HARDENING CYBER SECURITY SUPPLY CHAINS

A GUIDE FOR AUSTRALIAN CRITICAL INFRASTRUCTURE

omni

CYBER SECURITY COOPERATIVE RESEARCH CENTRE

INTRODUCTION

The critical infrastructure supply chains of today are characterised by complexity, interconnectedness and fragility. One weak link in the chain can have significant and far-reaching ramifications for availability, reliability and redundancy, resulting in threats to the economy, national security and community safety.

Traditionally, organisations have focussed on physical supply chains – those that ensure the provision of manufactured goods and the delivery of particular services. In our digitally connected world, however, cyber security supply chains are now as important as physical supply chains - they underpin everything from payment systems through to production and automation. Furthermore, given the operations of much critical infrastructure extends across national borders, the cyber security supply chains that support them may also be impacted by geopolitical shifts and new and emerging threat vectors.[1]

As noted by the Department of Home Affairs' Cyber and Infrastructure Security Centre (CISC): "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".[2] Therefore, it is vital that critical infrastructure owners and operators consider their cyber security supply chain and potential risks and weaknesses it may present.

As various products, people or entities come into contact with your organisation's data and systems, their own exploitable gaps or faults can impact the security, integrity and availability of your data. The extent of impact and the guise it takes can vary according to the nature of the contact and/or the role that the product, person or entity has in the storage or transmission of your data. Therefore, it is vital to evaluate and monitor how well your orgnanisation's third-party suppliers manage their own cyber security. Often that means engaging in some calculated risk. And, as with any risk, it is vital to be as well informed as possible.

This guide was created by Omni and the Cyber Security Cooperative Research Centre (CSCRC) to help critical infrastructure owners and operators – as well as the information and communications technology (ICT) organisations that support them – develop a stronger understanding of cyber security supply chain risks. Rather than attempt to reinvent key domestic and international guidance regarding cyber security supply chain resilience, this guide augments existing information in a way that can be easily understood and digested by a non-technical audience.

Key guidance covered in this guide includes that produced by the Australian Signals Directorate (ASD), the CISC, the CSCRC and the Australian Institute of Company Directors (AICD), the National Institute of Standards and Technology (NIST), and the European Union Agency for Cybersecurity (ENISA).

[1] ICC-2024_Protecting-the-cybersecurity-of-critical-infrastructures-and-their-supply-chains.pdf
[2] 2024 Critical Infrastructure Annual Risk Review

THIS PROJECT WAS A COLLABORATION BETWEEN THE CSCRC AND OMNI

CYBER SECURITY COOPERATIVE RESEARCH CENTRE

omni

WITH THE SUPPORT OF

Australian Government
Department of Industry, Science and Resources

Cooperative Research Centres Program

WHAT IS A CYBER SECURITY SUPPLY CHAIN?

The Oxford English Dictionary defines 'supply chain' as "the routes or means by which supplies are received and the chain of processes involved in the production and distribution of a commodity".[3] Therefore, in cyber security terms, it is helpful to think of the cyber security supply chain as any product or entity that touches, houses or controls your organisation's data.

This could include everything from an internet service provider (ISP) through to computer hardware and software, or entities used to store your data. It comprises all suppliers, manufacturers, distributors and retailers through which an organisation procures cyber security products and services,[4] an interconnected network of hardware, software, personnel and data flows delivering digital products or services, from development through to deployment and ongoing support. This includes managed service providers (MSPs), cloud service providers, data centres, software and hardware providers, and the personnel that deliver these services.

According to the ASD, the first step in enhancing organisational cyber security supply chain risk is identifying and mapping all suppliers, manufacturers, distributors and retailers, and, where possible, their subcontractors.[5] However, this can be difficult, meaning organisations should identify their most valuable assets and systems and map these specific cyber security supply chains as a priority.

The ASD's *Annual Cyber Threat Report 2023-24* highlighted cyber security supply chain risk, noting that "it is essential that organisations undertake due diligence on a supplier's products and cyber security practices before and while engaging suppliers".[6] According to the report, in FY 23-24, the ASD responded to 107 cyber security supply chain incidents, comprising about nine per cent of all incidents.[7]

WHAT IS CRITICAL INFRASTRUCTURE?

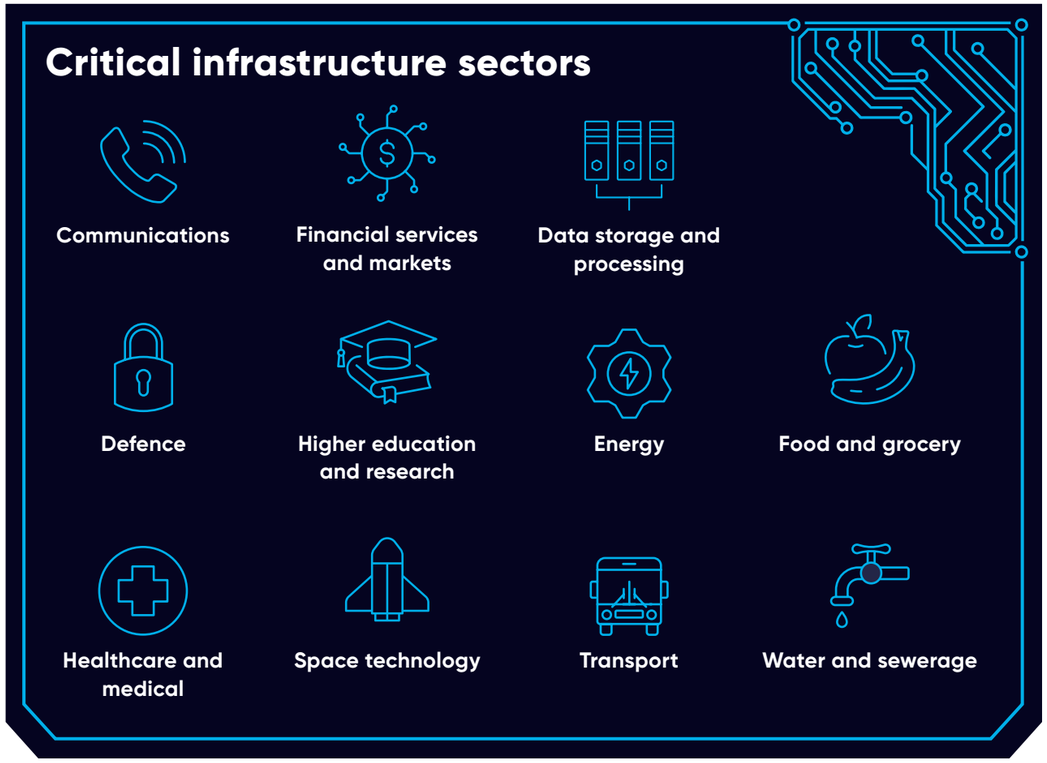
Over the past several years Australia's critical infrastructure regime has undergone significant reform. The number of captured sectors has been expanded from three to 11 and enhanced security obligations have been enacted for the nation's most critical assets.

Critical infrastructure is defined by the CISC 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".[8]

Under the *Security of Critical Infrastructure Act 2018*, (SOCI Act) captured entities are required to take an 'all hazards' approach to risk management across their operations, especially in relation to cyber security. Those assets identified as systems of national significance (SoNS) have enhanced cyber obligations under the SOCI Act, requiring them to adopt, maintain and comply with a written risk management program, develop a cyber incident response plan, undertake vulnerability assessments, run cyber security exercises and provide system information to develop and maintain a near real-time threat picture.[9] Furthermore, under new amendments to the SOCI Act obligations relating to the protection of 'business critical data' have also been clarified, explicitly requiring such data to be adequately protected.[10]

Certain entities are also required to lodge a board-attested Critical Infrastructure Risk Management Plan (CI-RMP) with the CISC. The CI-RMP's role is to identify all hazards that present a material risk to a critical infrastructure asset's availability, integrity, reliability and confidentiality, outlining measures that have been undertaken to prevent or mitigate each risk.[11] For example, mitigations could include enhanced cyber security controls, background checking of critical personnel and having back-ups of key systems.[12]

The CISC's 2024 *Critical Infrastructure Annual Risk Review* noted numerous incidents of supply chain attacks, with an enhanced need for critical infrastructure asset owners to "assess and take into account the overall quality of the products and cybersecurity practices of their suppliers, including whether they apply secure development procedures".[13]



[3] Logistics and supply chain (The University of Manchester)
[4] Cyber Supply Chain Risk Management | Cyber.gov.au
[5] Cyber Supply Chain Risk Management | Cyber.gov.au
[6] ASD Cyber Threat Report 2023-24
[7] ASD Cyber Threat Report 2023-24
[8] Security of Critical Infrastructure Act 2018 (SOCI) (cisc.gov.au)

[9] Security of Critical Infrastructure Act 2018 (SOCI) (cisc.gov.au)
[10] 2023–2030 Australian Cyber Security Strategy: Legislative Reforms | CONSULTATION PAPER
[11] Draft Risk Management Program Guidance for Industry (homeaffairs.gov.au)
[12] 2023–2030 Australian Cyber Security Strategy: Legislative Reforms | CONSULTATION PAPER
[13] ENISA

WHAT IS CYBER SECURITY SUPPLY CHAIN RISK?

Cyber security supply chain risk refers to the potential for harm or compromise that may arise from cyber security suppliers and their supply chains, products, services and personnel. According to NIST, cyber security risks throughout the supply chain generally result from exploitable vulnerabilities or exposures within products and services themselves or threats that exploit vulnerabilities or exposures within the supply chain itself.[14]

The CISC's definition via CI-RMP guidance takes a broader approach, defining supply chain hazards as "malicious actions to exploit, misuse, access or disrupt the supply chain; an overreliance on particular suppliers, and other disruption from issues in the supply chain, including a failure or lowered capacity of supply".[15]

Over the past several years, significant cyber security supply chain attacks have highlighted the ability of malicious actors to exploit vulnerabilities in third-party suppliers, either to gain access to the systems of a specific company or to undertake cyber operations at scale. This was highlighted by Australia's Director-General of Security Mike Burgess in 2024 threat assessment, which noted that: *"ASIO has uncovered cases where foreign spies have travelled to Australia with the intention of setting up sophisticated hacking infrastructure targeting computers containing sensitive and classified information"* [16]. Therefore, establishing clear cyber security expectations and responsibilities with third-party suppliers about their cyber security responsibilities are important to manage and mitigate such risk.[17]

ATTACK TECHNIQUES USED TO COMPROMISE A SUPPLY CHAIN	
Malware infection	e.g. spyware used to steal credentials from employees
Social Engineering	e.g. phishing, fake applications, typo-squatting, Wi-Fi impersonation, convincing the supplier to do something
Brute-Force Attack	e.g. guessing an SSH password, guessing a web login
Exploiting Software Vulnerability	e.g. SQL Injection or buffer overflow exploit in an application
Exploiting configuration vulnerability	e.g. taking advantage of a configuration problem
Physical attack or modification	e.g. modify hardware, physical intrusion
Open-source interlligence (OSINT)	e.g. search online for credentials, API keys, usernames
Counterfeiting	e.g. imitation of USB with malicious purposes

Source: ENISA

[14] Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
[15] 2024 Critical Infrastructure Annual Risk Review
[16] https://www.intelligence.gov.au/news/asio-annual-threat-assessment-2024
[17] 2024 Critical Infrastructure Annual Risk Review

CUSTOMER ASSETS TARGETED BY A SUPPLY CHAIN ATTACK	
Data	e.g. payment data, video feeds, documents, emails, flight plans, sales data and financial data, intellectual property.
Personal data	e.g. customer data, employee records, credentials.
Software	e.g. access to the customer product source code, modification of the software of the customer.
Processes	e.g. documentation of internal processes of operation and configurations, insertion of new malicious processes, documents of schematics.
Bandwidth	e.g. use the bandwidth for Distributed Denial of Service (DDoS), send SPAM or to infect others on a large scale.
Financial	e.g. steal cryptocurrency, hijack bank accounts, money transfers.
People	e.g. individuals targeted due their position or knowledge.

Source: ENISA

Prominent software supply chain disruptions

SolarWinds: The SolarWinds Orion attack that occurred in 2022 was a massive supply chain hack that impacted more than 30,000 organisations – public and private – around the world. The attack was the result of threat actors inserting malicious code into a legitimate Orion update which, when deployed and installed by customers, activated malware that allowed the threat actors access to their systems. Given the sophistication of SolarWinds, it is believed the attack was the work of a state-sponsored threat actors.[18]

Kaseya: The Kaseya ransomware attack occurred in 2021, compromising MSPs and their clients around the world. attack manifested itself and raised the need for further and dedicated attention to supply chain attacks affecting managed service providers and their customers. To launch the attack, threat actors exploited a zero day vulnerability in the software, enabling them to bypass authentication and gain authenticated access.[19]

MOVEit Transfer: In 2023, MOVEit Transfer software - which enables organisations to move large amounts of often sensitive data over the internet - was compromised by hackers, impacting more than 1000 organisations around the world. The attack occurred when a zero day vulnerability was exploited by threat actors, allowing access to MOVEit Transfer's servers and the theft of customer data. It is estimated the attack has resulted in damages exceeding US$9 billion.[20]

CrowdStrike: In July 2024, a bug in cyber security platform CrowdStrike's software update validation system failed to detect an issue with the update, which was pushed out, resulting in outages all over the world when the update was automatically downloaded.[21] In what has been described at the largest IT outage in history, the incident resulted in business systems around the world being rendered unavailable. The CrowdStrike outage starkly illustrates how overreliance on a particular vendor can have far-reaching impacts right across the economy and the globe.

[18] 4 companies charged by SEC for misleading investors after SolarWinds breach - Cyber Daily
[19] An in-depth analysis of the Kaseya ransomware attack: here's what you need to know
[20] MOVEit, the biggest hack of the year, by the numbers | TechCrunch
[21] CrowdStrike outage: We finally know what caused it - and how much it cost | CNN Business

EVALUATING RISK

Evaluating cyber security supply chain risk can be difficult – a range of factors need to be taken into account, as well as every organisation's own unique risk profile. However, there are several key approaches to evaluating cyber security supply chain risk owners and operators of Australian critical infrastructure should consider.

As noted previously, under the SOCI Act critical infrastructure owners and operators are required to adopt an 'all-hazards' approach to evaluating risk. Furthermore, the SOCI Act highlights that supply chain risks form a key part of such an all hazards approach, including cyber security supply chain risks. The regime encourages organisation to consider their risk profile in relation to their unique characteristics and assets. Therefore, for entities required to comply with the SOCI Act, it is foreseeable that all risks associated with connected systems should be considered, especially under the new data protection provisions.

The ASD's *Cyber Supply Chain Risk Management* guidance provides a strong framework through which organisations can evaluate and manage risk. By providing advice for organisation's to identify the cyber supply chain, understand cyber supply chain risk, set cyber security expectations with suppliers, audit for compliance, and monitor and improve cyber supply chain practice, the guidance is a practical and pragmatic tool.[22]

These key principles of the guidance are explored below.

ASD's Cyber Supply Chain Risk Management guidance

Identify the cyber supply chain: Identify all suppliers, manufacturers, distributors and retailers, and where possible, their sub-contractors. Know what data they process and what processes rely upon them. Update and review regularly.

Understand cyber supply chain risk: Consider factors like ownership of cyber supply chain entities, their security practices, their level of transparency, and governance. Develop a list of trusted suppliers, manufacturers, distributors and retailers.

Set cyber security expectations: Clearly document cyber security expectations in contracts and agreements – this will help provide assurance that an organisation is fulfilling its cyber-related obligations. Ensure that such contracts or agreements include the requirement for transparency in the event of a cyber incident.

Audit for compliance: Undertake routine audits or technical assessments to satisfy your organisation that cyber supply chain providers are fulfilling their cyber-related obligations. Such activities should be stipulated in contracts and agreements.

Monitor and improve cyber security supply chain practices: By working closely with parts of your organisation's cyber security supply chain, security practices can be strengthened and enhanced over time. For this to occur, the relationship must be based on trust, transparency and collaboration.

Source: ASD
The NIST framework for evaluating risk is also a useful four step plan, which considers risk as an ongoing process. It is outlined below.

NIST framework for evaluating risk

Frame risk: Establish the context for risk-based decisions and the current state of the enterprise's information and communications technology and services and the associated supply chain.

Assess risk: Review and interpret criticality, threat, vulnerability, likelihood, impact, and related information.

Respond to risk: Select, tailor, and implement mitigation controls based on risk assessment findings.

Monitor risk: Monitor risk exposure and the effectiveness of mitigating risk on an ongoing basis, including tracking changes to an information system or supply chain using effective enterprise communications and a feedback loop for continuous improvement.

Source: NIST

Assessing cyber supply chain risks: Australian Government resources

ASD

- *The Information Security Manual (ISM)*
- *Cyber Supply Chain Risk Management*
- *Identifying Cyber Supply Chain Risks*
- *Choosing Secure and Verifiable Technologies*
- *Exercise in a Box*

CISC

- *Critical Infrastructure Annual Risk Review*
- *Trusted Information Sharing Network*
- *Organisational Resilience Health Check Tool*
- *AusCheck background checking*

[22] Cyber Supply Chain Risk Management | Cyber.gov.au

CYBER SECURITY SUPPLY CHAIN GOVERNANCE

In the second edition of their *Cyber Security Governance Principles* (the Principles), the Australian Institute of Company Directors (AICD) and the Cyber Security Cooperative Research Centre (CSCRC) focus on the governance of the cyber security supply chain. In particular, the Principles highlight that, while outsourcing certain digital functions can bring cyber security benefits any gains should be balanced with specific cyber and supply chain risks.

The Principles note that board oversight of due diligence, monitoring and reporting on key external providers is critical to understanding how a particular outsourced function impacts the cyber posture of an organisation. Furthermore, it is essential to monitor the performance of key providers via interviews, testing or certification checks and vendor security assessments. The board may also obtain additional oversight on key providers through the provider itself presenting to the board and/or the use of independent assurance.

According to the Principles, key components of the board oversight of cyber security supply chain risk may include:

- Understanding the location and ownership structure of the provider, including interdependencies with other IT systems and infrastructure providers, shareholdings, links or cooperation arrangements with foreign governments and foreign intelligence agencies;
- Understanding and monitoring the cyber security posture and settings of the partner, encompassing what contractual obligations it regarding cyber security and adherence to standards benchmarks;
- Visibility of how a key provider utilises subcontractors or partners to provide the services, as well as notification obligations when these subcontracting arrangements change;
- Security considerations are appropriately captured in contractual obligations and oversight arrangements, for example reporting by the provider and notification settings for incidents of supply failures;
- The role of these providers is appropriately reflected in the organisation's cyber security strategy and related plans; and
- Direct engagement by the board with key supplier representatives, including interviews or presentations.

The basics of cyber security supply chain risk oversight for boards

Supplier diversification: Use multiple suppliers for critical products or services – don't rely on a single provider.

Geographic distribution: Spread suppliers across different regions or countries to reduce location-specific risks.

Data backups: Maintain copies of crucial data and system in separate, secure physical or virtual locations.

Stockpiling: Maintain an inventory of critical hardware or software.

Source: AICD/CSCRC Cyber Security Governance Principles

Key questions to consider

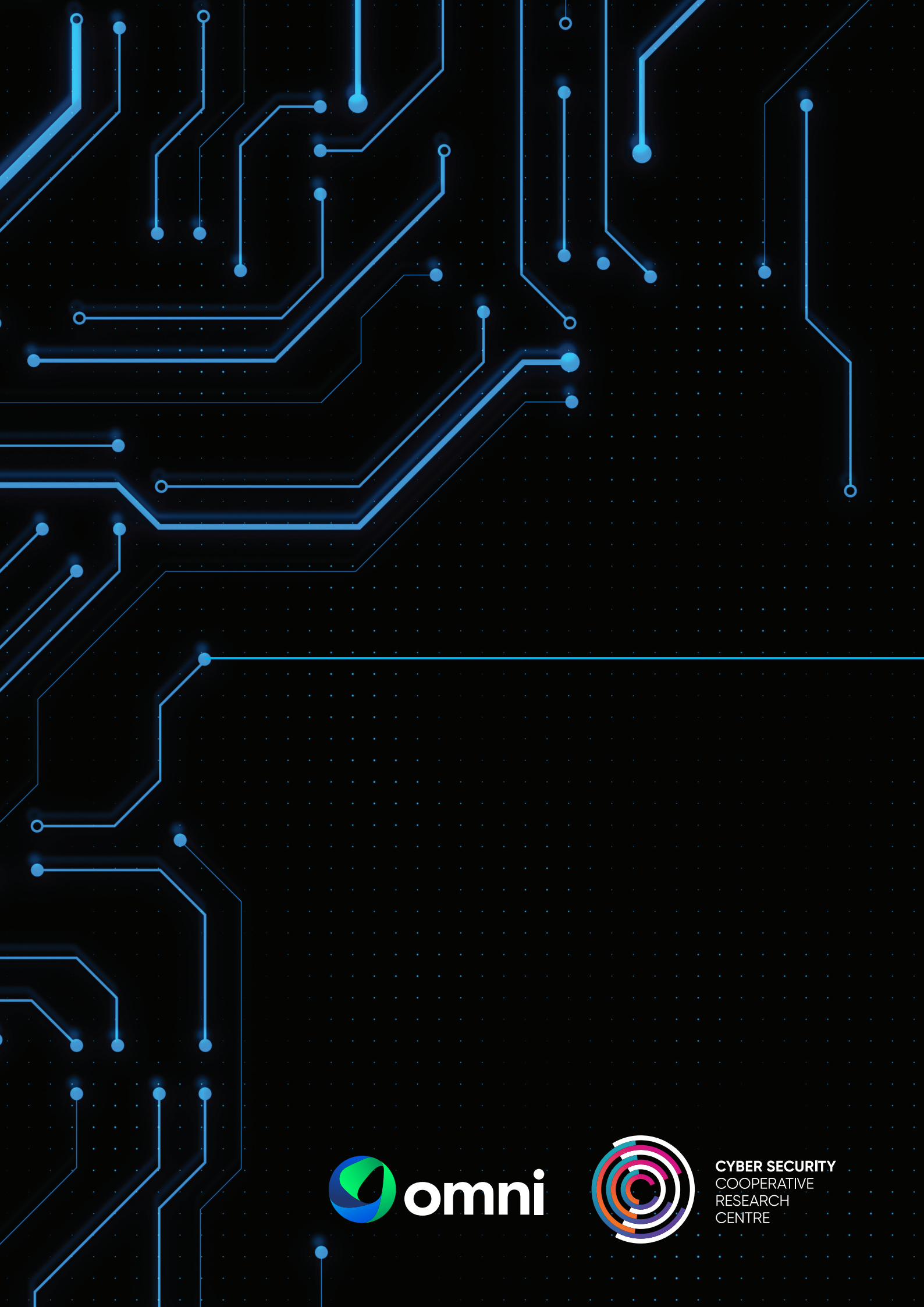
- Who are your organisation's ICT suppliers and service providers? Have they been mapped in terms of criticality? Has a singly point of failure been identified?
- What are your organisation's key cyber security supply chain risks? Have these been noted in the cyber security strategy, incident response plans and risk registers?
- Where are your ICT suppliers located? Who owns these companies? Where and how is your business critical data being stored?
- Are existing and emerging cyber threats being monitored and reported on? Have responses to such plans been simulated?
- Are personnel aware of the risks? Have the personnel of ICT staff with access to sensitive information been appropriately vetted?

Source: ENISA

CONCLUSION

Almost all Australia's critical infrastructure is reliant upon digital systems. Therefore, ensuring the cyber security of these systems is vital and key to this is effective management of cyber security supply chain risk.

While there is no silver bullet to ensure cyber security, which can never be fully guaranteed, the practical advice provided in this guidance will help owners and operators of Australia's critical infrastructure build a stronger understanding of what their cyber security supply chain comprises, what the key risks are, and how they can be managed.


omni
CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE