hannam, Director of Asset Management for Infrastructure at IFM Investors. In airports, “digital passports and e-gates mean less room is needed for customs, creating more space for operational areas such as baggage handling, retail opportunities or food and beverage enhancements.” Automation and digitisation have also improved airport efficiency through self-check-in and automated baggage drop off[6].

Sustainability is another driver. Ports operator Patrick Terminals has reduced the company’s carbon emissions while increasing rail capacity at its Port Botany terminals by introducing automated electric, rail-mounted gantries (ARMGs)[7]. “Introducing more modern and efficient rail handling equipment and technology has enabled a significant increase in rail capacity and provided sustainability benefits to our customers being a low emissions container supply chain,” says Victoria Moore, Patrick Terminals’ Chief Strategy, Development and Legal Officer. “Rail freight produces 16 times less carbon pollution than road freight per tonne kilometre travelled” she says.

Digital twins, which use 3D modelling, real-time analytics, and artificial intelligence to create a digital double of physical assets and systems, also help asset owners and operators to optimise project building and decision-making across the asset life cycle. In NSW, a digital twin modelling the state’s electricity network helps to predict the impact of risks such as flooding[8].

John Holland utilises data and various technology environments to deliver its projects. Using these integrated systems aids project teams in decision-making and de-risks delivery. Some of the advances in component modelling and data interrogation have been significant and rapid, says John Holland's Group Manager of Digital Engineering, Mitch Erickson. "We are continuously improving our digital tools and usage within the business. It is critical to ensure we upskill our delivery teams to help them do what John Holland does well - deliver projects".

Expansion of technology outsourcing and procurement challenges

Yet, to realise the benefits of connected technologies, asset owners and developers must navigate a range of new procurement and contracting challenges.

The integration of infrastructure and technology is increasing complexity. A typical transport network now requires a sophisticated back end to run digital payments systems so commuters can tap to pay at physical gates equipped with mobile devices and sensors. “Infratech projects like these can no longer be approached as traditional equipment and construction transactions,” says Ken Saurajen, intellectual property and technology partner at Clayton Utz.

> “For some infrastructure, utilities and energy asset developers, accustomed to traditional construction contracting, the expansion of technology issues they now need to factor in is a steep learning curve. ”

Technology, unlike traditional brick-and-mortar infrastructure, undergoes continuous development. Fixed-scope contracts can often require immediate variation. “It’s like living through a horror home renovation,” says Mr Saurajen. “We can’t predict which technology innovation we will want delivered if it doesn’t exist yet.”

According to KPMG, investors and asset owners increasingly want to know how their assets will absorb new, as yet unknown, technologies[9]. This is why establishing a well thought out governance standard for the lifecycle of the project is essential to deal with changes in the future. “The philosophical perspective parties bring to a transaction is now much more important in infrastructure,” says Saurajen. “It’s no longer sufficient to staple a template governance schedule to the back of a contract and put it in the bottom drawer,” he says.

New layers of due diligence

Connected technologies also introduce new layers of commercial and legal due diligence into infrastructure projects. Asset owners and investors are increasingly conscious of these considerations early in the process, and a trend has emerged in the past 12 months for digital considerations to be prioritised in the first rounds of transactional due diligence. Intellectual property (IP), cyber resilience, critical IT systems and data privacy are joining traditional headline due diligence factors such as competition and pricing. “Increasingly, technology factors are impacting whether infrastructure deals progress from the early stages,” says Walid Sukari, a Partner at Clayton Utz.

IFM Investors’ Peter Hannam notes that when assessing infrastructure investments, he looks to see whether prospective assets have sufficient awareness of technology risks, resourcing and cyber controls in place. “It’s resilience and recovery that we absolutely focus on in our diligence efforts,” says Hannam.

Vendor size can be a challenge in the Australian market

The more complex a project, the higher the likelihood it will require an integrated system approach involving various partnerships with technology vendors. The ever-changing landscape of asset owners requires an agile delivery lens. "The key is not only having partnerships with large technology providers but also smaller agile, modular developers that can help de-risk the models, data and overall the project and broader business.," says Mr Erickson.

"We find ourselves in a world in which connected infrastructure projects require the successful procurement and harmonisation of many different components," agrees Mr Saurajen. "The more complex the solution becomes, the less likely it is that one service provider can do all of it."

For assets considered 'critical infrastructure', data management and data sharing rules restrict the potential pool of companies that can provide services and systems. "There is a level of legislative compliance that needs to be considered with technology procurement strategies that didn't exist a few years ago," says Mr Hannam.

Australia's relatively small size in the global technology market can impact local asset owners' bargaining power with 'big tech' suppliers. This is particularly an issue in the transport and property sectors, says Clayton Utz partner Lina Fischer. "Replacing or modifying systems becomes difficult when the contract does not include sufficient IP rights and the asset owner is locked in to dealing with a particular supplier," she says.

"The supplier can charge as they like and may choose not to support a particular project. Trying to retrofit or replace that system can be very expensive," she says.

Construction contracts don't typically deal with proprietary rights or IP only being available to one supplier, says Clayton Utz technology partner Simon Newcomb. "Operators that don't factor in maintenance as part of the original construction contract find they're left exposed to the demands of the technology supplier," he says.

Once a technology is installed in an infrastructure project, vendors are able to pursue a 'chokepoint' patent strategy, locking customers into "unavoidable technology moats" of IP-protected technology. AI technologies are being patented at speed, faster than all other patent filings, especially in the industrial, energy and engineering fields[10]. As technology vendors integrate AI advances into projects, asset owners will be forced to raise the sophistication of their procurement strategies in response.

Is data the new asbestos?

Recent high-profile data breaches have raised concerns among businesses about the potential liability and reputational risks associated with their projects. Projects and technologies that collect large amounts of data may be especially at risk. For some, the risk-reward ratio no longer justifies storing data to be used opportunistically in the future.

> "Rather than thinking 'data is the new oil' they couldn't get enough of, some businesses now consider 'data the new asbestos' they want to get rid of."
>
> Monique Azzopardi,

"Holding on to certain types of data creates a liability exposure for businesses if there is a hack or data breach," warns Monique Azzopardi, Special Counsel at Clayton Utz. In response, data purging and de-acquisition to reduce cyber risk exposure is gaining favour among some businesses. Yet, according to a Governance Institute of Australia survey, only a third of organisations regularly purge their data[11].

But dropping the data 'hot potato' may come at a cost. If attempts to mitigate data risk go too far, asset owners may lose insights, miss opportunities, and slow down innovation. Striking the right balance is key. "We cannot put all data into the same bucket. The legal and operational risks associated with collecting, using and holding personal information are different to those associated with other types of data" says Ms Azzopardi. "When used well, in a legally compliant manner and with appropriate due diligence, smart buildings and technologies and their associated data outputs can deliver key insights and drive benefits for industry and the consumer," she says.

CLAYTON UTZ

Complexity Driver 2

Interoperability

As Australian infrastructure, energy and utilities assets become more technically complex and connected, their data and systems must be interoperable across projects and even whole sectors. The challenges are vast. Operational technology (OT) and information technology (IT) are converging as legacy equipment becomes interconnected with digital systems.

Connected projects require contracting with a tangle of providers, and project proponents are all asked to roll disparate data into common pools. While coalescence brings new capabilities to the sector, it also creates new integration risks.

Interoperability of internal IT and OT systems

Marrying old and new systems remains an ongoing and highly capital-intensive challenge for Australian assets. Legacy OT, including industrial control and supervisory systems, may have been designed before internet-connected tools were in use. The challenges of modernising commuter trains, adding terminals to existing airports and integrating renewable energy into the electricity grid have caused many asset owners to lose sleep.

Ensuring internal technologies are interoperable is a priority for Icon Water. "We span a whole vertical from water catchment to treatment, through to retail, then waste and its treatment. There are quite a lot of technologies along the way that we need to bring together to drive operational efficiencies," says Tony Pollock.

"The data from our lakes and catchments helps our modelling team understand how much network capacity we need, informing water sourcing strategies or for planning our future capabilities and climate adaptation."

Tony Pollock

At Patrick Terminals, the need to manage security risks means ensuring suppliers can provide interoperable solutions. Patrick's ARMG project saw separate procurement arrangements for the automation equipment and its connected systems. "Adopting an integrated contracting model for procuring and operating equipment with technology is something we've been doing for a long time," says Ms Moore, "this involves a multi supplier approach that supports the delivery of interoperable solutions" she notes.

Pooling data across projects and sectors

Interoperability is especially crucial when infrastructure operators need to exchange data to carry out commercial transactions. Australia's transport sector has been grappling with this for several years. Toll roads and tag payment systems must be interoperable across asset operators to ensure traffic data collection and payment settlement arrangements are consistent for motorists.

Payment infrastructure has similarly disrupted the Australian energy sector. The increasing flow of renewable energy in the electricity grid requires a faster snapshot of consumer energy use to enable trading. To speed the process up, Australian energy companies had to switch from settling energy transactions every 30 minutes, to every five minutes. "It sounds like a simple change, but for some energy operators it was the biggest technology and IP project they had ever carried out," says Mr Newcomb.

"The whole market had to become even more interoperable. And it had to take place at the same time, so companies were competing for the same IT resources at once."

Simon Newcomb

A wide range of technologies and data are often pooled together at the project level, too. Brisbane's Cross River Rail Project brought business information modelling, geospatial and interactive 3D modelling into one digital tool for the first time in Australian infrastructure[12]. Data from upstream suppliers, contractors and government agencies was filtered for use downstream once the project was completed. "With so many players tipping their data in, it was important to have standards in place, as well as clarity on the licensing, collection, security and liability issues associated with its various uses," notes Mr Newcomb.

The adoption of modelled project delivery, including components and geospatial datasets, has significantly increased in Australian infrastructure projects. Both government and private sector organisations are recognising the benefits of digitising their approaches, which not only enhances their internal capabilities but also improves project delivery and procurement models. "At John Holland, we are continually working with our client base to help deliver a delivery structure that allows the projects to be delivered on time, on budget and safely but also to bring our clients along for the journey," says Mr Erickson. "This is something managing contractors have been notoriously bad at in the past. But, it is something we are changing to help deliver these projects and improve our offering in the Australian infrastructure market, as John Holland continues to develop into a data-centric business."

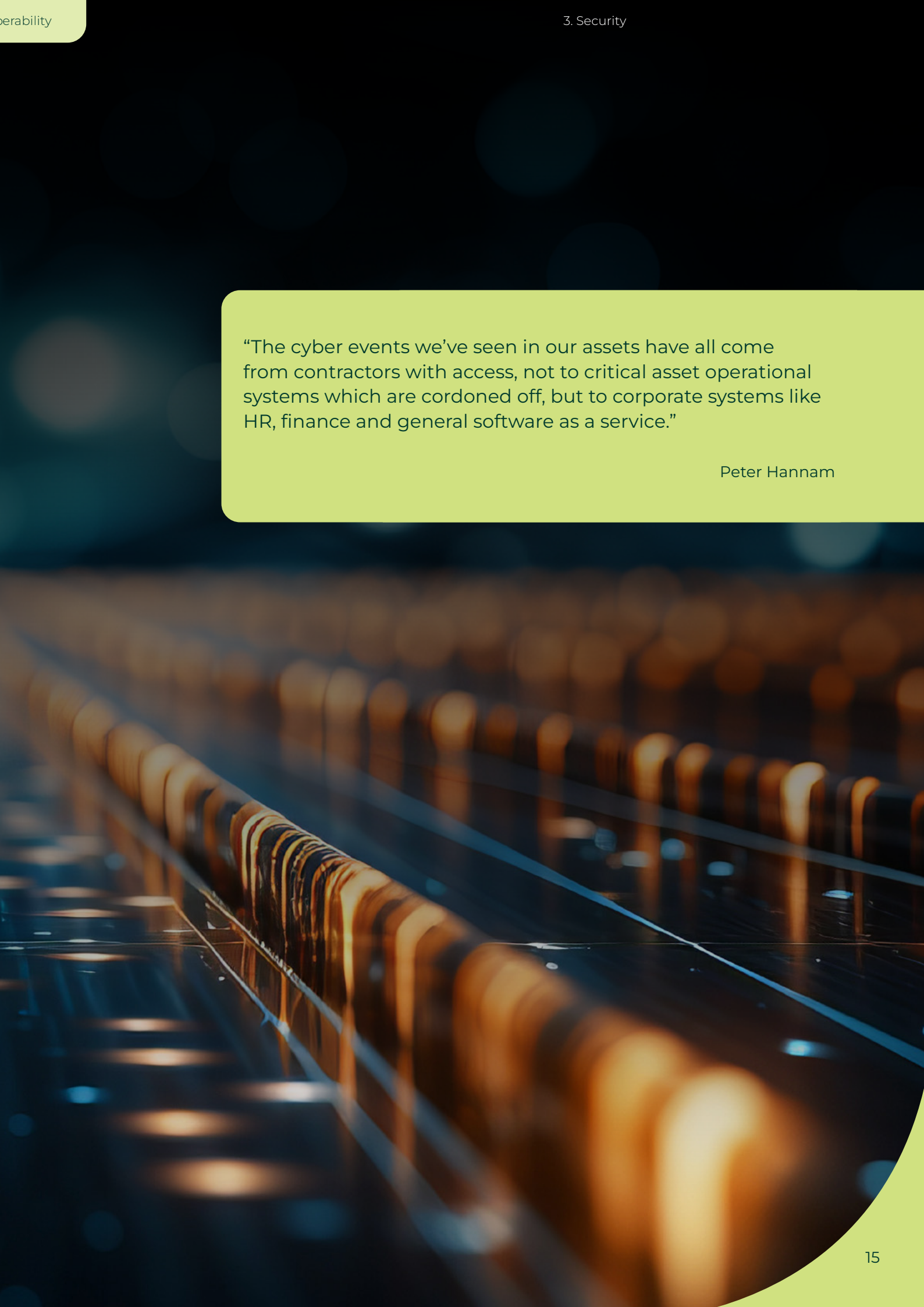
Integration or contamination?

While the business case for enhancing interoperability is clear, it brings with it an often tangled web of additional digital risks. Incorporating multiple players into shared systems ratchets up the potential that one party may open a cyber risk window, allowing in threats that can impact the other parties.

> Third-party exposure to cyber threats, such as contractors plugged into networked systems, has become a contamination risk for Australian assets.

Hackers stole old Sydney Cross City Tunnel data from a third-party service provider in 2023[13]. Researchers hacked into Google Australia's Pyrmont headquarters in 2013, gaining access to the building's blueprints[14].

"There's value in talking with your supply chains, but when you open up access, you lose some of the control," says IFM Investors' Mr Hannam. "The cyber events we've seen in our assets have all come from contractors with access, not to critical asset operational systems which are cordoned off, but to corporate systems like HR, finance and general software as a service," Hannam notes. The hard lesson for many asset owners and operators is to remain vigilant not only about their own cyber risks but also those of their contractors and partners.



"The cyber events we've seen in our assets have all come from contractors with access, not to critical asset operational systems which are cordoned off, but to corporate systems like HR, finance and general software as a service."

Peter Hannam

Complexity Driver 3

Security

The increasing sophistication of cyber threats against digitally connected infrastructure, energy and utilities assets is making headlines worldwide. Australian assets too are being targeted as geopolitical tensions and trade disputes have intensified in recent years. Consequently, the pool of asset owners and investors subject to cyber resilience regulatory and compliance obligations is growing. While the implications for investors considering Australian assets are continuing to play out.

Cyber risk is increasing

Australian asset developers and owners have been managing cyber risks for decades, but the growing volume and sophistication of cyber threats is heightening their focus on safeguarding both their assets and Australia's national security. Extortion-based ransomware attacks and malicious, sometimes politically-motivated, hacks pose the most frequent threats[15].

The Australian Signals Directorate (ASD) reports that internet-connected critical infrastructure networks in Australia have become a deliberate target for "state cyber actors"[16], the hacking groups supporting foreign government espionage activities such as those in China and Russia. The ASD warns that attacks and infiltration of Australian infrastructure networks will increase as the assets themselves "grow in size and complexity"[17]. The number of cyber security incidents against critical infrastructure grew to 143 in the 2022-23 financial year, compared with 95 incidents the year before[18].

In a Lowy Institute poll, 70 per cent of Australians nominated cyberattacks as the leading threat to the country[19]. This fear is well-founded. Recent cyberattacks on Australian infrastructure assets include a coordinated attack on Energy One's Australian and United Kingdom systems, causing a data breach in 2023.[20] Similarly, Queensland's CS Energy found its corporate network hacked in 2021.[21] Infrastructure services provider Ventia's systems were taken offline in July 2023 following a cyberattack[22]. Stevedore DP World Australia shut down its container terminals in late 2023 following an attack disrupting its trucking and terminal communications[23].

For infrastructure asset owners and operators, managing the risk of being digitally connected comes at a cost. Cyber insurance premiums have tripled and, in some cases, quadrupled[24].

How technology diplomacy can protect infrastructure

The flare up in geopolitical tensions between China and Australia since the COVID-19 pandemic has heightened awareness of potential cyber risks in Australian supply chains.

Keeping potentially problematic foreign interests out of critical infrastructure supply chains has been bipartisan Australian government policy since banning Huawei from providing technology to the country's 5G telecommunications networks in 2019[25]. Australia's decision to use 'tech diplomacy' in this way stemmed from worries that China could use its equipment for surveillance or to lock the country into technological dependency[26].

Similar concerns have been levelled at Chinese-made solar panel inverters, millions of which are connected online through smart home energy systems in Australia. The Cyber Security Cooperative Research Centre warns that the ubiquity of connected inverters has increased the vulnerability and "cyberattack surface" of Australia's electricity grid[27].

Fears about embedding malicious code in Australian infrastructure through equipment backdoors are gaining prominence. Australian cybersecurity agencies, and those of its allies, confirmed just such a threat in July 2024[28]. The Australian Signals Directorate shared intelligence about a Chinese state-sponsored hacking group, APT40, sometimes known as Volt Typhoon, infiltrating Australian infrastructure networks with the aim of sabotaging them in the future.

Australia's expanding infrastructure cybersecurity regulatory regime

As cyberthreats have heated up, so too has the Australian government's regulatory response. The definition of 'critical infrastructure' has been widened to include assets that may never have had to consider national security implications.

In 2021, the *Security Legislation Amendment (Critical Infrastructure) Act 2021 expanded the scope of Australia's Security of Critical Infrastructure* (SOCI Act) to include additional sectors such as energy, communications and transport.[29] The legislation requires asset owners to comply with cybersecurity protections, risk management plans, reporting and cyber incident disclosure obligations and makes company directors liable for failures to safeguard assets[30]. The SOCI Act also permits the government to step in to assist private assets to respond to critical threats[31].

For many infrastructure operators, these laws have created a new overlay of reporting and compliance obligations they have not had to contend with before. "Traditionally, operating technology such as sensors, cameras and fans have not been factored into cyber security considerations," says Mr Newcomb. "Consequently, many asset owners and operators have large compliance gaps to fill." The SOCI Act requires asset owners and operators to apply the same cyber security governance and controls to OT systems as they apply to IT systems[32]. The added compliance costs will be a factor for asset owners and investors as developers price these new risks into their bids[33].

> "Traditionally, operating technology has not been factored into cyber security considerations. Consequently, many asset owners and operators have large compliance gaps to fill."
>
> Simon Newcomb

Third party risk imposes an additional layer of obligations on organisations. "With many compliance activities already underway, these need to be considered as well," says Brenton Steenkamp, lead partner of Clayton Utz's cybersecurity practice. "Many businesses are still using legacy technology systems that may not have been upgraded or replaced. The push to digitise systems often means relying on third party support and services, which can increase the 'attack surface' of cyber and data related incidents," says Mr Steenkamp. Responsible oversight should therefore also extend to the risks third party providers bring.

More is yet to come. The Australian government aims to be the 'most cyber secure nation by 2030',[34] with additional legislation on the country's cybersecurity strategy being drafted at the time of writing[35].

Asset recovery is key

> "We're now planning to make sure our infrastructure assets, whether they're electricity or gas networks, or a toll road, are always available, because that's the consumer expectation."
>
> Peter Hannam

Compliance aside, for investors, the most important priority is to minimise asset downtime due to cyber incidents. "We're now planning and investing in resilience and recovery frameworks to make sure our infrastructure assets, whether they're electricity or gas networks, or a toll road, are always available for use, because that's the consumer expectation and how we maximise our returns," says Mr Hannam. "If we can minimise downtime, we can maximise the valuation of an asset in a bid-style situation," he adds.

Protecting against risks is perennial, but as the water utility for Australia's capital city, Icon Water is placing increasing effort on its cyber resiliency, says Dr Pollock. "While we continue to invest in protecting our assets and detection of incidents, it's really about our response and recovery to ensure we have programs in place to isolate incidents and bring systems back up as quickly as we can," says Mr Pollock.

Implications of Australian cyber scrutiny for foreign investors

Australia's emerging era of digital complexity will increasingly impact offshore investors interested in infrastructure, energy and utility opportunities. In its Future Made in Australia Act, the Australian Government set out its intention to increase scrutiny on foreign investment proposals for critical infrastructure and investments involving sensitive data sets[36]. The Foreign Investment Review Board (FIRB) is increasingly focused on the data governance implications of foreign investment transactions, says Mr Sukari. "The FIRB want to know what data security controls are in place, how much data an asset has, where it's stored and how it's handled, as well as broad questions like how asset owners may make changes in relation to data," he says. Asset owners can expect deal times to blow out as a consequence as the increased scrutiny slows down the foreign investment approval process.

> While data sovereignty concerns are a drag on deal certainty for foreign investors, they can be an advantage for domestic infrastructure investors.

Investors who can demonstrate their credentials as digitally responsible asset owners enjoy a smoother approvals process. Others, however, will find their market opportunities curtailed. "Digitising early and closely aligning data and information security gives the business the confidence to assess the right projects to bid on, especially in new emerging markets such as renewable energy," Mr Erickson says.

A checklist of questions to ask in vendor negotiations:

- What are the support arrangements? Does the vendor have people available locally to provide support and what's the pricing of the support structure?
- What are the arrangements for future upgrades to the software?
- What rights does the asset owner have to implement modifications themselves to the software?
- What access does the asset owners have to source code if at some point the relationship sours, or if there's an insolvency or an obsolescence?
- What happens if the tech becomes obsolete? What continued support will be provided, and what ability is there to replace it with new tech solutions?
- What are the ownership rights if a bespoke solution is being developed? Can asset owners use it on other projects?
- What technologies are contractors using that connect to an asset's systems?

Learn more

To find out more about procurement models and managing risk in digitally-connected infrastructure, energy and utilities assets visit our Digital Economy Hub

Read more about the ways private equity is adapting to a volatile economic climate in our report *A New PE Playbook: Economic Headwinds Spur Private Equity Evolution*

Get in touch

Paul Sutherland
Head of External Communications

T: +61 434 136 256
psutherland@claytonutz.com

End notes

1. Joris Toonders, Data is the new oil of the digital economy, Wired, 31 October 2017, link
2. IFM Investors, Embracing the Infrastructure Revolution: Siezing present opportunities and adapting for the future, Infrastructure Outlook 2024, link
3. Economist Impact, Across the procurement-verse: changing trends in the procurement function, 2024, link. Survey of 2307 C-suite executives.
4. Consult Australia, *Confidence and continuity report*, 13 May 2024 link. Survey of 23,510 industry association members in 2024.
5. IFM Investors, Harnessing technological trends within infrastructure, Tech Foresight, July 2022, link
6. Cyber Security Cooperative Research Centre, Smart Airports, link
7. Australasian Rail Industry Awards, August 2024, Australasian Railway Association, link
8. Ry Crozier, *Endeavour Energy to create digital twin of its electricity network*, IT News, 15 Dec 2021, link
9. KPMG, Emerging trends in Infrastructure, 2024 link
10. Cooper Veit, Michael Poppler, Viraj Deokar and Jess Dyroff, The AI patent gold rush — fortunes hinge on IP control, Sherpa Technology Group, 3 January 2024, link
11. Governance Institute of Australia, *Data governance in Australia report,* 2023 link, online survey was deployed in August 2023, n=345.
12. Aerometrex, Cross River Rail Project, link
13. Daniel Croft, *Sydney's Cross City Tunnel attacked by Russian state-sponsored hackers*, Cyber Daily, 14 Jun 2023, link
14. Kim Zetter, *Researchers Hack Building Control System at Google Australia Office*, Wired, 6 May 2013
15. Digital Nation, As our nation goes digital, critical infrastructure entities need a renewed focus, 15 February 2024 link
16. Australian Signals Directorate, Cyber Threats Report 2022-2023, November 2023, link
17. Australian Signals Directorate, 2022-2023 Cyber Threat Trends for Critical Infrastructure, link
18. Australian Signals Directorate, Cyber Threats Report 2022-2023, November 2023, link
19. Lowy Institute, *Lowy Institute Poll 2024*, link. National survey of 2028 Australians deployed between 4-17 March 2024.
20. David Carroll, *Cyberattack highlights energy grid security concern,* PV Magazine, 22 August 2023, link
21. Julian Bajkowski, ASD reveals foreign state hackers hit Australian 'energy provider', The Mandarin, 4 November 2022 link
22. Ventia, 7 July 2023, link
23. Jenny Wiggins, Nick Bonyhady, Ronald Mizen and Euan Black, *DP World hack strands 30,000 shipping containers*, Australian Financial Review, 12 Nov 2023, link
24. Digital Nation, B*oardroom Impact: Critical Infrastructure and Cybersecurity, 2024* link
25. International Institute for Strategic Studies, Australia, Huawei and 5G, October 2019 link
26. Bronte Munro, Australian Strategic Policy Institute, *Tech diplomacy: what it is, and why it's important,* The Strategist, ASPI, 8 May 2024 link
27. Rachael Falk and Anne-Louise Brown, Power Out: Solar inverters and the silent cyber threat, Cyber Security Cooperative Research Centre, link
28. Australian Signals Directorate, *APT40 Advisory: PRC MSS tradecraft in action*, 9 July 2024 link
29. Clayton Utz, *Reforms to Security of Critical Infrastructure legislation to significantly impact management of cyber risk*, 9 June 2022 link
30. Australian Government, Department of Home Affairs, *2023–2030 Australian Cyber Security Strategy*, Action Plan, 2023, link
31. Kate Weber, *Dept Home Affairs continues building out the SOCI Act*, Digital Nation, 3 May 2024 link
32. Digital Nation, As our nation goes digital, critical infrastructure entities need a renewed focus, 15 February 2024 link
33. KPMG, Emerging trends in Infrastructure, 2024 link
34. Melissa Coade, *Cyber security: coordinator calls for improved response,* The Mandarin, 6 June 2024, link
35. Tom McIlroy, *Cybersecurity: Home Affairs Minister Clare O'Neil says cyber is the fasted growing threat to national security*, Australian Financial Review, 23 July 2024 link
36. Phil Coorey, *Jim Chalmers' plan to unlock foreign investment*, AFR, Apr 30, 2024 link

CLAYTON UTZ

claytonutz.com