Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Critical Infrastructure Annual Risk Review

Second Edition
November 2024

Contact us

Enquiries regarding the licence and any use of this document are welcome to enquiries@CISC.gov.au, or:

Critical Infrastructure Security Policy Branch
Department of Home Affairs
PO Box 25, BELCONNEN, ACT 2616

Contents

Foreword

I am pleased to introduce the Australian Government's second edition of the Critical Infrastructure Annual Risk Review, a product that reflects on the breadth of threats and hazards facing Australia's critical infrastructure, and addresses emerging and persistent risks impacting Australia's national security and economic stability.

This Critical Infrastructure Annual Risk Review serves to support a greater shared understanding of the risks faced by critical infrastructure owners and operators which, if not addressed, could impact the essential services all Australians rely on.

Owners and operators of critical infrastructure need to maintain clear visibility of the extent of risks they face, including from cyber, personnel and physical threats, and from supply chain hazards and natural disasters. This review was designed to reach a diverse audience across all levels of enterprise, government, and the broader community.

This year saw a number of cyber security incidents impact Australia's critical infrastructure, caused inadvertently through human error or system failure, as well as from malicious activity. The consequences of incidents are increasingly causing enduring impacts beyond the initial disruption leading to longer-lasting disruption to capabilities. The incidents that have impacted Australia this year exemplify the vulnerabilities of interconnected networks and how cascading effects can flow through critical infrastructure dependencies, disrupting critical functions.

Conflict and severe weather events have highlighted the vulnerability of domestic and international supply chains to disruptions, impacting supply lines and the availability of critical materials. Ensuring that resilience is built into how critical infrastructure delivers its services has never been more important.

The Cyber and Infrastructure Security Centre collaborates in the spirit of genuine partnerships with governments, industry and the broader critical infrastructure community, to safeguard Australia's critical infrastructure and to help critical infrastructure owners and operators to augment their understanding of the risk environment, while meeting their security obligations. Following extensive collaboration, I have also introduced the Cyber Security Legislative Package to parliament, which serves to address legislative gaps and take the next step to ensure Australia is on track to become a global leader in cyber security. Subject to the passage of this legislation, Australia will have its first standalone Cyber Security Act, and the package will also progress and implement reforms under the *Security of Critical Infrastructure Act 2018* (SOCI Act).

Our industry partners should be applauded for the steps already taken to enhance the security of their critical infrastructure assets through targeted investments to recognise and address vulnerabilities, harden their systems and secure their data. Through strong industry partnerships, we will enhance risk maturity, meet regulatory obligations and achieve our vision of becoming a world leader in cyber security by 2030.

Together we will build a more secure, prosperous and resilient nation.

The Hon. Tony Burke MP
Minister for Home Affairs, Minister for Cyber Security

About the Cyber and Infrastructure Security Centre

The Cyber and Infrastructure Security Centre (CISC) in the Department of Home Affairs works with government partners and industry stakeholders to maintain a comprehensive and sustainable all-hazards critical infrastructure protection regime. We actively assist Australian critical infrastructure owners and operators to understand the risk environment and meet their regulatory obligations for the shared benefit of all Australians.

Our role as a regulator

We are committed to being a best-practice regulator. The CISC is responsible for the regulation of critical infrastructure assets under the:

- *Security of Critical Infrastructure Act 2018* (SOCI Act)
- *Telecommunications Act 1997* (Part 14)
- *Aviation Transport Security Act 2004*
- *Maritime Transport and Offshore Facilities Security Act 2003*.

Our programs and regulatory functions are developed to mitigate risks commensurate with the current threat environment. In 2024-25, the CISC's SOCI Act compliance regulatory posture will aim to balance educational and awareness-raising activities with compliance activities. The CISC also administers the *AusCheck Act 2007*.

Our mission

Our mission is to collaboratively ensure the security, continuity and resilience of Australia's critical infrastructure.

The CISC supports the security and resilience uplift of Australia's critical infrastructure assets and supply chains by ensuring owners and operators have robust security practices in place to identify, prevent and mitigate all-hazards risk.

We support our stakeholders using a dynamic and collaborative approach to engagement, partnerships, guidance, exercises, modelling, compliance and enforcement.

We leverage expertise

Responsibility for critical infrastructure security is shared between government and industry. We leverage government partner and industry stakeholder expertise to understand the operating environment and develop best-practice approaches and advice.

We leverage partnerships and facilitate engagement to prepare for potential incidents by supporting industry to develop robust risk management strategies to safeguard assets and ensure the reliable delivery of essential services needed for all businesses to plan, grow and thrive.

We engage with industry through town halls, webinars, podcasts and social media. We provide guidance material to support our stakeholders, and we host events, including the Critical Infrastructure Security Excellence, Workshops and the biennial national conference to engage with critical infrastructure partners across Australia.

Trusted Information Sharing Network

The TISN is the primary forum for connecting owners and operators of Australian critical infrastructure with all levels of government, who work together to enhance the security and resilience of critical infrastructure.

The TISN focuses on key critical infrastructure sectors in Australia and brings together not only owners and operators with government, but also peak bodies, academics, subject matters experts and supply chain entities. The network is a trusted, non-competitive environment for the critical infrastructure community to better plan, prepare, respond and recover in the face of all-hazards.

Since its creation in 2003, the TISN has evolved to be a sophisticated network with an all-hazards and all-sectors approach, providing flexible collaboration and multilateral engagement for members.

For further enquiries please contact us at:

enquiries@cisc.gov.au

Introduction

The second edition of the CISC's Critical Infrastructure Annual Risk Review outlines the key risk-driven issues that have impacted the security of Australia's critical infrastructure in 2024.

Risk issues for each of the hazard categories outlined in the SOCI Act and accompanying rules for the *Critical Infrastructure Risk Management Program* (CIRMP) are included in the review.

A challenging risk landscape

In the 2023 edition of the Annual Risk Review we identified that high levels of cyber incidents, instability in global supply chains, ongoing workplace skills shortages and disruption from severe weather events were key areas of concern for the security of Australia's critical infrastructure. In 2024, this has continued, with an emergence of new risk challenges.

Frequent cyber incidents have permeated across all critical infrastructure sectors, causing stoppages or disruptions to the integrity, availability or confidentiality of some infrastructure providers for periods of time.

Ongoing **foreign interference** of our critical infrastructure, including the targeting of vulnerable personnel and exploiting of new technology such as artificial intelligence (AI), is a principal security concern. Insider threat and risk management strategies will need to adapt.

The threat of **politically motivated violence** has elevated, including violence affecting our critical infrastructure. In August 2024, the Australian Security Intelligence Organisation (ASIO) raised the National Terrorist Threat Level to PROBABLE.

Ongoing **global conflicts** continue to target critical infrastructure through direct military action and the use of grey zone tactics. Our global supply chains are being frequently disrupted by conflict, trade disputes and natural hazards, which will persist into 2025.

Natural hazards events contributed to widespread service outages across Australia in 2024. Of note, severe storms and wind in Victoria disrupted energy and communication networks, and flooding cut off key supply chains in and out of Western Australia. A changing climate will require changes and resilience built into how critical infrastructure delivers its services.

Our social and economic **interconnectivity** and rapid implementation of technologies is changing the nature of threats to national security, and introducing new, unconventional ones.

Challenges exist between and within sectors where there is a wide disparity in security maturity levels, regulation, approaches to information-sharing and disclosure, and where retrofitting new technological efficiencies into legacy infrastructure takes place.

National security risk is business risk

Incidents affecting critical infrastructure have consequences for national security. We are seeing disruption to capabilities compounded when critical infrastructure is impacted, even if critical operations were not initially targeted or affected.

For example, cyber attacks that steal operational or personal information might not immediately disrupt delivery of critical services, but they can create a wider decline in reputation and confidence, not only for the entity impacted but also for other critical infrastructure sectors.

Targeting critical infrastructure could be used as a tactic to break down confidence in the nation's ability to deliver critical services, or even to demonstrate a foreign state's power to influence public support for conflict or support of allies.

Critical infrastructure providers already manage a wide range of risks to their operations. A focus on national security risk may differ from the way entities have viewed risk in the past (for example, with financial or shareholding interests as a focal point). However, a framing of risk in this context (within existing risk management strategies) will improve Australia's national security and socioeconomic resilience.

Interdependency exposes critical infrastructure to risk outside areas of control

It is easy to presume that our essential goods and services will always be available, and that the processes behind delivery are simple and predictable. When we need water or electricity, we simply turn on the tap or a switch. We tend not to consider the numerous natural and built systems and processes that ensure we get that product or service. We do not have a complete picture of the increasing number of ways the systems we rely on can be disrupted, nor of the full range of processes and end users supported by a product or service.

Interconnectivity delivers measurable benefits, such as more efficiency, less resource use and the ability to automatically correct errors. However, interconnected networks may also involve more threat exposure, more severe consequences, unpredictable system behaviour, and more difficult recovery from disasters.

Some critical infrastructure networks are complex and impossible to model accurately, with complicated global supply chains, energy and communications dependencies and the use of AI and automation in operational decision-making.

The resilience of infrastructure systems depends on all the connected systems, including third-party systems, and involves critical operational, corporate, physical and digital systems. In heavily interdependent networks it is almost certain that unanticipated failures will occur.

We need to expect and prepare for the unexpected.

Overview of methodology for cross-sector risk prioritisation

This report introduces a comparative visualisation of cross-sector risk prioritisation for each of the 5 hazard sections: Cyber/Information, Supply Chain, Physical, Natural Hazard and Personnel.

Each graphic (Figs.2–6) plots the risk issues identified in this report under each hazard category against the CISC's assessment of plausibility and damage. This may assist critical infrastructure owners and operators in the prioritisation of risk mitigations within and between each type of hazard.

This assessment draws on CISC's insights into the national critical infrastructure risk landscape and reflects an all-hazard approach. It is based on the following components:

- **Plausibility.** Reflects risk likelihood, based on CISC's assessment of a threat or hazard impacting critical infrastructure sectors. Plausibility considers the threat or hazard and also the vulnerability of sectors to that threat or hazard.
- **Damage.** Reflects CISC's assessment of the broad consequence for critical infrastructure sectors, based on worst-case impacts that could arise from the threat or hazard.

Critical Infrastructure Risk and Regulation

The CISC is the Commonwealth regulator for critical infrastructure security and supports organisations to better understand risks within the broader national security context, and assist them to adapt their existing risk practices accordingly.

In the CISC's *Critical Infrastructure Resilience Strategy 2023*, critical infrastructure is defined as:

> *"...those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security."*

In the context of national critical infrastructure, risk is related to our national and societal resilience. Disruptions to critical infrastructure can have serious implications for business, governments and the community, affecting the security of resources, supply and service continuity, and damaging our economic growth.

Assessing risk for national critical infrastructure

Risks that impact the social or economic stability of Australia or its people, or have the potential to undermine Australia's national security and resilience, need to be considered and framed within critical infrastructure providers' existing risk management strategies.

For critical infrastructure owners and operators, an all-hazards approach to determining risk is necessary. All-hazards is an integrated approach to risk management, preparedness and planning that focuses on businesses enhancing their capacity and capability to protect against a full spectrum of threats and hazards to Australia's critical infrastructure.

An all-hazards risk assessment considers human-sourced threats and natural and environmental hazards that could impact on a critical infrastructure provider and their operations. In Australia's evolving critical infrastructure risk environment, this is needed to fully understand potential compounding and cascading effects on national resilience.

CIRMP and hazard definition

The CISC drives an all-hazards critical infrastructure approach to risk assessment in partnership with governments, industry and the broader community.

The SOCI Act and its accompanying CIRMP may require or highly recommend that responsible entities establish, maintain, and comply with a written risk management program that identifies and takes steps (so far as is reasonably practicable to do so) to minimise or eliminate material risks that could have a relevant impact on their critical infrastructure assets.

This review highlights risk issues under the 5 hazard categories defined in the SOCI Act and CIRMP. Collectively, these issues capture CISC's overview of the critical infrastructure risks of the last 12 months.

Relevant impact

Critical infrastructure owners and operators face a wide range of disruptors to the continuity of operations and are uniquely positioned to assess material risks in the context of their own systems and vulnerabilities.

Assessing whether a risk is a material risk considers both the likelihood of a hazard occurring and the relevant impact. This includes direct or indirect impacts on the availability, integrity or reliability of a critical infrastructure asset, as well as the confidentiality of associated data or information.

For example, a data breach may have an immediate impact on data confidentiality and availability; however, the integrity of data and information may also be impacted (including through misinformation and disinformation) and needs to be considered as a material risk.

Proper consideration and assessment of the full extent of the relevant impact can help prioritise mitigation efforts in order to protect the critical infrastructure asset and gain the greatest return on mitigation investment.

What we are doing

The CISC remains committed to the continued improvement of our regulatory and policy approach to securing Australia's national critical infrastructure and is collaborating with industry to achieve the best security and resilience posture.

Effective compliance activities support an objective of the SOCI Act to provide a framework for managing risks relating to critical infrastructure.

Helping industry understand the implications of these obligations, and ensuring compliance, is not just a matter of legal obligation; it is necessary to protect the essential services all Australians rely on.

Over the last 12 months, the CISC has been working on:

- Legislative reform to strengthen the SOCI Act to ensure it is fit for purpose and includes the telecommunications sector security obligations under one Act
- Legislative reform that will strengthen Australia's aviation, maritime, and offshore facility security settings against current and emerging threats, and enable government to regulate in a flexible, risk-based and scalable way. This includes the introduction of all-hazard security obligations to existing security legislation
- Guidance to critical infrastructure providers to carefully consider risks to operational and information technology networks
- Promoting greater consideration of the impact of risk on assets, and how this cascades to other entities or sectors
- Positioning our SOCI compliance regulatory posture, over the next 12 months, to provide balanced educational and awareness raising activities and compliance activities.

CIRMP Hazard Definitions

Cyber and Information security hazard includes where a person, whether authorised or not: (a) improperly accesses or misuses information or computer systems about or related to the critical infrastructure asset; or (b) uses a computer system to obtain unauthorised control of, or access to, the critical infrastructure asset that might impair its proper functioning.

Supply Chain hazard includes malicious actions to exploit, misuse, access or disrupt the supply chain; an over-reliance on particular suppliers, and other disruption from issues in the supply chain, including a failure or lowered capacity of supply.

Physical security hazard includes the unauthorised access to, interference with, or control of CI assets, to compromise the proper function of the asset or cause significant damage to the asset.

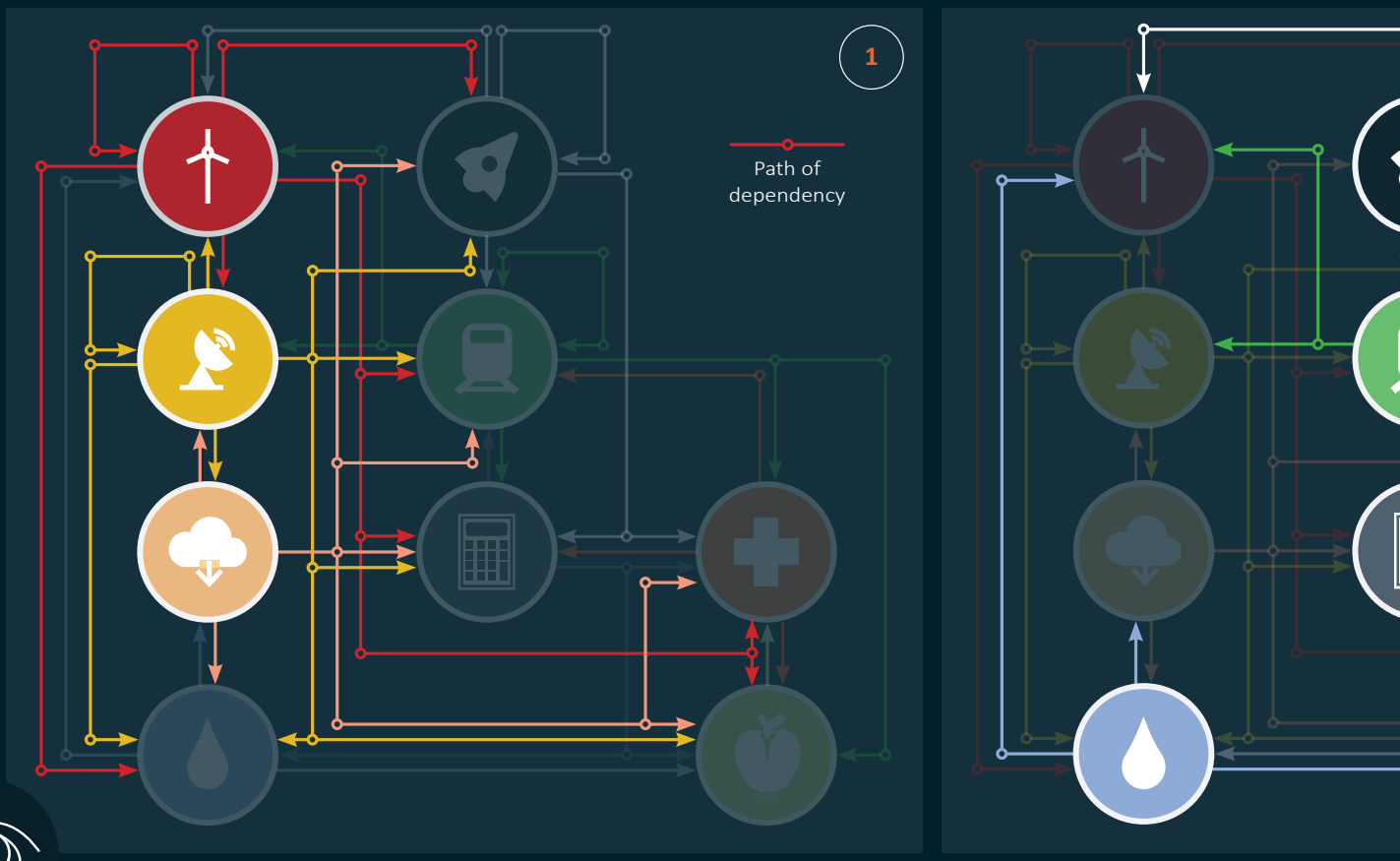
Natural Hazard includes damage or disruption from fire, flood, cyclone, storm, heatwave, earthquake, tsunami, space weather or biological health hazard (such as a pandemic).

Personnel security hazard includes where a critical worker acts, through malice or negligence: (a) to compromise the proper function of the asset; or (b) to cause significant damage to the asset.

Sector Interdependency

The following illustrated example (Fig.1) demonstrates how cascading effects might flow through critical infrastructure dependencies following the impact of a severe storm weather event. The nature of sector interdependencies can be a factor in whether or for how long part or all of a capability is disrupted.

If, for example, the Energy and Communications sectors were directly impacted by a natural hazard event like this, it is likely cascading effects would cause disruption to most other sectors. Initial sectors impacted may also face prolonged delays in recovery due to supply–demand imbalances or



Energy Sector outages, such as a transmission network or generation failure, would quickly cause outages and disruption across most sectors.

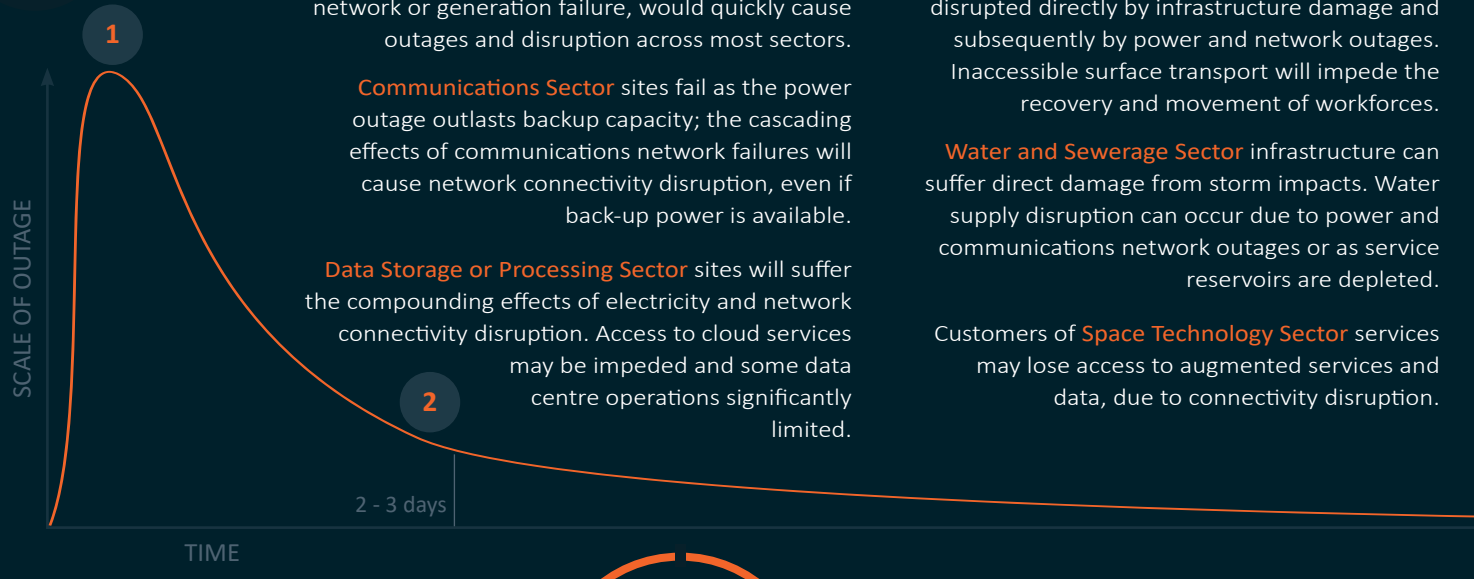
Communications Sector sites fail as the power outage outlasts backup capacity; the cascading effects of communications network failures will cause network connectivity disruption, even if back-up power is available.

Data Storage or Processing Sector sites will suffer the compounding effects of electricity and network connectivity disruption. Access to cloud services may be impeded and some data centre operations significantly limited.

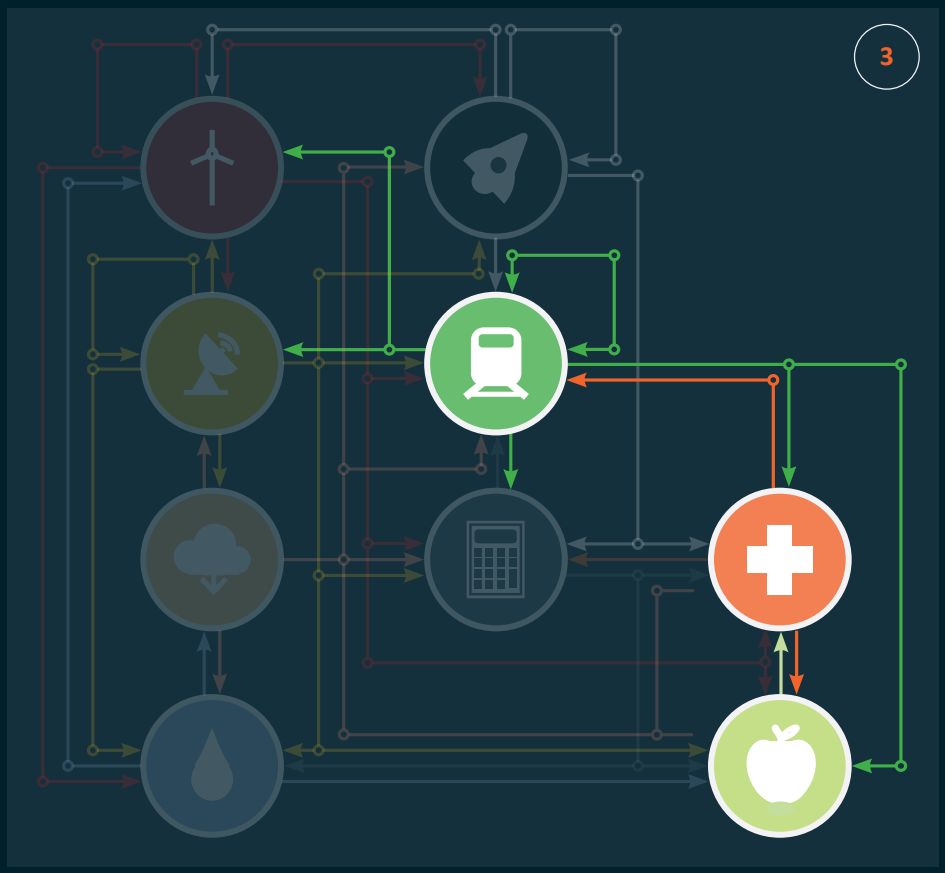
Transport Sector sites, networks and routes are disrupted directly by infrastructure damage and subsequently by power and network outages. Inaccessible surface transport will impede the recovery and movement of workforces.

Water and Sewerage Sector infrastructure can suffer direct damage from storm impacts. Water supply disruption can occur due to power and communications network outages or as service reservoirs are depleted.

Customers of Space Technology Sector services may lose access to augmented services and data, due to connectivity disruption.



through causal impact loops, whereby a failure in one, or part of, a sector disrupts the service or recovery of another. Critical infrastructure networks do not always connect in obvious ways or behave as expected when impacted by a hazard. When a failure lies deep within interconnected systems, behaviour and recovery can be more unpredictable; as such, a capability that an asset is dependent on may not behave as expected during an outage. Similarly critical infrastructure in an impacted area may escape disruption, while others far from direct hazard impact lose services due to unexpected or cascading failures.



Access to Financial Services and Networks Sector payment systems depend on connectivity, and outages can disrupt the ability to make payments or access finances.

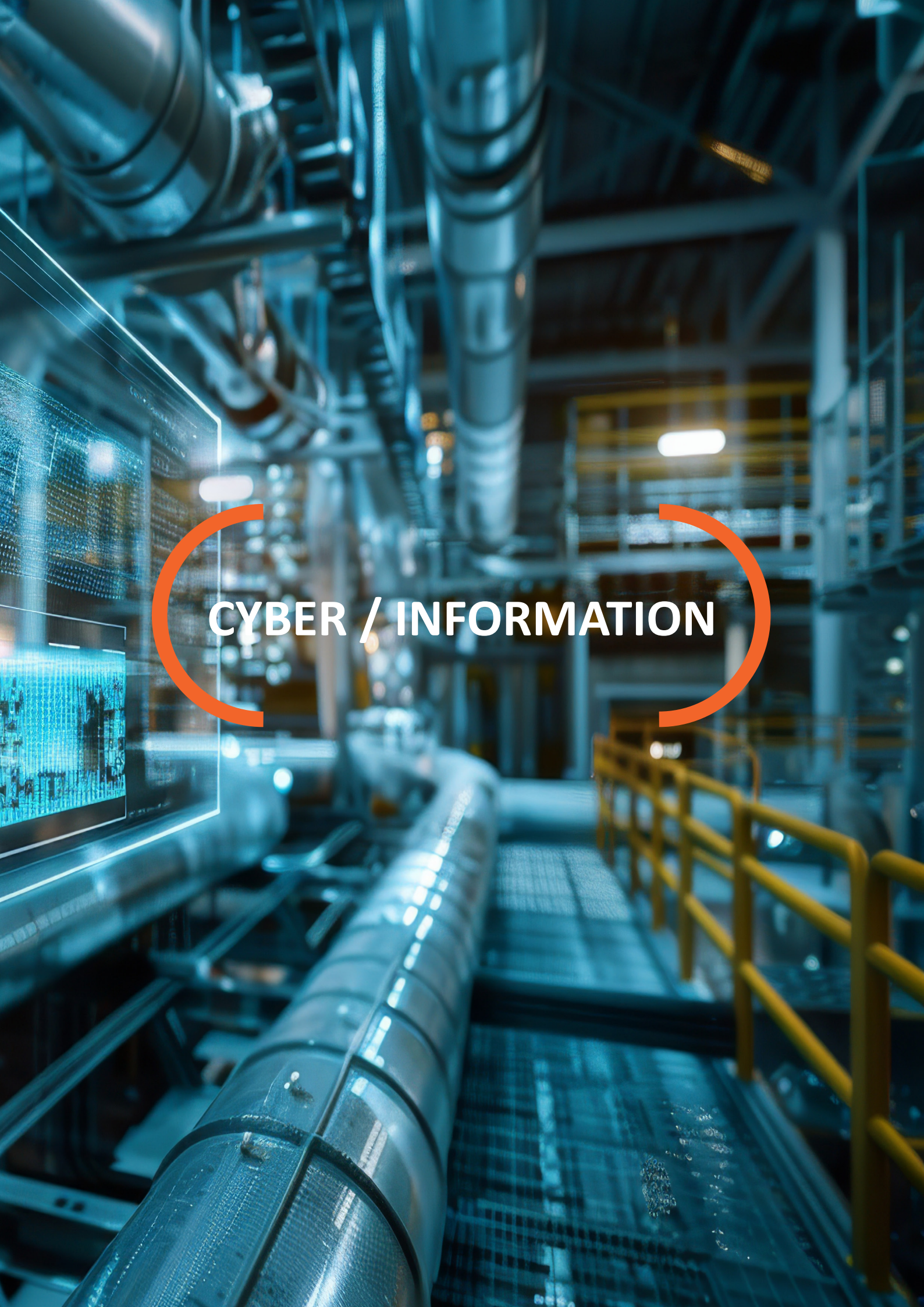
The Transport Sector recovers slowly due to closures and continuing elevated demand, even after restoration of utilities like power, communications and water. Driver availability may remain an issue in the post-incident environment.

The Food and Grocery Sector is impacted by the compounding effects of power failures, transport disruption, communications network and payment system failures, which restrict supply and distribution, continuing after restoration of most services.

The Healthcare and Medical Sector is affected by the compounding effects of power failures, transport disruption, communications network and payment system failure, and possible supply disruption.

Fig. 1. (Above) an illustration of sector interdependencies following the impact of a hypothetical severe weather event

(Below) a typical recovery curve following a major service outage


CYBER / INFORMATION

Cyber / Information

Continuing frequent cyber attacks targeting critical infrastructure have exposed the nexus between national security and business risk. (1)

Among the persistent cyber attacks on critical infrastructure, a number of incidents in Australia have dominated reporting and public scrutiny. The cyber threat to critical infrastructure is pervasive, with the strategic environment characterised by the interconnectivity of critical infrastructure networks and complexity of resilience to an incident.

Both state-sponsored and financially-motivated actors present a high level of threat. Among their objectives are espionage, pre-positioning and financial gain (including through ransomware and data exfiltration). Where data is stolen, personally identifiable information, financial details, corporate files and health information are among the most attractive targets.

The direct business risk arising from a breach of information has been demonstrated by multiple incidents targeting critical infrastructure operators. The increasing size of breaches and the aggregated data being stolen is almost certainly eroding public confidence in the security of critical service delivery, even if operational capability is unaffected by an incident.

The exploitation of data by malicious state and non-state actors, with growing capability and strategic intent, highlights that risk to national security has become closely aligned with breaches of personal and corporate information.

Underestimating the pre-positioning threat will leave critical infrastructure vulnerable to capability disruption or attempts to influence decision-making. (2)

There is growing recognition of the extent that malicious cyber actors seek to target critical infrastructure, not just for cyber espionage or intelligence collection but also to pre-position on networks for future disruption of critical functions (likely to be initiated in the event of a major crisis or conflict).

Reporting on the threat actor called Volt Typhoon (attributed by Five Eyes countries) and their prepositioning of malicious code on United States critical infrastructure illustrates how well-resourced, malicious actors, with significant intent and capability, can gain persistent and ongoing access to systems without detection. Foreign powers and their proxies are demonstrating a high level of skill in deploying cyber capabilities to compromise and hold at risk critical infrastructure systems and assets with limited inherent espionage value, to support broader strategic objectives.

The diversity and constant evolution of infiltration tactics, with purposes ranging from one-off compromise to persistent pre-positioning activities, requires organisations to have a multi-faceted and comprehensive approach to risk management, detection and system hardening that is continually updated to meet new threats.

Large portions of industry are still not meeting basic levels of cyber literacy and awareness. (3)

Human error remains a leading cause of cyber security breaches. Malicious actors continue to exploit human vulnerabilities and a lack of cyber awareness to infiltrate or compromise critical, data-rich systems, often through social engineering of employees. Poor understanding of cyber hygiene and best practice security within an organisation creates vulnerabilities, and can lead to unintentional mishandling or disclosure of sensitive information.

Social engineering manipulates the poor security of individuals in order to gain unauthorised access to systems or data. Despite critical infrastructure operators building awareness of the techniques required for social engineering, the demonstrated success of this form of attack and exploitation of new technologies, means more attention to cyber resilience is required. Meeting basic cyber literacy standards across all aspects of an organisation should be viewed as a principal security measure. Promoting a strong culture of cyber security awareness can help workers to detect and report suspicious activity. This helps to prevent data breaches and to reduce the financial and reputational costs associated with such incidents.

Lack of security coordination between information technology (IT), operational technology (OT) and internet of things (IoT) technologies can make systems more vulnerable to malicious activity. [4]

Malicious actors are exploiting gaps and vulnerabilities as critical infrastructure systems converge. A breach of any system is a risk, but the convergence of IT, OT and IoT systems increases the risk of threat actors moving laterally between systems, compounding the impacts of operational disruption, physical harm or the compromise of sensitive data.

IoT has become a tangible intersection of the digital and physical worlds. The vast number of interconnected devices in IoT-driven infrastructure creates a massive attack surface. These devices often have limited processing power and often do not have the robust security features more common in IT and OT systems.

Improved communication and coordination between OT and IT teams can enhance organisation-wide visibility over their operating environment and enable greater coordination of threat detection, incident response and vulnerability remediation.

Cyber security governance for third-party risk is lagging behind levels of risk awareness. [5]

The number of data breaches stemming from third-party exposure underscores the importance of ensuring third-party relationships are secured commensurate with the security level of the critical infrastructure service provider. Critical infrastructure owners and operators increasingly employ third-party providers to support their operations, and these providers can have varied levels of cyber security maturity.

Malicious actors will exploit vulnerabilities in third-party vendors to infiltrate a target entity, or to conduct cyber operations at scale – to capture, for example, an entity's customer information.

Poor visibility and limited control of third-party vendor security controls and data-handling practices compound the risk arising from these indirect cyber attacks. Establishing clear cyber security expectations and responsibilities within third-party relationships can assist critical infrastructure operators in mitigating such risks.

Rapid uptake of artificial intelligence is enabling more persuasive and individually targeted cyber attacks, complicating mitigation. [6]

AI-driven attacks will further complicate the cyber security environment within Australia. Threat actors are embracing, integrating and evolving the use of AI in their operations. AI is already facilitating the creation of adaptable malware and enabling more realistic and tailored social engineering attacks to manipulate targets.

AI is lifting the capability of all cyber threat actors to conduct attacks at greater speed, scale and effectiveness, and at a rate that may outpace many system defence capabilities.

Less skilled threat actors are leveraging the increased commercialisation and public availability of AI tools to deploy ransomware, create deep fakes or conduct low-effort, yet high-yielding social engineering campaigns. These can be highly convincing and difficult to distinguish from authentic interactions, making detection efforts increasingly challenging for organisations and individuals.

Case Study

Over the last 12 months, cyber attacks on Australia's critical infrastructure, most notably in the communications, healthcare and higher education sectors, have elevated business disruption as a clear national security risk.

Breaches of large amounts of personal and sensitive information have resulted in significant financial and reputational impacts on some of Australia's prominent critical infrastructure providers. The effect on public perception of the reliability of these operators in some instances has been long-lasting.

Continued large-scale data breaches nationally can have the cumulative effect of eroding public trust in our ability to securely deliver critical infrastructure. Although these recent events have primarily been financially motivated, foreign powers and their proxies may target perceptions of reliability and trust to influence public support and government decision-making.

CROSS-SECTOR RISK PRIORITISATION FOR THE CYBER / INFORMATION THREAT

Fig. 2 highlights the Cyber/Information risk issues with a comparative visualisation of plausibility and damage for all-hazard risk issues in this review.

Over the last 12 months, risks arising from cyber and information security hazards are among the most plausible and damaging compared to other hazards.

Cyber attacks are persistent, and because of the different operational requirement across critical infrastructure sectors, impacts can vary significantly.

The potential for more damaging impact exists in cyber threats that are pre-positioned to maximise effects, or where breaches provide access to multiple systems.

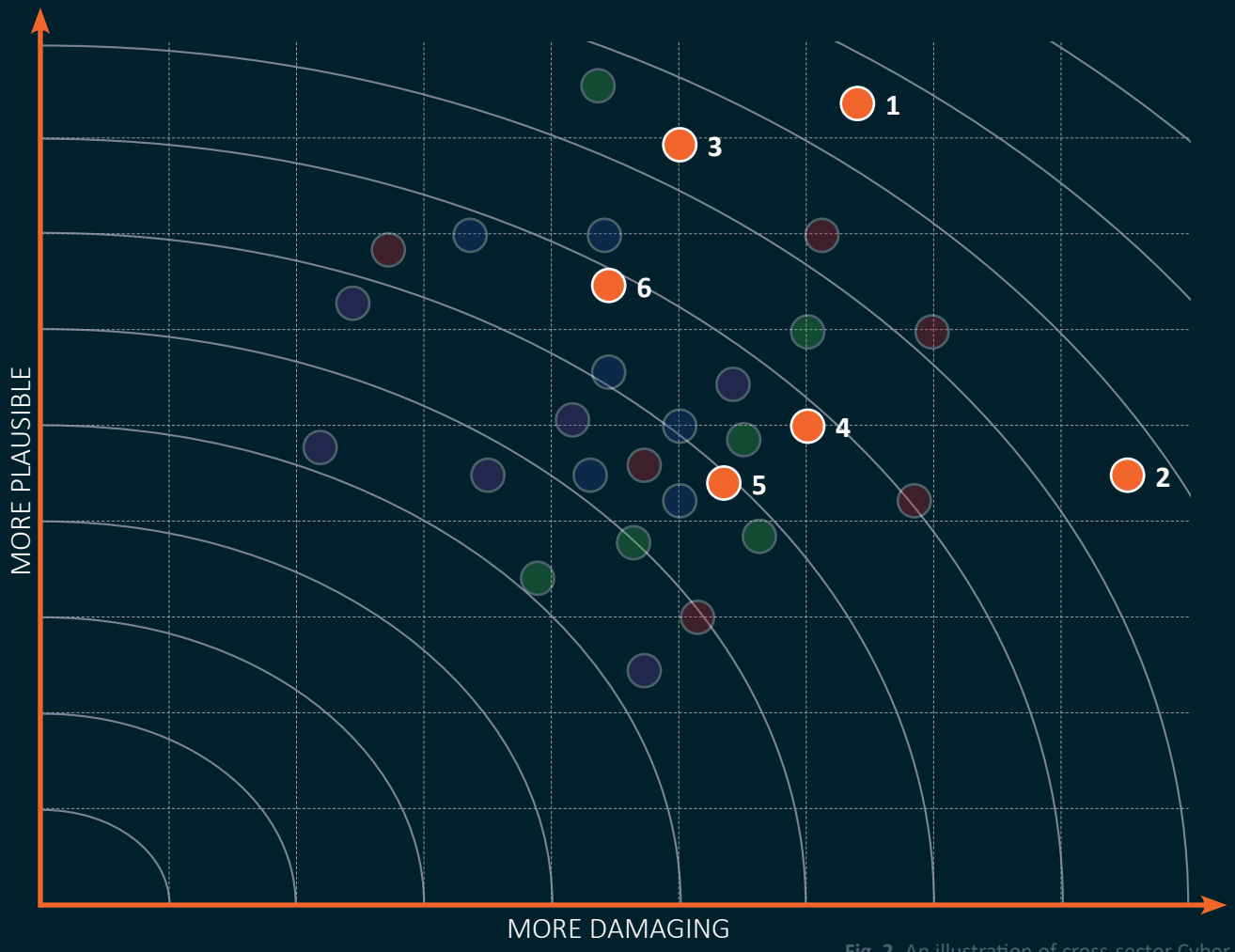


Fig. 2. An illustration of cross-sector Cyber and Information risk prioritisation considering risk plausibility and damage

1 Large-scale data breaches

2 Pre-positioned cyber threat

3 Poor cyber literacy and awareness

4 IT/OT/IoT convergence flaws

5 Third-party cyber risk

6 AI augmented cyber threat


SUPPLY CHAIN

Supply Chain

Geopolitical issues are expediting a need for supply chain shift. [7]

A geographic concentration of the production, fabrication and manufacture of critical technologies, components and resources creates a significant supply risk for Australia's critical infrastructure.

For example, the production of solar panels, batteries and semiconductors is highly concentrated geographically. Disruption (whether due to natural hazards, conflict, significant demand surge, or domestic policy changes) can result in price rises, increased lead times, or even cessation of supply. The limited domestic manufacturing capability for many critical components impedes flexibility to pivot to alternative suppliers to minimise disruption.

In mitigating supply chain risk, there is danger that excessive focus on supply chain paths could result in overlooking risk arising from supply sources and key nodes (e.g. ports, distribution hubs, warehousing). Supply shift and increasing supply diversity may be important proactive resilience measures for positioning a business to quickly transition or respond to supply disruption.

The clean energy transition will drive demand and increase competition for the required technology and materials. [8]

As global economies shift to depend more on renewable electricity generation, technological transformation is driving demand for solar panels, wind turbines, storage and other technologies. There is greater competition for resources and components such as rare-earth metals, semiconductors, silicon wafers, and lithium-ion batteries.

The transition is affecting a number of sectors, most obviously energy and transport, including their upstream and downstream dependencies.

Critical infrastructure owners and operators will need to monitor transitional impacts and manage supply chain risk with a view to how future energy and transport systems will affect operations.

Australia's dependence on global maritime supply lines leaves Australia highly vulnerable to impacts outside of our control. [9]

Supply chains to and from Australia are primarily reliant on maritime supply lines. Over the last 12 months, multiple events have impacted maritime trade, resulting in downstream impacts on Australia's supply chains. Regional destabilisation in the Middle East, disrupting Red Sea and Gulf of Aden supply lines, have increased insurance costs and resulted in longer routes, investor uncertainty, shipping delays, shortages and higher supply costs.

Within Australia, a number of threats and hazards have impacted container ports responsible for receiving incoming goods, including cyber attacks, protest activity, and tropical cyclones.

Upward freight pressures on maritime supply lines are likely to continue in the medium term, exacerbated by increasing demand for critical materials and components. Pouring more and more freight into an already tight supply chain crunch is resulting in financial impacts and delay. The system of globally interconnected maritime freight paths and nodes means a problem in one area is likely to cause problems in other parts of the network.

Australia's high reliance on road and rail for domestic supply compounds any disruption to this infrastructure. [10]

Australia's domestic supply lines remain dependent on a network of surface transport infrastructure, much of it planned and built well in the past. The wide distribution of major cities, maritime port locations and regional centres in Australia means road and rail transport are vital to onshore supply chains, limiting options to mitigate this reliance.

Evolving supply and distribution operations and practices can also contribute to vulnerability across sectors. For example, just-in-time delivery, increasing automation, long supply lines and supplier rationalisation highlight significant dependence on some critical supply nodes.

When major freight corridors are disrupted, freight providers must use detours and alternative routes, resulting in costly delays or shortages of supplies. In March 2024, both the Trans-Australian Railway and Eyre Highway were cut by flooding, significantly disrupting supply between eastern and western Australia, affecting inputs to other critical infrastructure.

More awareness of software supply chains is required.[11]

Complex and interconnected supply chains for software, third-party IT and associated services can provide opportunity for, and obscure the activities of, malicious actors.

Although exposed to threats and hazards in a different way, software and IT supply chains can still be disrupted by local and global outages or geopolitical events. Reduced transparency of supply chains, and poor understanding of managed service and digital service provision, can mean infrastructure operators are unprepared for these risks.

Some factors that can expose third-party vulnerability include unmaintained open source (or closed source) code; use of AI in operational decision-making or third-party systems; complex business models; and systems with excessive or high-level access, including remote access to supervisory control and data acquisition (SCADA) systems.

Critical workforce shortages have permeated all critical infrastructure sectors.[12]

Shortages in skills and labour, which had an acute impact during the COVID-19 pandemic, persist across the economy. Shortages of specific skills impact each critical infrastructure sector in different ways. Skills and labour shortages are a critical issue across all sectors.

Sectors which experienced significant pressures in skills and labour during the pandemic, such as healthcare and aviation transport, are still experiencing shortages of specific skills. More broadly, an insufficient number of engineering and construction workers has been identified as a factor delaying construction of new infrastructure developments, which can have an impact on all critical infrastructure sectors.

Competing demands for skilled employees has required more flexibility in the workforce, exacerbating other sector workforce challenges, including an ageing workforce, dependence on migrant workers and a shortage of skilled workers.

Case Study

Australia remains dependent on the global supply and maritime supply lines for urea, a key component of nitrogen-based fertiliser and an additive for AdBlue, which regulates diesel emissions. The concentration of supply and seasonal agricultural spikes in demand for urea leave our supply vulnerable to a variety of hazards.

In 2021, Australia's primary source for urea, China, halted exports, disrupting multiple critical infrastructure sectors, including agriculture (via fertiliser prices) and transportation. Australia has improved the diversity of its supply, but demand and the price of urea continue to rise. This is likely to persist due to current cost and capacity pressures on maritime supply lines.

The disruptions to the supply of urea and the dependency on it as a component of other critical materials highlight that supply vulnerabilities are often hidden by network complexity – and may not be recognised until a significant disruptive event occurs. The first links in supply chains are probably well understood by business, but much less is known about subsequent supply tiers. This can lead to underestimation of supply chain risk.

CROSS-SECTOR RISK PRIORITISATION FOR THE SUPPLY CHAIN HAZARD

Fig. 3 highlights the Supply Chain risk issues with a comparative visualisation of plausibility and damage for all-hazard risk issues in this review.

More damaging impacts from Supply Chain risk disruption are more likely for time-sensitive supply chains or where no alternative supply sources are available. Long, international supply lines, especially maritime, tend to experience more frequent disruption.

The extent of damage to operations can often be mitigated or limited through effective planning.

Many Supply Chain risks trend to more moderate levels of occurrence and impact. This is due in part to fluctuation in levels of disruption from global events and some diversity and flexibility of supply chains. Workforce and skills shortages continue to impact all sectors, and risk factors depend on how each sector manages and mitigates risk.

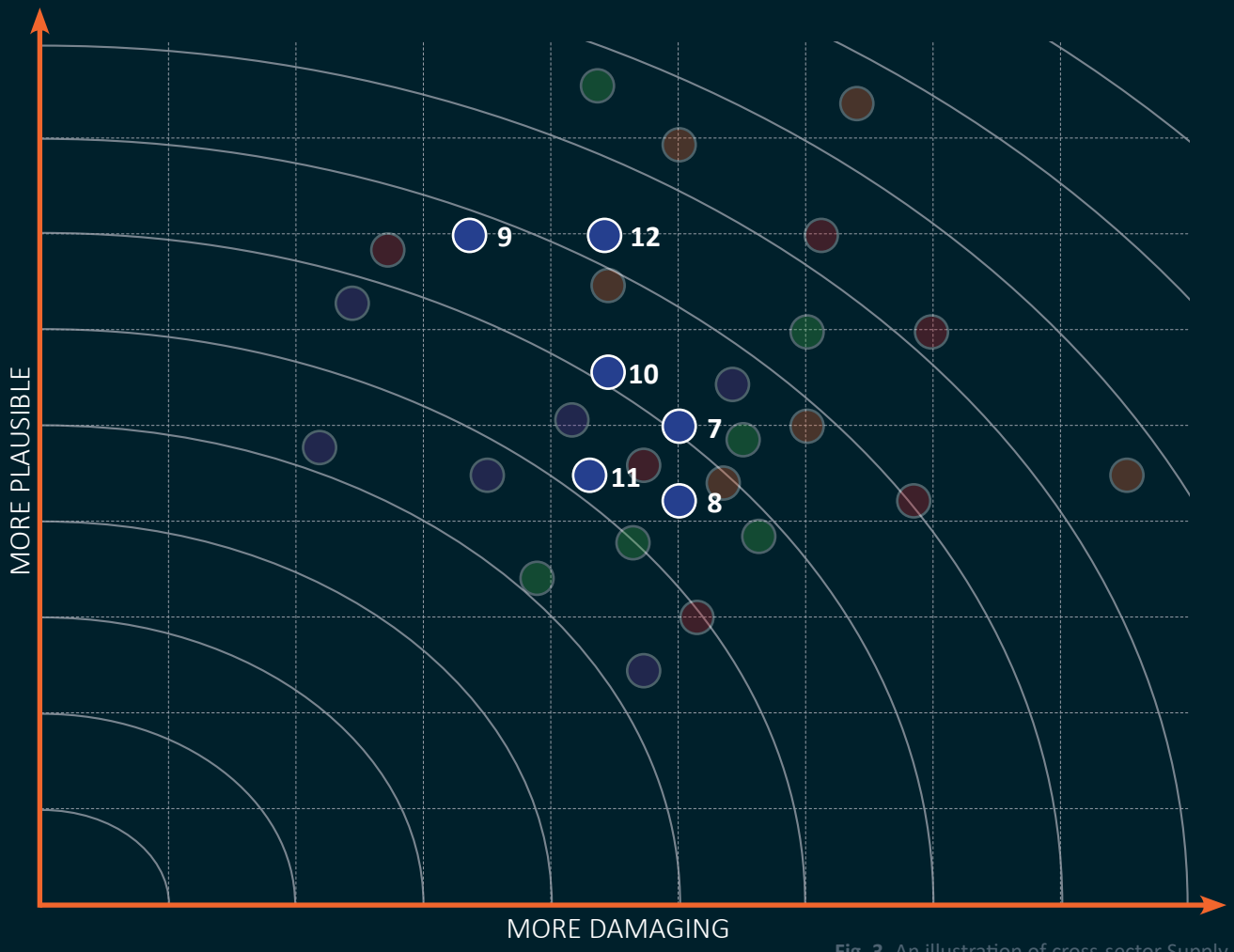


Fig. 3. An illustration of cross-sector Supply Chain risk prioritisation considering risk plausibility and damage

7 Geopolitically driven supply chain disruption

8 Restricted availability of critical technology and materials

9 Disrupted maritime supply lines

10 Disrupted domestic surface transport

11 Software supply chain risk

12 Critical workforce and skills shortfalls


PHYSICAL

Physical

Espionage and foreign interference, along with politically-motivated violence, are ASIO's principal national security concerns. [13]

A willingness to employ violence, particularly of members of society who adhere to the more extreme ideologies, was a key factor behind ASIO's 2024 decision to raise the National Terrorism Threat Level to PROBABLE. However, the threat from espionage and interference by foreign powers and their proxies remains increasingly persistent and broad reaching.

Critical infrastructure providers are targets for espionage and foreign interference. Our critical infrastructure presents a multi-level espionage target for adversaries, who continue to deploy varied methods to infiltrate and extract information. Building relationships through false job advertisements, consultancies, academic and research collaboration, these 'spies in disguise' necessitate vigilance and robust risk management by critical infrastructure operators to maintain vigilance, according to ASIO.

Sensitive information will remain highly desirable. An ability to interfere in how a critical infrastructure provider makes decisions and operates or doesn't can achieve the aims of foreign powers and their proxies in the course of doing business. This can result in critical operations being vulnerable to overt actions in the event of a rise in geopolitical tensions where Australia becomes a direct or indirect target of aggression.

Our vulnerability to grey zone tactics is heightened in areas outside Australia's direct control, such as the undersea and space domains. [14]

Reliance on international supply chains, third-party providers and foreign owners and operators can increase the likelihood of physical tampering or espionage occurring outside Australia's direct control. Incidents have demonstrated that sabotage of critical infrastructure can be used to destabilise relationships.

Undersea cables, critical for Australian internet and communication infrastructure, cross vast stretches of ocean. It can be difficult to determine whether the cause of damage to cable systems is natural, accidental or malicious. There are ongoing concerns that malicious actors could tap into cables to monitor and siphon sensitive data flowing in and out of Australia.

Non-destructive anti-satellite capabilities that disable or deny access to satellites, rather than physically destroy them, may lead to an increased use of grey zone operations in space, especially prior to a military conflict.

Grey zone conflict can provide ambiguity as to the source of any attack. Isolated impacts on specific infrastructure assets may have cascading effects across critical infrastructure sectors. As such, it is important for providers to have a clear understanding of both upstream and downstream dependencies that can be impacted, even by events well beyond the Australian region.

Geopolitical issues have intensified issue-motivated activity, and actors threaten to shift their tactics to infrastructure disruption. [15]

Social division and polarisation can increase the risk of an escalation of issue-motivated activities, including attempts to disrupt or disable critical infrastructure. Domestic disruption activities such as blockades or strikes generally aim to draw attention to a cause rather than permanently damage an infrastructure or capability. However, increasing polarisation can push groups more towards the extreme and a willingness to deploy more direct disruptive tactics.

The use of misinformation and disinformation amplifies untruths, which can be difficult to mitigate and contain. The direct targeting by issue-motivated groups with distorted information is also a tactic to influence human behaviour, spawning protest, activism or harmful actions.

Next-generation technology and defence program initiatives will cement foreign state interest in domestic research. [16]

A number of national capability initiatives involving Australian research and development activities will interest foreign states. These include the National Reconstruction Fund, investments in quantum and other critical technologies, rare-earth materials manufacturing and the AUKUS security agreement. Critical infrastructure entities and personnel involved in these and other critical areas of research will be high-interest targets for potential acts of espionage to access sensitive domestic or foreign partner information.

To remain globally competitive and to ensure a resilient and diversified economy, investment in advanced technology skills and research capabilities is critical. Increased activity on more sensitive research – including robotics, biomedical, advanced manufacturing, defence capabilities, AI and quantum computing – will require targeted training and development for a new type of workforce. Building the necessary skills and knowledge in the timeframe required for this expected future workforce could lead to vulnerabilities through knowledge gaps and a need to source foreign expertise to meet demand.

Sabotage of critical infrastructure to create destabilising impacts is being used outside of conflict zones to some effect. [17]

The use of physical sabotage to disable critical infrastructure outside of conflict areas is emerging as a key risk. Critical infrastructure is particularly vulnerable to this threat, where key facilities are located in less secure environments. In February 2024, the Director-General of Security said the sabotage threat in Australia had receded in recent decades but had the potential to re-emerge, particularly in relation to critical infrastructure.

ASIO assesses that a number of cohorts – including extremists, foreign states and their proxies – are increasingly discussing, researching and conducting reconnaissance for sabotage, although no plans for an attack have been identified at this time.

Over the last 12 months, events have highlighted the fact that strategic targeting of infrastructure can cause widespread and cascading disruption. For example, on the eve of the 2024 Paris Olympics, attacks on the French railway network followed damaging attacks against French fibre optic telecommunication infrastructure by similarly aligned issue-motivated actors. In Australia, multiple mobile communication towers have been vandalised, and copper theft has impacted the delivery of internet and electricity, causing significant regionalised disruption to critical services.

The need to depend on international parties for growth exposes entities to greater risk from foreign involvement. [18]

Limitations in the domestic market often necessitate the use of foreign partnerships and providers; a relationship with the wrong partner exposes critical infrastructure providers to adverse risk. While foreign parties operating in critical infrastructure may be legitimate their operation may also involve purposes, principles or regimes that are inconsistent with our own. Divided loyalties may lead to an entity acting against the national interest of Australia.

Foreign investment, ownership or control can also provide privileged access to sensitive operational and corporate information, industrial secrets, or broader information on vulnerabilities across a critical infrastructure sector.

As part of foreign ownership due diligence, critical infrastructure operators need to ensure and protect against the material impact of foreign involvement risk on their assets.

Case Study

In September 2024, a large issue-motivated protest in Melbourne, largely driven by anti-war sentiment about the Israel-Palestine conflict, was marked by violence and disruption in the city's centre. The catalyst for the protest was against a Defence Industry Sector conference, disruption was caused to transportation and the movement of people to and from work locations. While there are obvious links between the defence industry and military conflict, issue-motivated groups are increasingly targeting for disruption of any sector or entity perceived to have links to issues or events that provoke strong disagreement or community polarisation. A willingness to deploy violent tactics increases levels of risk.

CROSS-SECTOR RISK PRIORITISATION FOR THE PHYSICAL THREAT

Fig. 4 highlights the Physical risk issues with a comparative visualisation of plausibility and damage for all-hazard risk issues in this review.

Damaging physical security threats to critical infrastructure have been less common in Australia than other threats, and the expected damage from such events is highly variable. Incidents of vandalism or theft tend to be less targeted, less intent on widespread disruption and have localised impacts.

Disruption and damage from more covert physical threats can be difficult to attribute, with the full impacts only belatedly being recognised or remaining unknown.

Impacts occurring offshore may take time to reach Australia, and effects on onshore operations may not have a clear link to the initiating event or actor.

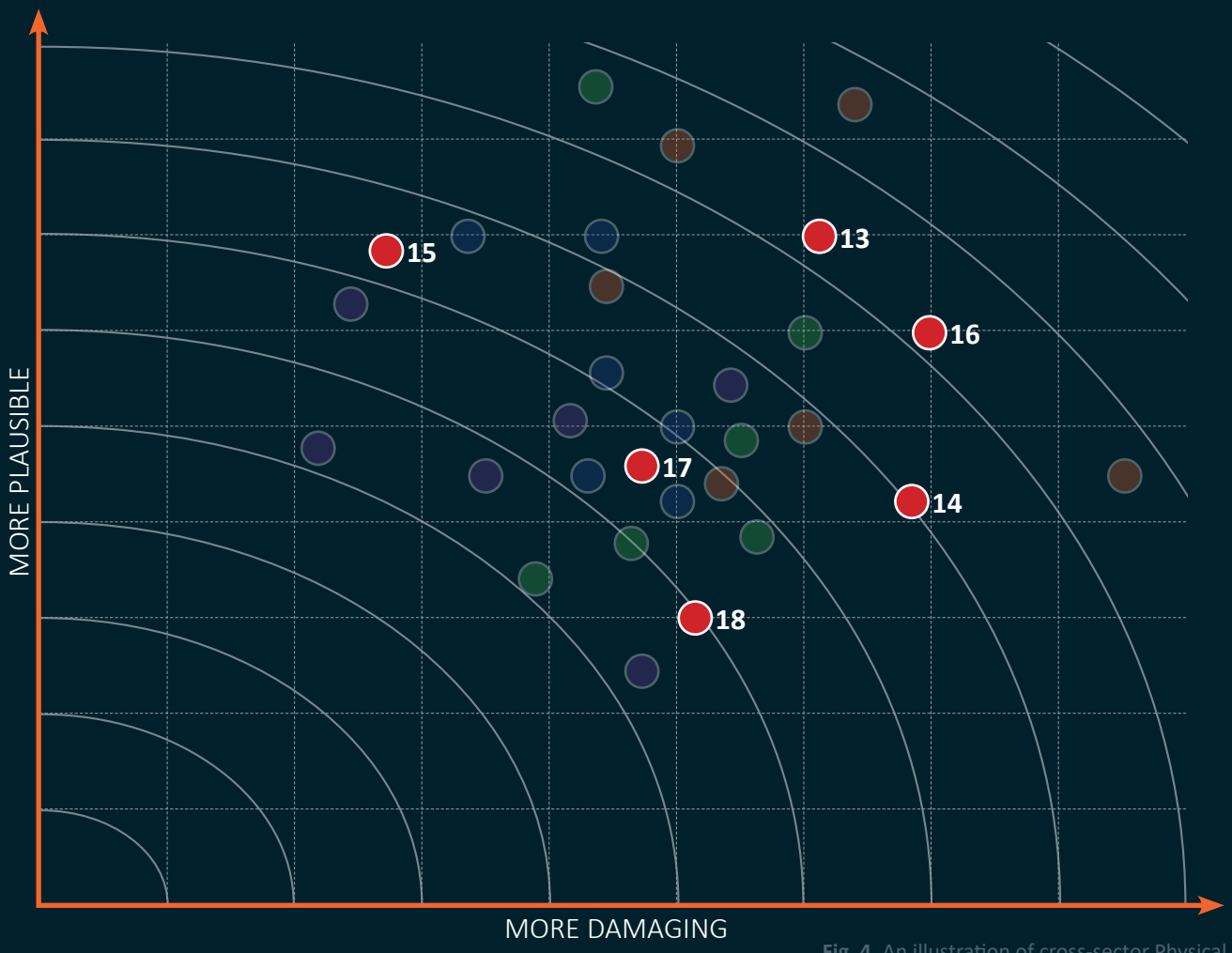


Fig. 4. An illustration of cross-sector Physical risk prioritisation considering risk plausibility and damage

13 Foreign interference risk

14 Risk from grey zone attack

15 Disruption from issue-motivated group activity

16 Espionage exfiltration of sensitive data

17 Sabotage of critical infrastructure

18 Foreign involvement risk


NATURAL HAZARD

Natural Hazard

Relying on past experience may not be suitable to prepare for addressing natural hazard risk on changing infrastructure requirements. [19]

Natural hazard risk to critical infrastructure continues to evolve, with changing weather patterns increasing the frequency and severity of some natural hazards. Australia's critical infrastructure is more extensive, expensive and interconnected than ever; it also remains interspersed with ageing components. Funding cycles and often significant capital investment required for resilient critical infrastructure may not keep pace with the need for change.

The vulnerability of systems can change over time as assets age or are replaced, or the role of assets within networks change. Critical infrastructure owners and operators need to understand how changing climate patterns will affect new and older infrastructure. More frequent monitoring of these variables will become increasingly important to maintain whole-of-system resilience against severe weather.

Technology's rapid integration into critical infrastructure can improve efficiency and reduce downtime. However, more reliance on automation and system complexity can make incidents more difficult to diagnose and recover from. Complex and interconnected systems are often more dependent on services outside an operator's control.

Impacts of severe natural hazard events are shifting into areas that have historically been at a lower level of risk. [20]

The locations exposed to severe natural hazards are changing due to broad changes in weather patterns, changes in land management, and expansion of our built environment. With this shift, the cost of extreme events affecting Australia and our critical infrastructure is increasing.

As boundaries change for historically well understood hazard zones, severe hazards may exceed standards originally intended for different conditions.

Changes in land and water management can affect the intensity of bushfires, the level of storm damage to power lines and flood behaviour around the built environment.

Densification is seeing cities expand into more hazard-prone areas and increasingly exposed to the impacts of high winds, flooding and bushfires. This is also the case for critical infrastructure. For example, an increasing energy infrastructure footprint, is likely to expose more infrastructure to natural hazards such as tornadoes, which occasionally occur in Australia but have historically rarely affected our built environment.

Natural hazard impacts will cascade beyond initial impacts due to the interconnectivity of critical infrastructure. [21]

Significant disruption in one sector caused by natural hazards, such as storm activity or bushfires, can cascade and influence the delivery of critical services by other sectors. Depending on the nature of the event, some critical infrastructure sectors may be directly affected, with cascading effects on downstream, interdependent sectors.

Cascading effects can disperse impact well beyond the initial impact location. Causal loop effects can also inhibit the speed of recovery, particularly where two sectors have a close interdependency.

For example, if power to a critical infrastructure operation was cut, causing disruption, the flow-on effects on key dependencies might result in delays, restricted movement or limits to supply that can in turn affect recovery operations.

Australia is highly vulnerable to biosecurity breaches. [22]

The movement of people and goods across Australia's border has returned to pre-pandemic levels. This has increased the risk of biosecurity breaches with potential catastrophic effects on agriculture, food products and healthcare across Australia.

Australia exports the majority of its agricultural product, which leaves us susceptible to widespread economic impacts in the event of a biosecurity outbreak. Australia's agricultural exports drive billions of dollars into the economy annually and such an event would have major and protracted impacts.

Beyond agriculture and food sectors, biosecurity breaches have a vast impact on multiple sectors. As witnessed during the COVID-19 global pandemic, impacts and responses can increase social unrest and decrease social cohesion. Supply chains that may be compromised for prolonged periods can also compound disruption to operations.

Critical infrastructure remains at a heightened level of disruptive effect from space weather during the current solar maximum period.[23]

Space weather events continue to pose a risk as a significant disruptor to critical infrastructure, as a solar maximum period continues to its expected peak in 2025. Given the absence of an extreme space weather event impacting modern critical infrastructure to date, it remains difficult to assess the full impacts of such an event.

However, it is likely that with increased reliance on satellites for communication and for position, navigation and timing systems, a severe space weather event would cause significant disruption to many critical infrastructure sectors which rely on this data – particularly the defence industry, transport and communications sectors. Physical damage to orbiting infrastructure poses repair issues that are more complicated than other sectors.

The space weather event in May 2024 was the first geomagnetic storm event to impact new low earth orbit satellite proliferation, causing the largest ever migration of satellites.

Changing global average temperatures will pose one of the greatest challenges for critical infrastructure operators.[24]

Climate change is already leading to more intense and frequent extreme weather events in Australia's global region, the Indo-Pacific. Heat and heat-related hazards are increasing worldwide, and Australia is one of the most vulnerable countries in a warmer world.

Extended periods of extreme heat will place extreme demand pressure on the energy sector, especially for cooling. As Australia moves to being a more electrified nation, capacity growth and ongoing reliability of electricity generation will be paramount to its national security. In the last 12 months, the National Electricity Market, which powers Australia's eastern and southern states, witnessed new records for electricity demand.

Extreme heat is a significant health hazard, with the potential to impact workforces, in terms of health and safety and availability. Heatwaves are Australia's deadliest natural hazard, particularly in cities. Longer periods of higher temperatures can push infrastructure and materials beyond temperature thresholds, particularly those designed for cooler climate levels. As more assets operate above thresholds, infrastructure is at risk of disruption or potential damage, with cascading impacts.

Case Study

In February 2024, a severe storm system in Victoria caused transmission towers to collapse leading to failures in energy supply, a disconnection of substantial generation, and some loss of communication networks. More than 500,000 customers across Victoria lost power, with full restoration taking weeks. The power outage also had cascading impacts on dependent critical infrastructure, including in food and grocery, transport and, healthcare and medical sectors.

Planning for disruptions is a normal part of operating critical infrastructure. Those plans may not consider failure of multiple services concurrently or be sufficient to operate through a prolonged outage. They may not adequately allow for unexpected behaviour in complex systems like power or telecommunications, or consider the impact on recovery of interdependencies in interconnected critical infrastructure. Events like the February 2024 power outage remind both businesses and individuals to reconsider their preparedness for major natural hazard events, the changing risk environment, and dependence on services.

CROSS-SECTOR RISK PRIORITISATION FOR THE NATURAL HAZARD

Fig. 5 highlights the Natural Hazard risk issues with a comparative visualisation of plausibility and damage for all hazard risk issues in this review.

Severe weather natural hazards are often infrequent, seasonal or cyclical. However, recent years have seen numerous damaging events, and heat-related impacts are expected to increasingly affect infrastructure operations.

Australian operators are experienced in managing the more frequently occurring natural hazards. However, infrastructure is becoming more extensive and more expensive, increasing the financial impact of disruptions.

Damage to critical infrastructure operations is likely to be higher when sectors are concurrently affected, or when cascading failures extend impacts beyond the initially affected area.

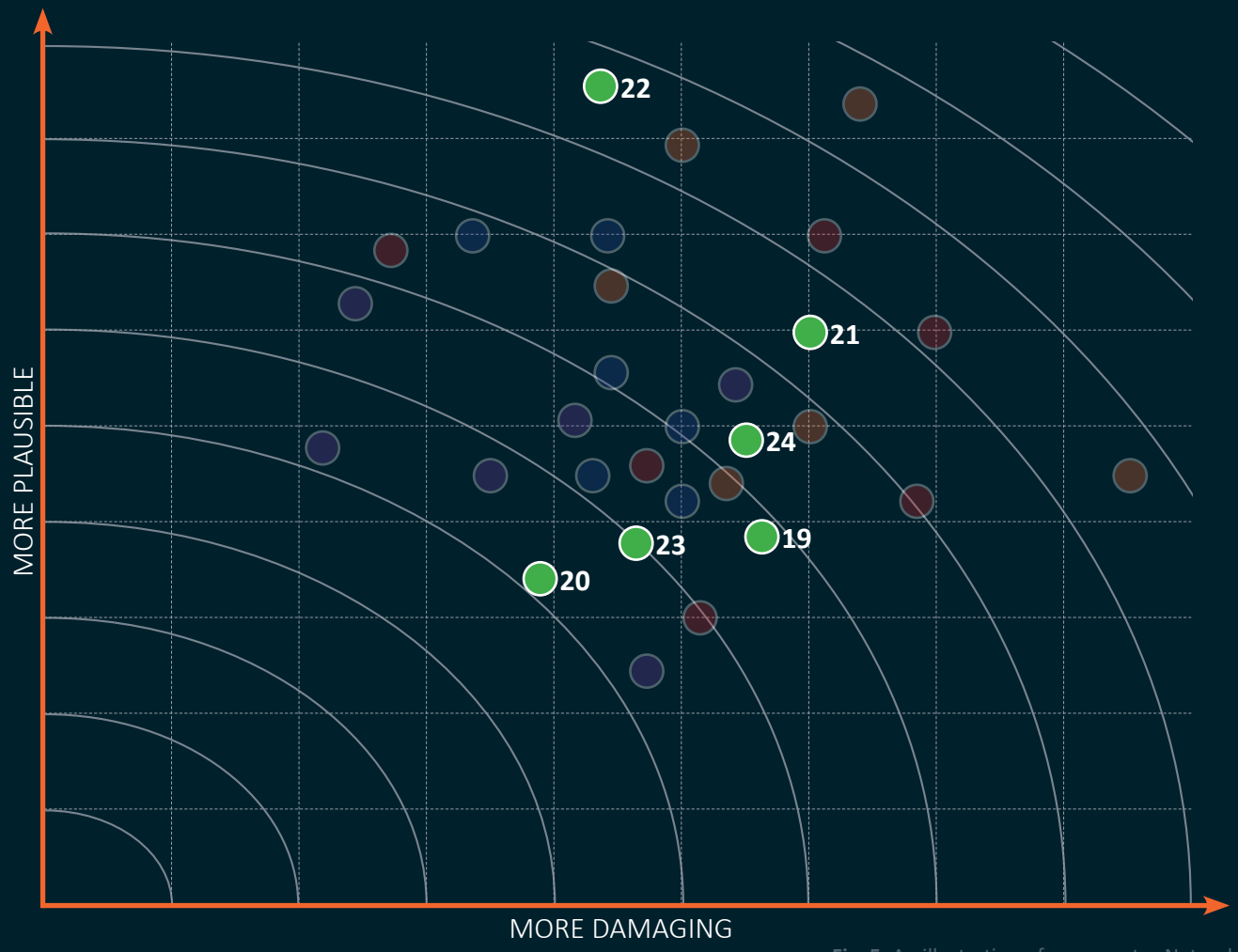


Fig. 5. An illustration of cross-sector Natural Hazard risk prioritisation considering risk plausibility and damage

19 Severe weather event unpreparedness

20 Wider geographic footprint for severe weather

21 Significant disruption from interdependent infrastructure

22 Biosecurity breach risk

23 Extreme space weather event

24 Increasing impact from extreme heat

PERSONNEL

Personnel

Critical infrastructure operators should not underestimate the espionage and foreign interference threat to their workforce. [25]

People can be both a strength and a significant vulnerability when considering threats to critical infrastructure. In 2023, ASIO publicly called out a 'hive of spies' attempting to steal information through recruited insiders, and emphasised the threat to critical infrastructure from espionage and foreign interference. Cost-of-living pressures are one of the predispositions that can influence the intent of an individual to be susceptible to financial incentives to undertake foreign interference and espionage activities.

For some foreign states, all information relating to Australia's critical infrastructure is of potential value and should be considered at risk. Information about critical services (energy, water and telecommunications), defence, biotechnology and other research is of high value.

Foreign interference within the workforce an create significant disruption, including through the spread of disinformation. This can create reputational risk for business and pose a broader threat to national security, sowing social distrust and divisiveness. Disinformation can be intentionally spread by an issue-motivated insider, or employees may unintentionally spread, or act on, misinformation.

Insider activities, malicious or negligent, continue to cause critical infrastructure outages in Australia and overseas. [26]

Insiders' potentially harmful behaviour can be difficult to detect as they usually operate in legitimate roles with authorised access. This inside knowledge and access can result in far greater harm to infrastructure or operations than can normally be expected from outsiders.

Malicious personnel with similar access and sufficient knowledge could cause outages with more ease, and potentially prolonged outages with significant actual and reputational damage.

Often, insiders will use the information they have to target more sensitive assets that can take longer to recover, causing significant financial and reputational impacts.

Even unintentional insider actions can cause widespread infrastructure disruption. Over the last 12 months, incidents of mishandling of software updates or patches by critical infrastructure and third-party providers have caused significant and widespread disruption.

Equally, the theft of property or intellectual property remains a concern for infrastructure assets who rely on their employees to handle commercial and security information. Any theft has the ability to compromise the functioning of critical infrastructure causing loss of commercial advantage or loss of sensitive information or research that might lead to an impact on the functioning of the infrastructure asset.

Misidentification of critical roles increases levels of vulnerability for malicious insider activity. [27]

Critical infrastructure owners and operators are required to identify critical roles as part of their CIRMP. However, entities will often have different approaches to, or interpretation of, critical roles, which can manifest as different vulnerabilities when considering how business, operational or national security risk might be managed.

Critical roles have access, knowledge, control or authority that provide opportunity to a malicious person, or can hide harmful activities. People in these roles can be at any level of an organisation, or they may be third-party providers who have critical knowledge or dependencies for the delivery of services.

A narrow focus on known high-risk operational or executive roles may miss critical vulnerabilities or personnel with deep operational knowledge. The number of employees with full end-to-end operational knowledge and access should be considered and (where appropriate) minimised.

Artificial intelligence has enhanced tools for social engineering, increasing the vulnerability of personnel with critical access and responsibilities. [28]

The compromise of accounts or credentials is the most common type of cyber security incident affecting Australian critical infrastructure, according to Australian Signals Directorate reporting.

Malicious cyber actors often use techniques such as social engineering to access accounts in order to exfiltrate sensitive information, or spread disinformation.

Social engineering for cyber access includes phishing (taking advantage of poor personnel security) and baiting (including leaving devices for employees), tempting employees to compromise security barriers, wittingly or unwittingly. Phishing can give malicious actors accesses that can support further malign activity, including through business email compromise.

Advances in AI and its wide availability have increased the effectiveness of some of these approaches. Text, image and video communications are likely to be far more persuasive than in previous years, and credentials may be more convincingly falsified.

Changes in workforce skills and ongoing workforce shortages demand increased focus on effective insider threat management to manage personnel risk. [29]

An inability to attract, and retain, a skilled workforce remains a critical challenge for industry. This is further exacerbated by ongoing workforce shortages across most industry sectors.

Rapid technological changes, most obvious in the energy transition, are requiring different skillsets, challenging an already strained personnel supply chain.

There are numerous risks associated with a changing workforce and skills shortages. In attempting to fill necessary roles, less robust on-boarding processes might be applied, and some workers may not be able to be effectively vetted. More dependence on foreign companies and individuals may be required. If changed and increased risks are not recognised and appropriately treated, the above factors will reduce the effectiveness of personnel risk mitigations and potentially increase malicious and non-malicious harm.

External global and domestic divisive issues can potentially heighten some workforce disquiet, leading to malicious activity. [30]

In Australia, individuals are increasingly embracing anti-authority ideologies, conspiracy theories and diverse grievances, with some identifying violence as a legitimate way to effect political or societal change. Intra-workforce disagreements on strongly held opinions are challenging to manage in workplaces and can be disruptive for operations.

Ongoing global conflicts and pressing environmental issues add complexity to how entities manage diversity, equity and inclusion policies. If not actively mitigated or even identified, rising division and harmful discourse can impact operations. Increased division can also push more people to ideological extremes, and influence human behaviour, spawning protest, activism or harmful actions. This can result in personnel being influenced by disinformation to act against an entity, or even use insider access to spread disinformation externally to reinforce ideological viewpoints.

Case Study

In 2023, a US third-party marketing service provider suffered 3 data breaches arising from a social engineering attack on employees. Attackers stole employee credentials and breached an internal customer support and administration tool, accessing the data of more than 100 customers and more than 100,000 individual users.

Critical infrastructure operators are relying more and more on third-party providers for many functions that were once undertaken in house. A successful breach at one of these entities could enable malign access to customer systems. While these breaches are relatively small for a large corporation, it is concerning that it experienced 3 similar successful attacks through lapses in personnel security practices. Critical infrastructure operators need to consider how insider threat management may need to extend to key third-party provider dependencies and those providers hosting sensitive data.

CROSS-SECTOR RISK PRIORITISATION FOR THE PERSONNEL THREAT

Fig. 6 highlights the Personnel risk issues with a comparative visualisation of plausibility and damage for all hazard risk issues in this review.

Insiders can cause significant disruption, but potential damage across a whole sector is often limited by smaller critical service areas, further mitigated by good workplace practices. Personnel-related risk events can be difficult to predict and are dependent on individual factors and opportunity.

Workforce and skills gaps exist in all sectors, but risks arising from those gaps can take some time to eventuate, and workforce practices and flexibility can further mitigate impacts.

Advances in technology can make malign influence more difficult to detect, where an error or malicious action can decrease the likelihood of timely detection.

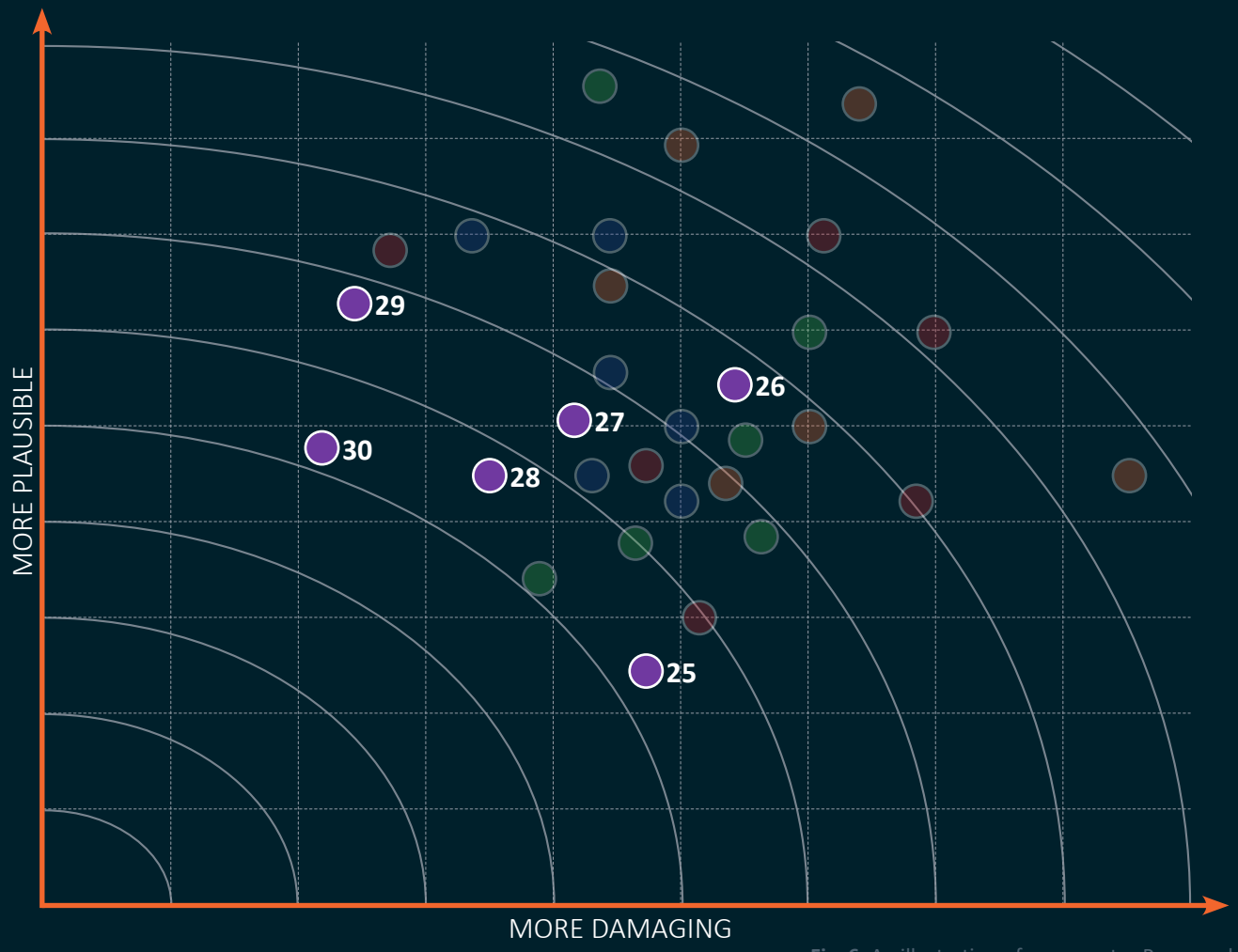


Fig. 6. An illustration of cross-sector Personnel risk prioritisation considering risk plausibility and damage

25 Foreign cultivation of critical workforce

26 Insider threat-initiated capability outage

27 Unidentified critical worker vulnerability

28 AI augmented social engineering of workforce

29 Workforce critical skills gaps

30 Increasing ideological divides in workforce

LOOKING AHEAD

Looking Ahead

The following trends and technology drivers will likely impact the risk profile of our critical infrastructure over the coming years.

Rapid technological change is creating skill and staffing shortfalls, including for skilled cyber security professionals.

It is likely that the shortage of skilled staff, and the demand for upskilling of staff, will expand in coming years.

For example, the transformation of the energy sector, while rapid, is lagging behind expectations globally. There is already global demand for the new suite of skills required for that work. Accelerated rollout of decarbonising and automation technologies in small and large businesses is very likely to be associated with a step change in exposure to cyber threats.

A lack of suitable staff can lead to short-cutting of security procedures: increasing sourcing from overseas, where vetting may not be possible; accepting lower skilled staff; and increasing reliance on third parties, with a consequent loss in transparency.

More and more critical operational decisions will be automated.

Automation is being rolled out into numerous sectors and in many business activities. Supply chains, customer service, food and grocery manufacturing, warehousing, network operations and other activities are rapidly using automation, including AI.

In the last year, consumer and business AI tools have been rapidly integrated into workflows, and may also be driving faster integration in an industrial and critical infrastructure context. Day-to-day operational decisions can now be made using specialised AI applications.

More and more operational decisions are being made with AI, or automated using other decision tools (often misunderstood as AI by the public).

There are both benefits and negatives to automation. In a business-as-usual environment, automation is overwhelmingly positive, but in the case of unanticipated failures or unexpected behaviour automation can obscure diagnosis and limit manual, alternative operations. For example, highly automated warehousing may have very limited function without operational systems.

Supply chain disruptions continue to affect domestic and international supply chains.

It is likely that disrupted supply chains will continue to be a feature in years to come. Trade decisions, conflicts, pandemics and natural hazards can affect trade with Australia and disrupt transport routes, with varied consequences for Australia's critical infrastructure.

In recent times shipping has suffered due to disrupted access to both the Suez (due to conflict) and Panama (due to climate) canals. These disruptions have been compounded by congestion at key trading locations. In Australia, flooding has cut off east from west coasts, disrupting the transport of key inputs to critical infrastructure sectors.

The race to 6G.

6G is the next planned generation of mobile telephony. It is touted to add or extend use cases originally planned for 5G. 6G use cases are likely to make the technology far more critical in an infrastructure context. It is possible 6G will be rolled out commercially by around 2030, but there is ongoing research necessary to achieve its full potential.

Some anticipated benefits are improved vehicle to vehicle communication, a more prominent role in pinpointing location, a stronger dependence for industrial processes and automation, and significant growth in wearable healthcare, and other, devices.

While there is attention on improved security for 6G, competition to deliver technology often results in compromises or incomplete functionality at release.

Technology that is heavily integrated into previously manual or independent processes risks lowering resilience in the case of disruption.

Traceability will present new risk challenges.

The supply and transportation of goods often relies on transfers between multiple parties and between different domestic and international jurisdictions. This can make tracing goods from 'source to sink' an ongoing challenge.

To meet the challenge of transparency, the traceability of goods is being actively improved in some sectors, including the food and grocery sector, in response to food safety and other priorities.

Interception and modification of goods in supply chains has been demonstrated as a risk, and this risk has the potential to increase due to ongoing global instability and economic pressures. Lower levels of, or disparities in, traceability along supply lines also have the potential to obfuscate interference, including risks of espionage and sabotage.

Technology advancement and implementation is ongoing across the transport sector, with increasing connection, autonomy and control of vehicles. Traceability is likely to also benefit from these technology improvements. Cyber security needs to be a priority as new, highly connected technologies are introduced, with security a key consideration for design and procurement.

Competition and conflict in space.

Space technology is changing. There has been a huge increase in the number of objects in low earth orbits, an increase in the use of shorter lifespan spacecraft, and ongoing congestion of geosynchronous orbits. There is little doubt that future wars will involve space technology.

Almost every critical infrastructure sector, and civilian life, relies on space capabilities. Awareness of dependence on space technology is low, even among many operators of critical infrastructure, and has not kept up with the growing use of satellite-enabled capabilities.

With the growing number of launched objects in space, especially into low earth orbit, there is an increasing risk that collisions could cause major service disruption. At the time of writing there were more than 6,800 Starlink objects in space, for a service that began in 2019.

By 2030, China's competing Qianfan constellation is planning around 13,900 satellites in low earth orbit. There is concern that objects from the Qianfan orbit will fall through other low earth orbits increasing risk of collisions with other satellites, following obsolescence or due to faults.

Ongoing moves to onshore or near-shore supply will gradually redraw the transportation map.

The concentration of manufacturing and the long supply chains are increasingly recognised as posing a risk to the resilient operation of critical infrastructure. There have been developments in government and the private sector to mitigate this by moving some manufacturing closer to the business customer or consumer.

These changes will begin to alter the global picture of supply chain resilience and the geographical picture of supply inside and outside Australia. A number of unknowns remain, including concerns about whether local manufacturing will be competitive and the possible consequences for trade relationships.

Sensitivity to supply and the need for resilient supply are especially obvious where limited supply options exist, where geopolitical or business uncertainty is affecting key supplies and where disrupted or congested supply chains are becoming more common.

Australian Government

Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE