



## Risk Assessment Advisory for Critical Infrastructure Healthcare and Medical Sector

The international and domestic threat landscapes continue to evolve; natural hazards are becoming more prevalent, with longer-lasting impacts and, critical infrastructure networks continue to be targeted globally by both state and criminal cyber actors. As a result, stakeholders within Australia's Healthcare and Medical Sector must adapt their risk management strategies to ensure risks to the operation of assets critical to the nation's economic and social wellbeing are being appropriately captured.

This material has been designed to provide guidance on assessing these types of risks to Australia's critical infrastructure. Through the provision of suggested risk assessment approaches, the material aims to assist sector stakeholders to adapt existing risk practices and help organisations understand risks within the broader national critical infrastructure context. The document comprises the following sections:



Risk in the critical infrastructure context



Determining criticality of assets



Interdependencies (upstream and downstream)



Understanding threats and hazards for risk



Risk controls and mitigations



A risk assessment methodology

Some features of risks in the **Healthcare and Medical Sector** are outlined below:

**A highly critical and sensitive service** – providing care to Australians, often when they are at their most vulnerable.

**Widespread access to highly sensitive information** – in the form of patient records and other medical information.

**Decentralised risk accountability** – as each health or hospital service often operates autonomously.

**Patient risk is at its centre** – as outages or the inability to provide services puts lives at risk.

**Storage of large amounts of perishable items** – including a range of items that need to be kept refrigerated to remain viable.

**Large amounts of ageing equipment** – particularly in connection with long-life devices in the biomedical sub-sector.

**Key ICT services often outsourced** – either through an 'eHealth' function of public health departments, or using commercial ICT managed service providers. Sector transitioning to digitalised record keeping.

**Key driver of the Australian Economy** – 15–20% of the Australian workforce is within the Healthcare and Medical Sector.

**Substantial uptake of Internet-of-Medical-Things (IoMT) devices** – to enable remote or automated delivery of patient care.

**More critical in an emergency** – when a disaster affects multiple sectors occurs, health services operate beyond normal capacity.

**Significant amounts of intellectual property** – through partnerships with research bodies in technology, medicine and therapeutics.



## Risk in the critical infrastructure context

### Identifying risk for critical infrastructure

Risk in the context of critical infrastructure is related to Australia's national and societal resilience. This may differ from the way entities have viewed risk in the past (for example, with financial or shareholding interests as a focal point). Risks that have the greatest impact on the social or economic stability of Australia or its people, the defence of Australia or national security, also need to be considered and framed within critical infrastructure entities' existing risk management strategies.

An example of how to identify this risk for the Healthcare and Medical Sector is framing a possible risk from a cyber attack against ageing medical equipment (such as a 15 year-old magnetic resonance imaging machine with an older, less secure operating system) impacting the integrity and reliability of medical results, potentially also denting confidence in broader health services provided by an entity or state/territory health service.

### Taking an all-hazards approach to risk.

For critical infrastructure organisations, an all-hazards approach to determining risk is recommended. All-hazards is an integrated approach to risk management, preparedness and planning that focuses on businesses enhancing their capacities and capabilities across a full spectrum of threats and hazards to Australia's critical infrastructure.

All-hazards risk assessment considers both threats (human-induced) and natural and environmental hazards that could impact on a critical infrastructure entity and its operations. Australia's critical infrastructure risk environment continues to evolve and an all-hazards approach is best placed to consider the potential converging of the wide-ranging threats and natural hazards it confronts, which could result in multiple and cascading effects on national resilience.

Critical infrastructure organisations are uniquely positioned to assess to critical infrastructure risk through the analysis of those identified threats and hazards to their sector against their own assessment of vulnerabilities. As part of this risk identification, organisations can consider broadly how the *confidentiality, availability, integrity* and *reliability* of their assets may be impacted during and after any incident.

Understanding this potential 'relevant impact' is important to prioritise risk and determine how best to both minimise the likelihood of the risk occurring and mitigate the potential impact. Examples of how these relevant impacts can be applied for assets in the Healthcare and Medical Sector has been provided in the **Understanding sector-specific risks** section of this document.

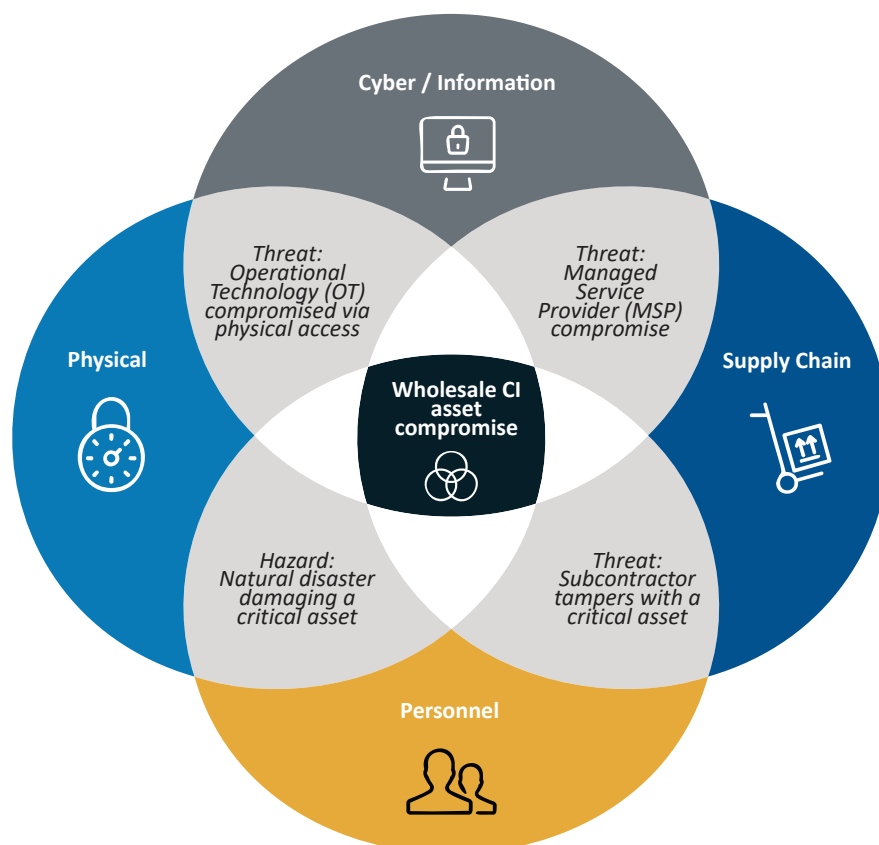
Some entities in the Healthcare and Medical Sector have security-related regulations already in place. Entities in the sector may need to consider guidance such as the Healthcare Identifiers Act 2010, or the Privacy Act 1988, or look to their state or territory government for regulatory frameworks and consider how they can incorporate national security-related risk into existing risk management frameworks. Entities should also refer to other CISC sector guidance for further information.

### Convergence risk

Australia's adversaries pose an increasingly sophisticated threat to our critical infrastructure and often look to exploit multiple vulnerabilities via multiple vectors in unison. Sector-wide convergence risks eventuate due to interdependencies within and across critical infrastructure sectors, as well as through other links, such as supply chain relationships. Furthermore, convergence risks could exist within organisation due in part to internal silos or lack of integration of risk management capabilities.

Adopting an all-hazards risk management approach is a strategy to combat convergence risks and ensure responses are comprehensive and integrated. This requires collaboration between all stakeholders, including internal business units, sector and supply chain stakeholders, law enforcement and emergency services. Organisations should leverage information from government stakeholders to appropriately consider appropriate threats and hazards. Adopting multidisciplinary approaches, collaboration and integration is a good approach for inclusion in a critical infrastructure entity's risk assessment. The following diagram illustrates an example of how a convergence threats can be represented as risk.

Figure 1. Examples of converging threat and hazard on risk identification





## Determining criticality of assets



### *Security of Critical Infrastructure Act 2018 (SOCI Act) – Section 5:*

health care and medical sector means the sector of the Australian economy that involves:

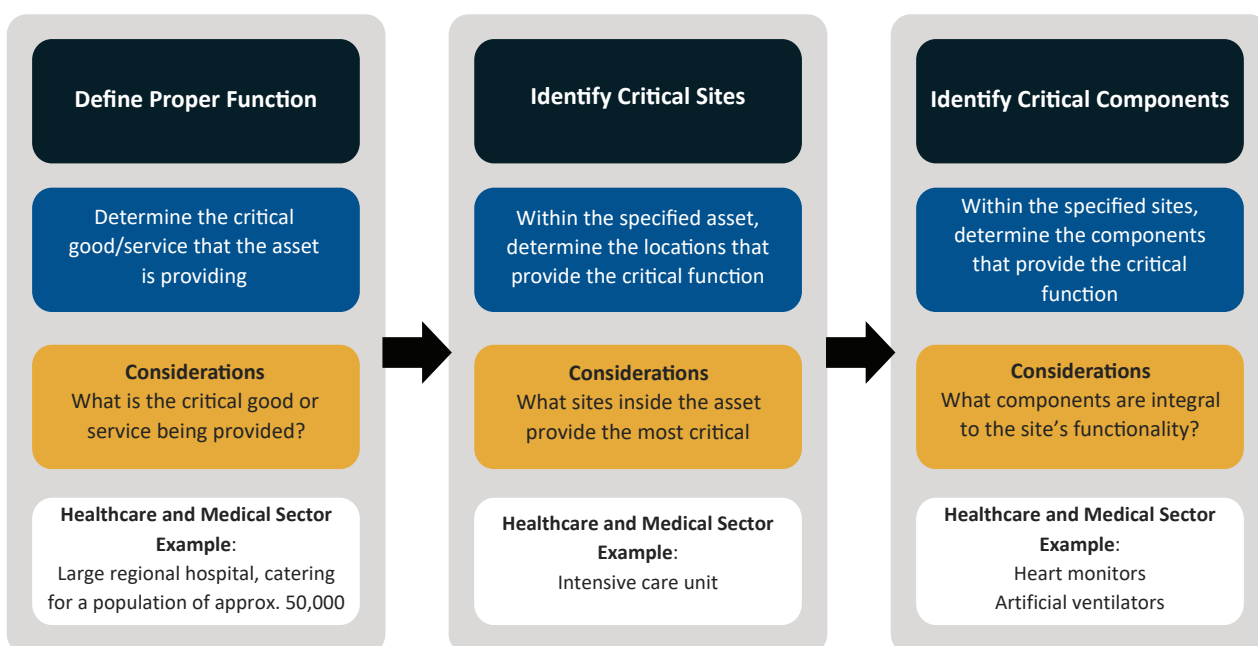
- (a) the provision of health care; or
- (b) the production, distribution or supply of medical supplies.

### Identifying and assessing criticality

For Healthcare and Medical Sector critical infrastructure providers, determining which sites and components of an asset should be considered critical involves identification and analysis of how an asset and its operations may be exposed to, or harmed by, threats and/or hazards. This process is vital for all hazards risk management, providing input into the identification of plausible risk scenarios that may impact operations. The critical sites and components of an asset are ultimately those most vital to its effective functioning and therefore integral to Australia's national security interests. Establishing criticality is designed to provide guidance on the allocation of resources to best protect the operational capability of the asset.

The 'responsible entity' for an asset is able to determine the extent of this activity; however, a suggested process using a select example is outlined below.

Figure 2. Example of determining criticality of an asset





A function of a critical infrastructure asset may be the provision of a critical good or service that is a contributor to the economic or social wellbeing, defence, or security of the nation.

Critical sites are physical locations that are part of an asset that are required for it to maintain its proper function. For a hospital, this could include intensive care units or maternity wards, and could also include data centres that host ICT services.

The responsible entity of a critical infrastructure asset is required to do what is 'reasonably practicable' to minimise and mitigate risk associated with critical components. This means entities must also identify critical components.

Critical components are anything that is required to maintain the function of the asset, or whose absence, compromise or damage could cause significant harm to the asset. For a healthcare and medical organisation, critical components may include the heating, ventilation and air conditioning system that controls the temperature of critical sites, or a dialysis machine that filters a patient's blood. Similarly, ICT systems, such as those which hold sensitive patient data, but may be hosted from physical locations outside of the hospital, need to be considered critical.



## Analysis of emerging trends and technologies

Identifying important trends and technology drivers and how they impact risk can be challenging; trends interact in unpredictable ways, with at times profound consequences. The following key trends and technologies have been identified as potential domestic changes that could impact on risk in the Healthcare and Medical Sector:

Figure 3. A selection of emerging trends and technology that can impact on risk in the sector

### Emerging Trends

- **Digital biomedical services are being adopted:** Improving the speed at which medical research can be returned and quality of medical guidance that can be provided to patients.
- **Health outreach services are expanding:** Improving the healthcare and quality of life for Australian living outside major cities and suburban hubs
- **Increasing use of low-cost processing services:** Such as transcription and radiology analysis. There are limited regulations or guidance for the use of these services, particularly those administered by overseas providers, and consumers of these services may not consider the security of services they use.
- **Green health will gain momentum:** The incorporation of environmentally friendly practices into healthcare delivery, providing benefits for citizens and the planet.
- **Patients and clinicians will increasingly choose between digital and in-person contact (rise of telemedicine):** There is now renewed optimism that healthcare could be entering a new era of digitalisation.
- **Mental health becomes a priority:** Many of today's chronic conditions are primarily caused by behaviour (such as overeating and smoking), leading to an increased focus on behavioural medicine.

### Emerging Technology

- **Electronic Medical Records (eMR) replacing existing paper-based practices:** Improving accessibility and clinical responsiveness.
- **Cancer research, treatment and prevention capabilities are being refined:** Providing continued improvement in life-extending care, therapies and quality of life, and palliative care.
- **Treatment for transmissible diseases are continually being developed:** As shown in Australia's (and internationally) responses to COVID-19.
- **Increasing proliferation of consumer wearable:** These capture personal health information and much of this is stored locally or in cloud-based services.
- **Growing integration of third-party medical devices for information, data sharing and data analytics:** Including integration with industries like insurances and education, creating and 'Internet of Medical Things'..
- **Consideration of software as a medical device:** Where software that controls or manages devices may introduce risk through misconfiguration, errors or omissions in testing.
- **Integration of AI in healthcare:** Artificial intelligence is already influencing dozens of different industries and healthcare is no exception.



## Sharing national security risk information with government

The Australian Government's national intelligence community collects and analyses information to constantly monitor, assess and provide advice on threats to Australia. Much of this information is classified and not made available to the general public; however, as part of their mandate the following portals provide open source information, assessments and advice designed to support critical infrastructure sectors.

Organisations are able to contribute to the process of monitoring and assessing threats through internal risk assessments. By identifying emerging risks, organisations are able not only to directly improve their security stance but share this information with external security bodies. The following organisations are able to receive threat information, distributing threat awareness across the sector:



CYBER AND  
INFRASTRUCTURE SECURITY  
CENTRE

### Trusted Information Sharing Network (TISN)

A set of bodies of industry and government representatives that meet to share information on issues relevant to the resilience of critical infrastructure and the continuity of essential services in the face of all hazards.

For further information on TISN and how to join the network, please go to:  
<https://www.cisc.gov.au/engagement/trusted-information-sharing-network>



Australian  
Cyber Security  
Centre

### Australian Cyber Security Centre (ACSC)

A hub for private and public sector collaboration and information sharing on cyber security. to prevent and combat threats and minimise harm to Australians.

To engage with the ACSC, fellow partners, and help uplift cyber resilience across the Australian economy, join the ACSC partnership program here:  
<https://www.cyber.gov.au/partner-hub/acsc-partnership-program>



### Australian Security Intelligence Organisation (ASIO) Outreach

Provides advice to government, industry and academia on current and emerging security threats.

To register to the Outreach program and gain access to security updates, please go to:  
<https://www.outreach.asio.gov.au/>



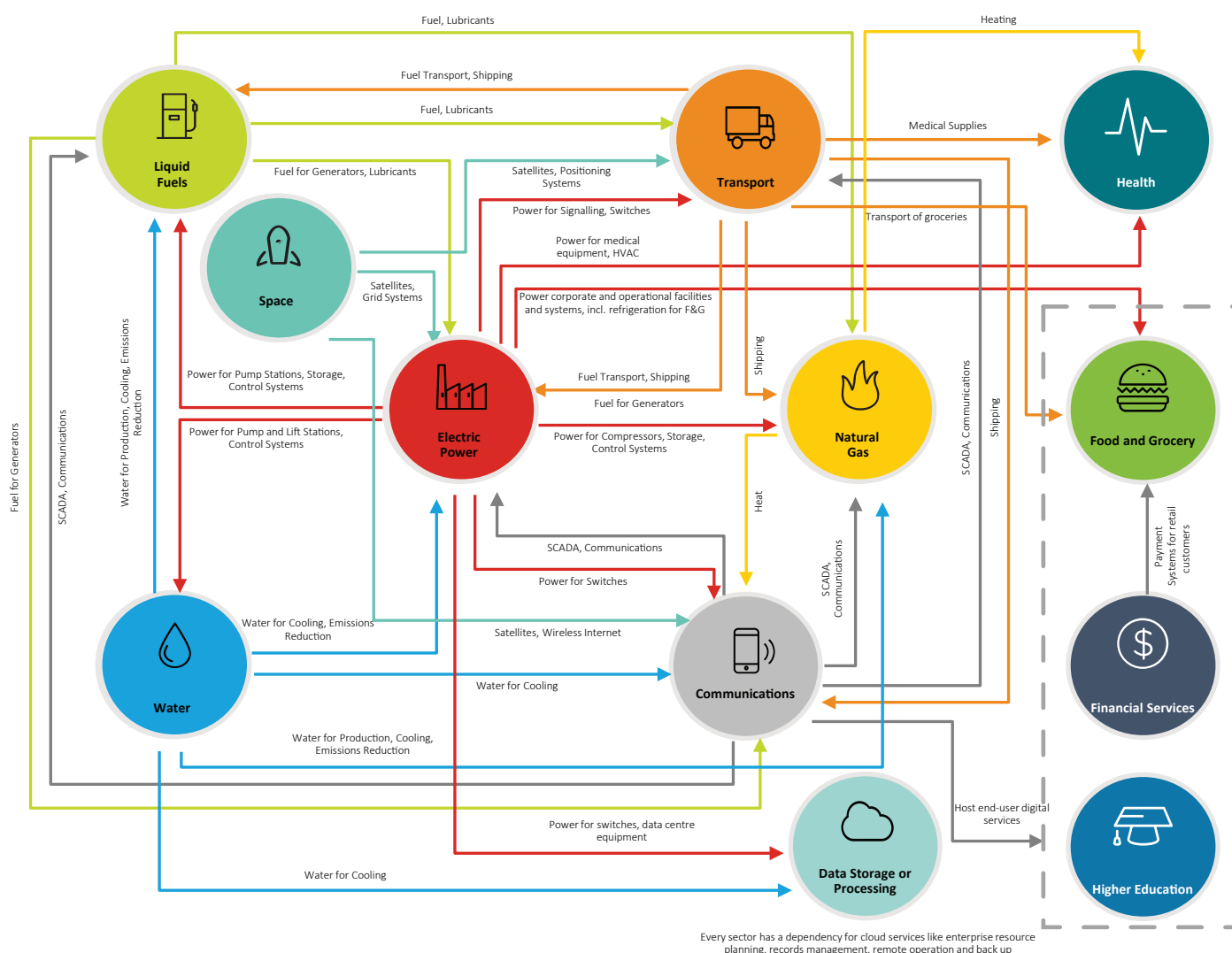
## Interdependencies (upstream and downstream)

### Sector interdependencies and relationships

Because critical functions can be exposed and vulnerable in the event of failure within another critical infrastructure sector, a critical infrastructure entity needs to carefully consider the sector interdependencies that interact with its operations as part of any critical infrastructure risk assessment.

The Healthcare and Medical Sector is an upstream dependency of a number of other critical infrastructure sectors; as much as other sectors rely on its downstream services. The following diagram provides one example of the explicit connections and dependencies, both upstream and downstream, that extend across critical infrastructure sectors.

Figure 4. An example of sector interdependencies and relationships

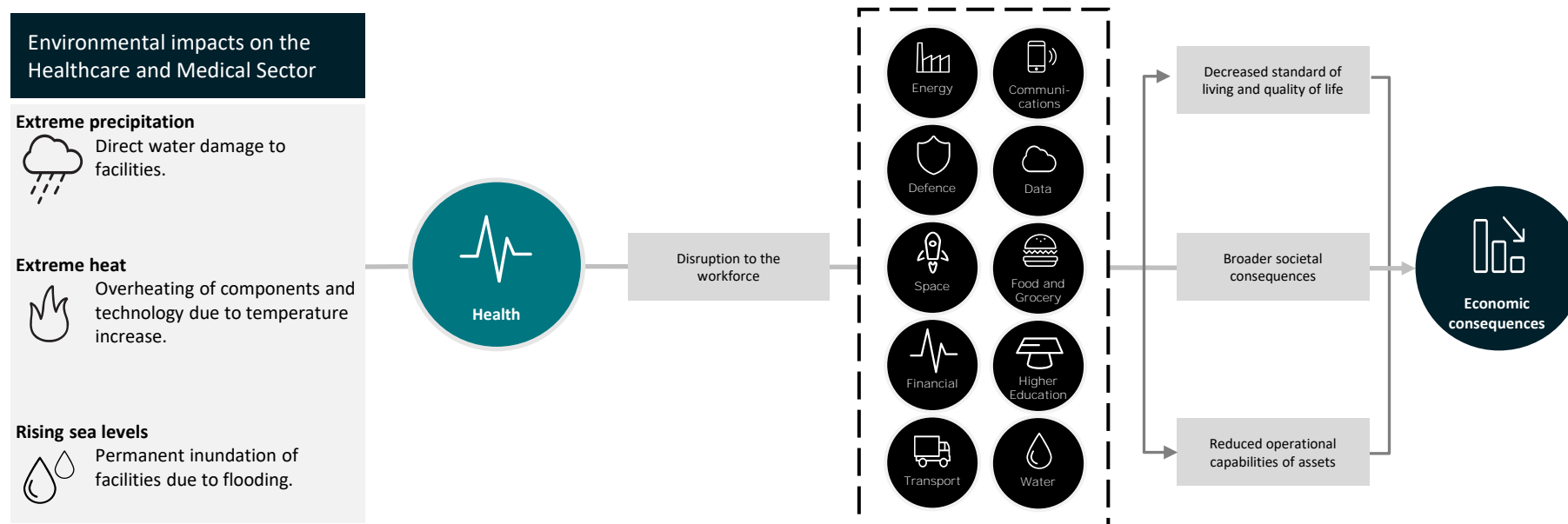




## Flow-on effects for relevant impacts against Healthcare and Medical Sector assets

The following diagram illustrates an example of the potential flow on effects to other interdependent critical infrastructure sectors following an impact from a possible threat or hazard event on the Healthcare and Medical Sector.

Figure 5. Example of flow-on effects from an impact against the Healthcare and Medical Sector





An outage affecting a critical asset in the Healthcare and Medical Sector could result in significant economic or societal implications, with effects including loss of life, reduced patient care, reputational damage, and financial and productivity loss. Examples of recent major incidents include:

- In mid-May 2021, hospital computer systems and phone lines in New Zealand were affected by a ransomware attack. Some surgeries were postponed as a result and seriously ill cancer patients were flown to Australia for treatment.
- At the height of the COVID-19 pandemic, it was discovered that low-quality respiratory masks were making their way into the US supply chain, with masks advertised as N95 (filtering out 95 per cent of particles) were actually filtering only 35–80 per cent of particles. This had the potential to put lives at risk as frontline workers may have been using unsafe or ineffective personal protective equipment.
- A woman in Germany died after being unable to receive medical treatment during a ransomware attack on a university hospital, in what is generally considered the first death directly linked to a cyber-attack on a hospital.
- The ACSC Annual Cyber Threat Report – July 2019 to June 2020 identified healthcare as a leading target for cyber attacks in Australia, second only to Australian Government entities.
- In May 2017, an entity in the United Kingdom experienced a widespread infiltration of the WannaCry ransomware, software which encrypted files before attempting to extort funds in Bitcoin; this resulted in the cancellation of over 19,000 medical appointments and caused more than GBP92m in damages and recovery costs.
- In 2018, the health records of over 1.5 million Singaporeans were compromised when their centralised medical health record database was infiltrated in a targeted cyber-attack, demonstrating the potential impact of sophisticated attackers seeking to exfiltrate medical information.
- A ransomware attack against two Australian health entities resulted in widespread outages across multiple systems; the consequent prioritisation of emergency procedures led to the turning away of patients with elective surgery needs

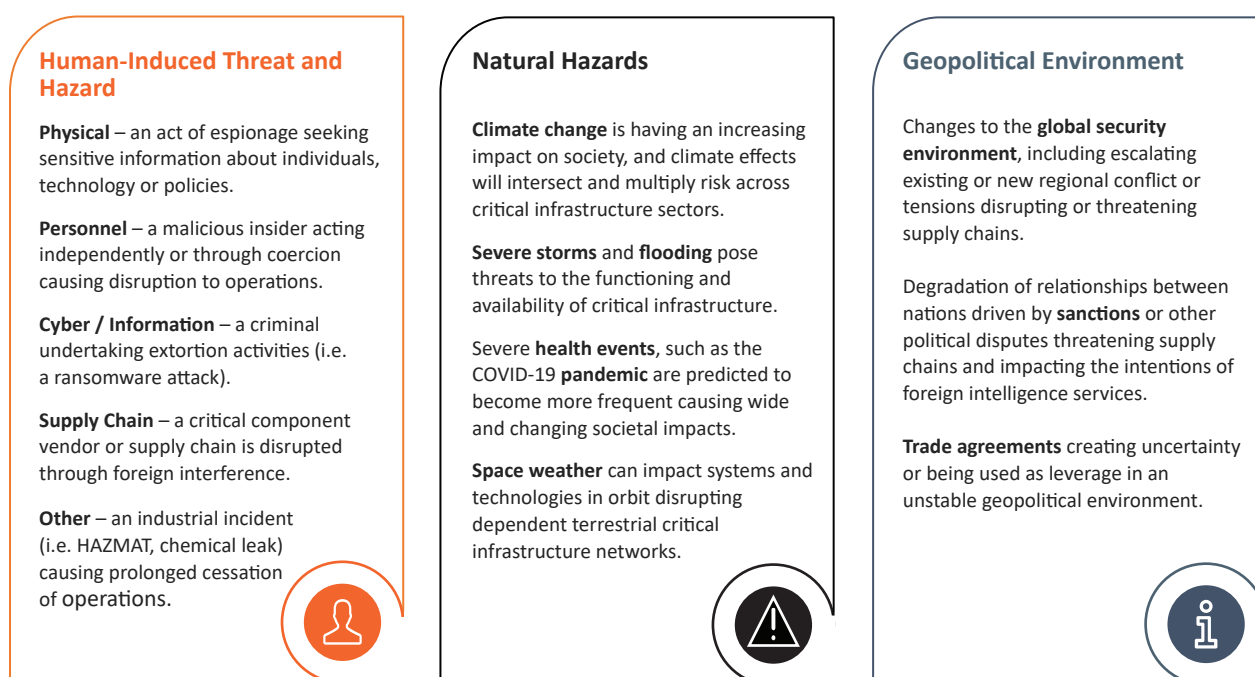


## Understanding threats and hazards for risk

### Identifying a threat and hazard landscape of the Healthcare and Medical Sector

All-hazards risk assessment considers both human-induced and natural threats and hazards. Given its role in critical infrastructure, the Healthcare and Medical Sector is an attractive target for threat actors seeking societal disruption; and natural hazards can severely damage infrastructure and, supply of critical equipment and medicine. A strategic representation of a threat and hazard landscape to a critical infrastructure sector could be structured as follows:

Figure 6. A representation of a threat and hazard landscape to critical infrastructure



It is essential to maintain a broad view of all-hazards risk and management activities for critical infrastructure that covers cyber/information, physical, natural, personnel and supply chain security, to continually monitor for likely threats and hazards.



The nature of physical, personnel, cyber, and supply chain threats to the sector is increasingly sophisticated and well resourced, and the frequency and magnitude of attacks is escalating. Additional considerations might include geopolitical tensions, pandemics, and the demonstrated potential for cyber technologies to be used as a long-distance act of aggression by nation states or other actors.

Threats will increase and the Healthcare and Medical Sector, driven by improvements in technology and the need to meet commercial outcomes, will become more interconnected. This means that stakeholders in the Healthcare and Medical Sector need to reevaluate risks regularly. The Healthcare and Medical Sector is especially susceptible to Natural hazards and associated risks due to its support function in caring for persons affected by these hazards. An example of this is the COVID-19 global pandemic, immense pressure from which has stretched the Healthcare and Medical Sector beyond its capacity, resulting in, for example, reduced availability of elective surgeries.






## Understanding sector-specific risks

This table outlines a select example of identified threat and hazard vectors that impact Healthcare and Medical Sector assets. When identifying risk in a critical infrastructure, each threat or hazard vector should be considered alongside the areas of an entity's operation it may potentially impact to allow for a more impact-led determination of plausible risk scenarios to assess.

	Threat or Hazard Vector	Risk Scenario Considerations
 CYBER / INFORMATION	Foreign interference	<ul style="list-style-type: none"><li>Confidentiality</li><li>Integrity</li><li>Availability</li></ul> Countries seeking to disrupt Australia's critical infrastructure may use advanced persistent threats or other modus operandi to scope, exert influence or attempt to disrupt healthcare and medical services or response.
	Cyber-espionage	<ul style="list-style-type: none"><li>Confidentiality</li><li>Integrity</li><li>Availability</li></ul> Cyber espionage could be used to exfiltrate, monitor, intercept and manipulate data pertaining to personal medical records or sensitive and commercial research.
	Financially-motivated cyber-crime	<ul style="list-style-type: none"><li>Confidentiality</li><li>Integrity</li><li>Availability</li></ul> Ransomware deployed into the networks of healthcare and medical providers has the potential to halt the functioning of an asset for extended periods with the intent to extract financial benefits.
	Remote access to operational technology	<ul style="list-style-type: none"><li>Confidentiality</li><li>Integrity</li><li>Availability</li></ul> Remote technology is often used to access interface between an asset's IT and Operational Technology (OT) systems. This can be exploited by malicious actors to gain quick and easy access to critical systems.
 NATURAL	Pandemic	<ul style="list-style-type: none"><li>Confidentiality</li><li>Availability</li><li>Reliability</li></ul> Pandemics such as COVID-19 have the potential to greatly alter the functioning of society, increasing the need for hospital beds and medical care, placing significant strain on the sector as it seeks to respond to the crisis while maintaining levels of general health care to the public.
	Severe weather event	<ul style="list-style-type: none"><li>Availability</li><li>Reliability</li></ul> With increasing extreme weather events, people in affected areas may experience difficulties in accessing emergency healthcare facilities or medical response, which could be compounded if weather impacts impede access to affected areas.

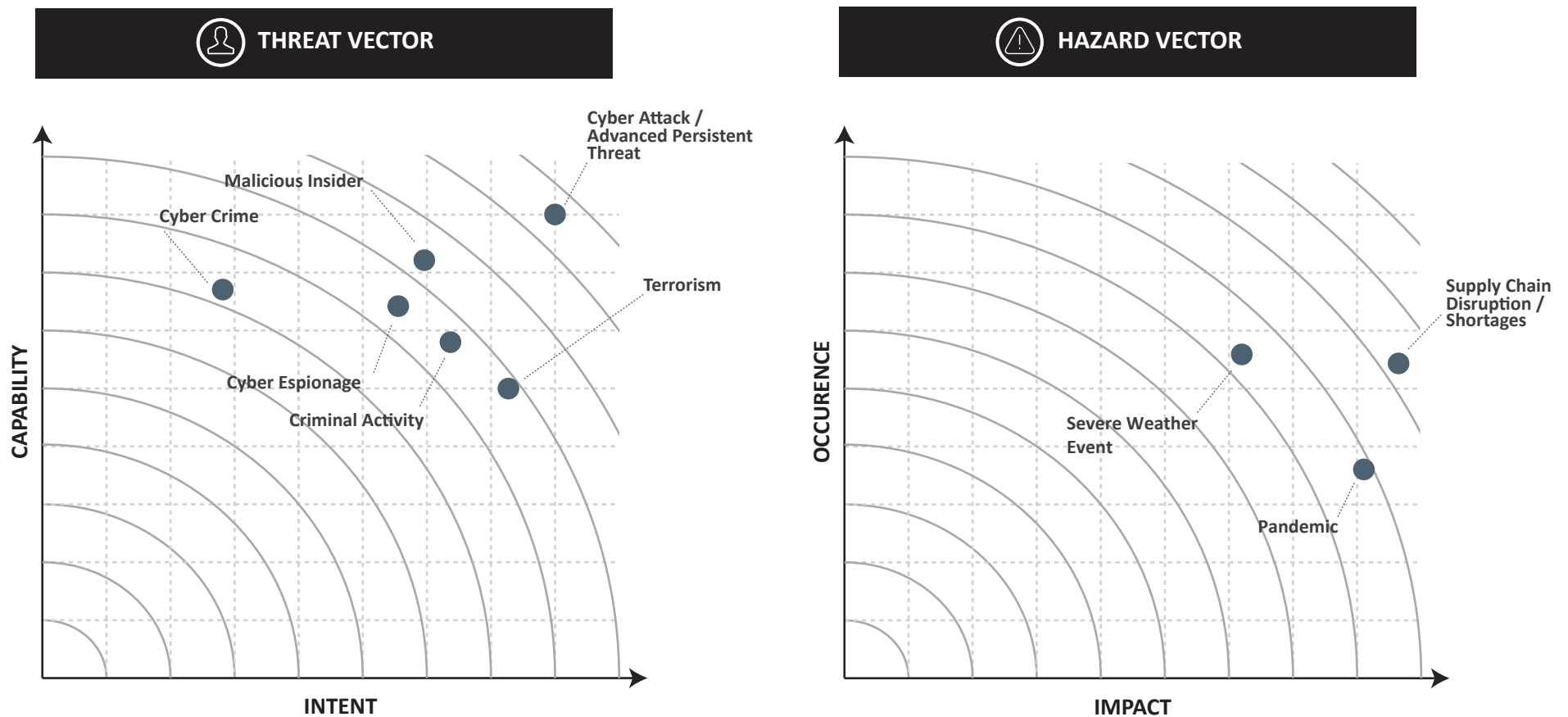


	Threat or Hazard Vector	Area of Potential Impact	Risk Scenario Considerations
 PHYSICAL	Criminal activity	<ul style="list-style-type: none"><li>• Integrity</li><li>• Availability</li><li>• Reliability</li></ul>	Criminal activity can cause damage through fraud, theft or coercion. These criminal activities can have broader consequences such as reputational damage and loss of income.
	Terrorism	<ul style="list-style-type: none"><li>• Confidentiality</li><li>• Availability</li><li>• Reliability</li></ul>	Groups that seek to make political statements through unlawful means may intentionally damage medical or hospital facilities as a second- or third-order effects in order to restrict levels of response.
 SUPPLY CHAIN	Supply issues/shortages	<ul style="list-style-type: none"><li>• Confidentiality</li><li>• Availability</li><li>• Reliability</li></ul>	The reliance of the sector upon international supply lines and resources can have a significant impact through labour shortage or shortcomings in critical supplies.
	Failure of third-party management	<ul style="list-style-type: none"><li>• Availability</li><li>• Integrity</li><li>• Reliability</li></ul>	Supplies provided by foreign may be affected by international sanctions, and even if components are available Australian communication entities may not be able to purchase needed components.
	Foreign Interference in supply chain by extra-judicial actions	<ul style="list-style-type: none"><li>• Confidentiality</li><li>• Integrity</li><li>• Reliability</li></ul>	Since third parties remain outside the security control of a given health asset, the compromise and failure of a third party can pose a threat to a healthcare asset. Fallout effects can only be mitigated, not prevented.
 PERSONNEL	Malicious Insider	<ul style="list-style-type: none"><li>• Confidentiality</li><li>• Integrity</li><li>• Availability</li><li>• Reliability</li></ul>	A trusted insider has the ability to cause significant damage to critical infrastructure such as deliberately disclosing privileged information or manipulating system used by assets with the intent to cause harm. For the Healthcare and Medical Sector, malicious insiders may seek monetary gain by providing medical records to third party actors.

## Prioritisation of sector threats and hazards

Organisations will need to form their own view on the threats most relevant to their operations. The following diagram provides a suggested approach to considering the prioritisation of threat and hazard vectors to the sector, by mapping them against intent and capability (threat) and, impact and occurrence (hazards). Understanding this prioritisation of threat and hazards is a key input to assessing levels of risk likelihood.

Figure 7. A representation of prioritisation of threat and hazard vectors



Source: Deloitte Risk Advisory and Cyber and Infrastructure Security Centre



## Risk controls and mitigations

Due to interdependencies among different critical infrastructure sectors and assets, it is necessary to manage many risks collectively. Many risks may be poorly addressed because their causes or effects are still misunderstood, they are novel, or there is a lack of guidance on how to address them. Accountabilities for addressing some risks may also be unclear. Some risks may be too rare to justify allocation of resources to mitigate them. Finally, the consequences may be too large for any entity to address by itself.

For a given Healthcare and Medical Sector asset, the disablement of its resources will cause issues downstream issues in other sectors that are potentially vast and more detrimental to other industries than the direct damages to the asset.

Ongoing analysis of risks can lead to a better understanding of mitigation strategies, including their application at the source.

Business continuity planning, consequence management, emergency management, disaster mitigation, vulnerability assessment, insurance and other related disciplines all provide a variety of possible actions.

Once controls and mitigations options have been identified by an entity, these should be continually evaluated and prioritised, particularly as threats and vectors evolve. The following criteria can be used for development of an implementation plan for risk controls and mitigations:

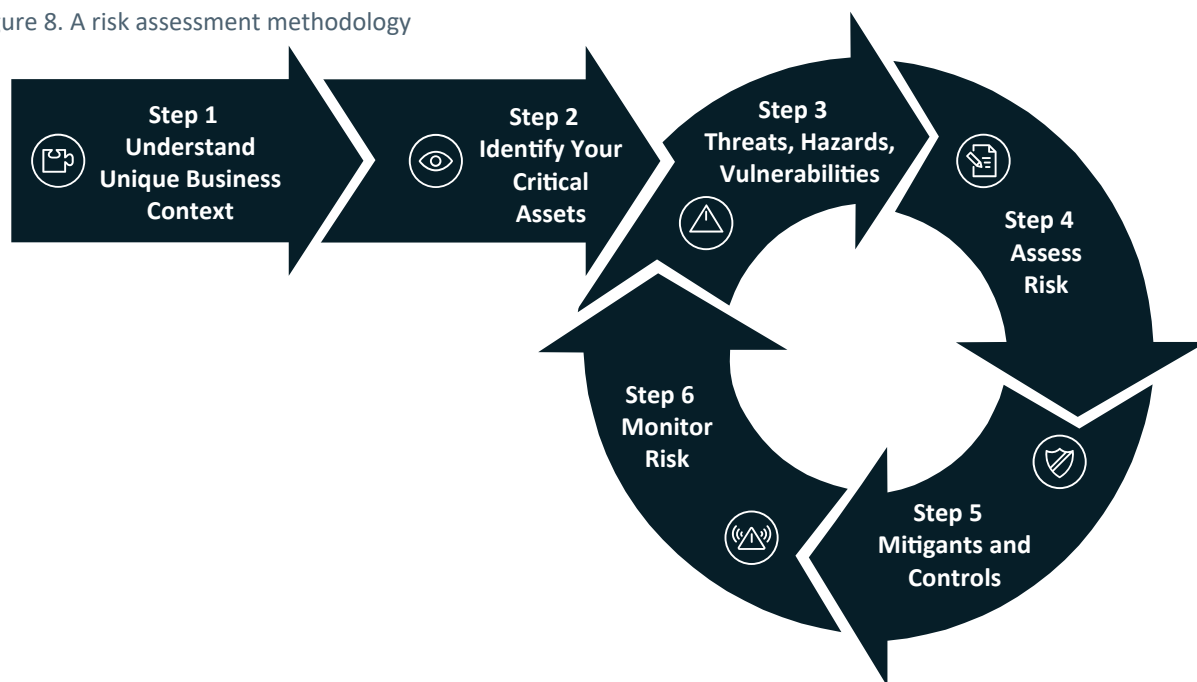
- Ease of implementation
- Cost-effectiveness
- Whether the action creates new risks and/or unintended consequences
- Environmental impacts (positive and negative)
- Multi-objective actions
- Long-term and short-term results
- Effectiveness
- Direct and indirect benefits
- Legal, regulatory, social and moral obligations
- Efficiency
- Equity and acceptability
- Timing and duration.



## Appendix – A risk assessment methodology

Healthcare and Medical Sector organisations looking to improve their risk management processes may want to consider this six-step approach to risk assessment, developed specifically to cater for critical infrastructure assets:

Figure 8. A risk assessment methodology



### STEP 1 – Understand business and sector landscape and how it fits under critical infrastructure

Identify the context of your individual organisation within both the Healthcare and Medical Sector and the Australian economy. Articulate your business objectives, identify your business threats, and understand the security regulations and legislative requirements that you need to follow. There is no one-size-fits-all approach for risk assessment and management. Organisations will need to determine how best to minimise and mitigate risk.

**Outcome** – Understand operational context for your business.





## STEP 2 – Identify your critical assets

Identify what you need to protect. What is valuable to you? Which services, assets and components if disrupted, damaged, or destroyed would adversely impact what is valuable to you? These are your critical assets. Consider: systems, services, networks, people, data, information, and other key elements. Identify dependencies and interdependencies.

Determine what is required for the continuing function of your 'critical infrastructure asset'. What are the key sites and components required to achieve the function of your asset? Components include systems, services, networks, information.

**Outcome** – Determine critical sites, components and personnel required to operate your critical infrastructure asset.

## STEP 3 – Threats, hazards and vulnerabilities

Analyse the threats and hazards that are likely to cause harm to identified critical infrastructure assets. Include consideration of known vulnerabilities that might impact assets, as well as information from the sector more broadly on similar organisations that have been targeted and how this was done. This can also include analysis of threat actors, their motivations and how they might gain access to and attack those assets (who, why and how).

**Outcome** – Identify the most relevant threats and hazards for your particular organisation.

## STEP 4 – Assess risk

Evaluate the risk that each threat poses. How likely is it that the threat might eventuate? What are the potential consequences if the threat is realised? Analyse existing controls that might reduce the likelihood and/or consequence of a security incident. Consider intent and capability for threats, and likelihood and consequence for hazards such as natural disasters.

**Outcome** – Identify risks relevant to your organisation that are likely to impact the confidentiality, integrity, availability or reliability of your critical infrastructure assets.

## STEP 5 – Identify mitigations and implement controls

Decide if the initial outcome of each risk is within a tolerable level, or if additional controls should be implemented. Implement the necessary controls and then update the risk profile (with altered control descriptions, likelihood and/or consequence). Controls might include technology controls, physical controls and/or activities across the spectrum of prevention, protection, detection, mitigation, response, and recovery.

**Outcome** – Treat identified risks as much as 'practicably possible'.



## STEP 6 – Monitor risk

Effective risk management is never a point-in-time exercise; it needs to be ongoing to cater for ever-evolving threats and changing assets and infrastructure that organisations need to protect. Use metrics to measure progress and effectiveness of security risk management activities, supported by appropriate governance arrangements. Undertake continuous improvement measures to harden critical asset vulnerabilities through activities such as red-teaming, post-incident review, and continuous assurance activities. Ensure the outcomes of these activities are used to regularly update and improve the existing spectrum of risk management practices. Maintain a positive security culture and high levels of security awareness.

Organisation size and complexity should determine how regularly risks should be monitored and reviewed, but an annual review or risk management processes is recommended at a minimum.

**Outcome** – Continual monitoring of risks and update to treatment strategies where required.