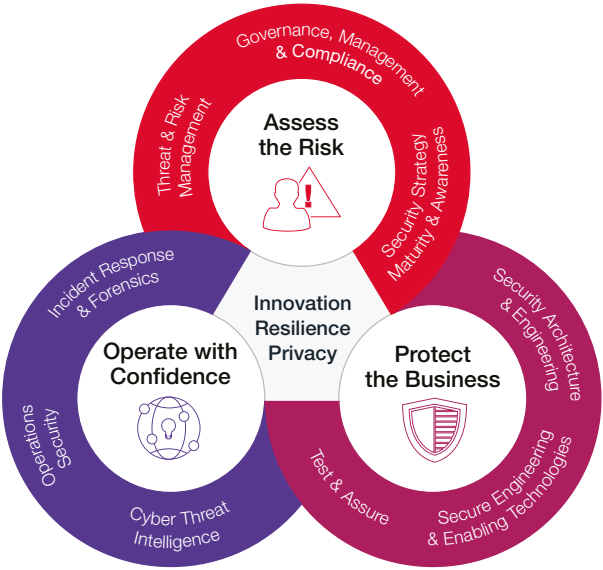
THIN**GUIDE**

Securing Critical Infrastructure

Australian Edition

A plain language guide presented by CGI

Cyber security is part of everything we do



Insights you can act on

At CGI, cyber security is part of everything we do. For more than 40 years, we have helped clients manage complex security challenges with a business focused approach – protecting what is most valuable to them.

For more information please visit
cgi.com/au/cyber-security

Email **sales.aus@cgi.com**

CGI

Foreword

Securing Australia's Critical Infrastructure is just that, critical. Recent legislation, including the Security Legislation Amendment (Critical Infrastructure Protection), has increased and better defined the obligations placed on Australian companies and citizens to strengthen our resilience against hazards and threats that impact the Australian way of life.

This guide sets out how CXOs and board-level decision-makers can approach securing Australia's Critical Infrastructure. The advice enclosed applies to all organisations whose assets are critical to business operations. It can also support you in setting up best practice protocols to mitigate reputational and financial damage to your organisation, its customers and your team members.

If time is of the essence, we encourage you to simply skim the headings and action lists in each chapter and think about how you apply the advice to your organisation. It might make all the difference.

THIN**GUIDE**

Securing Critical Infrastructure

Australian Edition

Published by Thin Guides Limited, London
Email: info@THINGUIDES.com

Typesetting, artwork, printing and binding by Mayfield Press (Oxford) Limited.

To read this THIN**GUIDE** online go to:

bit.ly/CGI-SCI

or scan the QR code.

www.THINGUIDES.com
Registered in England and Wales. Company N

THIN **GUIDE**

Securing Critical Infrastructure

Australian Edition

Authors
David Topping
David Tebbutt

Glossary

ACSC: Australian Cyber Security Centre which now includes Critical Infrastructure advice

CI: Australian Critical Infrastructure

CISC: The Government's Cyber and Infrastructure Security Centre

ECSO: Enhanced Cyber Security Obligations

IEC64423 series: Helps secure IACS throughout their lifecycle

(I)IoT: (Industrial) Internet of Things – connected objects that collect and exchange data

ISO/IEC 27000 series: Information security management standards

NISD: Network and Information Systems Directive protects critical national infrastructure IT systems

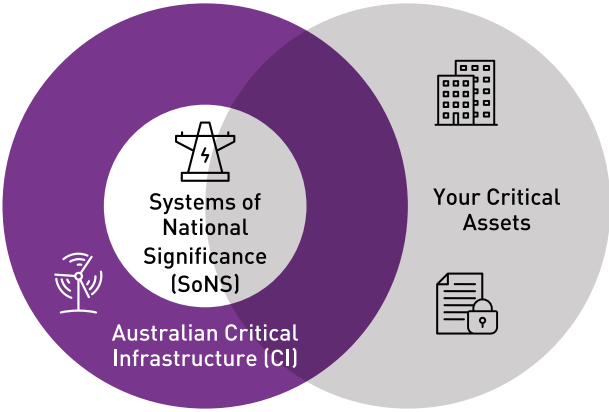
NIST CSF: The US National Institute of Standards and Technology's Cybersecurity Framework

OT: Operational Technology

RMP: Risk Management Program – an obligation under the SLACIP Act

SOCI, SLACI, SLACIP: Acts of Parliament to protect Australian CI

Contents


Systems of National Significance (SoNS)
Australian Critical Infrastructure (CI)
Your Critical Assets

Critical Infrastructure and you

Australian Critical Infrastructure (CI) is all the 'critical infrastructure assets'; the core services, businesses, organisations, institutions, and designated Systems of National Significance (SoNS), that the Commonwealth needs to ensure the ongoing operation of a modern economy and the services required to support its citizens.

If you are responsible for one or more of Australia's CI assets this guide will help you find out what you need to know and what you are required to do to secure it. The advice in this THIN**GUIDE** can equally be applied to your critical assets.

The Department of Home Affairs has identified and created legislation to cover eleven CI Sectors.

- Communications
- Food and grocery
- Financial services and markets
- Health care and medical
- Data storage or processing
- Space technology
- Defence industry
- Transport
- Higher education and research
- Water and sewerage
- Energy

The current legislation amends the original SOCI Act (Security of Critical Infrastructure Act 2018) and clearly defines which organisations and companies are included.

For each sector, the legislation defines varying types and classes of critical assets. As well as those mentioned above, these can include specific items of equipment or even people. They can be individually designated by the government as a named System of National Significance (SoNS) – the most structurally vital assets in Australia – or classified because of their size or effect on a significant number of citizens. Examples could be energy or water suppliers to >100,000 customers, or hospitals with a critical care unit or simply an organisation that supplies a service to the Commonwealth. They can be public or private businesses, organisations, or institutions.

This responsibility is far reaching and inherited; it not only lies with the organisation directly owning the critical asset or providing the service, but also on entities that own more than 10% of that organisation, regardless of nationality or legislative regime.

First Steps:

If you don't already know, your first step is to find out if you are affected. The Government's Cyber and Infrastructure Security Centre (CISC), an organisation set up to assist working with Australian CI, has a webpage that lists, for each sector, organisations and examples of assets that are included and how the new rules may be further developed:

bit.ly/CGI-CISCLEG

It is your responsibility to find out what your CI assets are and what your security obligations may be, such as mandatory cyber incident reporting, developing an enhanced cyber security policy or developing an overall risk management program.

If you're not a named SoNS or responsible for Australian CI assets, because you fall outside the numerous different sector parameters such as size, you may still have obligations because you are a supplier to one or more of those named organisations. Quite apart from this duty you are also helping to protect the Commonwealth.

Even if you are not subject to the legislation, securing your own critical assets is quite simply something you should do as a responsible business.

How do you secure CI?

While your own critical assets and Australian CI can be defined, how to secure them is not always clear. You need to agree what securing means for your organisation. This can only be done by the people who have ultimate responsibility. It might involve workgroups but, without commitment and understanding at the executive level, you are unlikely to create a good starting point and, without involvement across the organisation, you won't grasp the breadth and interconnected nature of risks.

Don't assume that 'Securing CI' is solely about security, either cyber or physical access. It is tempting, particularly in today's global climate to over-emphasise the risk of attack on infrastructure. Neither is it simply about conforming to legislation.

A risk mitigation model such as PPRR (Prevent / Prepare / Respond / Recover) only works when it is applied to the whole organisation and risks that encompass not only attack but natural disasters and equipment or supply chain failure. Securing your critical assets is as much about long-term

preparedness and planning as it is about responding to short-term incidents.

What is Failure?

Failure is when the following measures of value are not fulfilled: availability; integrity; reliability; safety and confidentiality. Imagining what could cause failure of these items is the key to what securing your critical assets and their role in Australia's CI infrastructure means.

This encompasses every aspect of your business or organisation, from cyber security for IT and Operational Technology (OT), to physical access security. Through plant maintenance to supply chain security or flood mitigation. Different businesses will have different priorities; a bank might concentrate on IT cyber security, a hospital on OT and backup power.

Every aspect can affect another, if your power fails then your IT systems fail, if your IT fails your access security may fail. This is why the whole business or organisation must be involved in the assessment of what securing your CI means.

- Find out if you are part of Australia's CI or a SoNS
- Start to Assess what securing your critical assets might involve
- Decide who must be involved
- Understand what constitutes a failure

Establish leadership

Securing critical assets is a board level responsibility. As an officer, an appointee, or someone with delegated authority, securing these assets is part of your job. Because of the wide nature of the risks it means the whole board must be involved. If your business or organisation is part of Australia's CI, this becomes a legal obligation as well.

Failure to secure your critical assets is likely to lead to a failure to deliver your goods or services, which can then lead to a loss of reputation or customer confidence and a subsequent loss of profit and shareholder value. And, because securing CI is a company-wide issue, not just IT or OT, it has to be led from the top.

While many Australian businesses have a board member responsible for cyber security; a Chief Information Security Officer (CISO), few of them carry responsibility beyond cyber infrastructure.

Appoint a leader

An early step is to appoint someone to lead your security efforts. Whether securing your critical assets or Australian CI assets this 'CI Security leader' has the same four primary responsibilities: representation, management and risk ownership, compliance, and improvement.

Representation

The CI security leader's most important role is to create and spread awareness of critical asset and CI security and its requirements. This will involve evangelism and change management as well as rigour and ability to deliver.

They need to represent CI security interests at board level, to the company as a whole, and to external business partners and responsible or regulatory entities. They also need a basic understanding of all stakeholders' interests, requirements and legal or other obligations. As such, they will need to be a good communicator, business savvy and a strong influencer.

Management and risk ownership

The CI security leader has to actively manage the company's efforts across every department and interest group and create actual or matrix teams to assess risk and develop policy, respond to incidents or events, create and run awareness, education and training programmes.

In addition, this role must carry responsibility for your own or Australian CI assets, identifying them, documenting them, and ultimately ensuring they are secure, if necessary, by accepting risk ownership. That will include IT and OT systems as well as physical infrastructure or people.

The leader needs to be the clearly identifiable single point of contact, inside the company and for external partners, the government and the public. They need to be suitably empowered and have the appropriate authority to make sure that things happen.

Compliance

If the business or organisation is subject to Australian CI regulation or any other regulations or standards, as most are, the leader needs to understand enough of the regulations to know how to comply and then monitor and demonstrate that compliance is being met.

Compliance works beyond your own organisation – the CI security leader needs to ensure that suppliers and partners are able to ensure continuity and quality of supply, as well as conforming to your security rules, policies and standards.

Improvement

Threats, technology, equipment, regulations, partners and employees all change over time. All need to be monitored continuously and your CI security policy and risk management plans need to be measured, monitored, and improved to match those changes.

Incidents, simple accidents and natural disasters happen, and your CI security leader needs to ensure that lessons learned are included into improved programmes to prevent recurrence of any negative outcomes.

Who is your leader?

Given the all-encompassing nature of critical asset security and the legal obligations if it's part of the Australian CI, it might seem that the leader needs to be an impossibly multi-talented person. In fact, they simply need to have 'sufficient knowledge', leadership ability, credibility, and personal authority.

The choice will also depend on the risk assessment that's unique to your business. A financial services business, for example, depends heavily on IT and it may already have a CISO. They will already have the broad skills, structures and systems in place so adding to their responsibility could suit that business best. An energy distribution company might assess risk differently and place physical plant, maintenance and security at the top. Here the role might be taken on by someone best able to manage continuity of supply.

For smaller businesses, where a dedicated role is not affordable, the choice is clear; it's the Chief Executive. Protecting your critical infrastructure is about business survival and that is the CEO's job.

Regardless of how you make your decision, it is more important to have someone who can deliver effective critical asset security than someone with the best 'security', legal or other qualifications. The board is responsible for all critical assets, whether part of Australian CI or not. This means you need that person to be at the most senior level and fully supported by the Chief Executive.

- Make critical asset and CI Security a board level topic
- Appoint an effective management leader of CI security with clear authority across disciplines
- Ensure that the CEO is fully supportive of the role

Appoint a response team

Your business will face an incident affecting your CI. It will be malicious, accidental, or a natural disaster. The severity of the outcome and its impact on your business will be determined by the actions you take during the first few hours of your response.

Your priority is to identify the impact, assess and fix the damage, address the cause, and mitigate any liability.

Don't waste those hours by failing to spot the incident, by having the wrong people dealing with it or delaying your response with internal 'blamestorming'.

Appoint a CI Response team **now**. Your CI leader and your board-level definition of 'Securing CI' will help identify likely candidates. Their first job will be to understand and document their own roles, responsibilities and interfaces to other CI Response team members and stakeholders.

The response team

Response team structures will vary between organisations depending on the nature of business. If required, speak to your security service provider for guidance. As a baseline, the essential roles are:

Main board member: Decides on and authorises the recommended actions of the incident manager – ideally your CI leader.

Incident manager: Assesses and oversees a) if an incident needs to be formally declared, the severity of the incident, if the CI response team needs to be activated and b) all the actions undertaken to stop, mitigate and repair the incident. The type of incident will determine who this should be – a response team decision.

Communications manager: Informs stakeholders (including customers, the public, investors and possibly government), response team members and the rest of the company of the status of an incident.

Legal adviser: Presents a clear view of obligations; legal, regulatory, or contractual; especially if it relates to Australian CI legislation.

Security or other experts (IT, OT, Operations, Work Health and Safety, etc.)**:** Plan and effect the actions needed to rectify and prevent or manage future incidents based on their detailed understanding of their specialised areas.

Each role needs a fully-briefed substitute.

Cyber desktop exercise

Even if your organisation is not subject to Enhanced Cyber Security Obligations (ECSO), a cyber desktop exercise is the simplest way to prepare a response team to be effective during a real incident. Participants role-play an incident: a natural disaster; an industrial accident; a ransomware attack; or something that has affected a similar business. It should be realistic and likely to affect all participants. Given the prevalence of cyber threats a cyber security exercise is a good example.

The team responds with its current level of knowledge about incident management including the processes, regulations and people involved.

Mandatory Cyber Security Incident Reporting: The team learns how to collectively address cyber incidents in a calm and orderly fashion, by creating a sector specific communications report template and breach details for the CISC. This will involve the incident manager, communications manager, legal adviser and board member review and sign off.

Information sharing / Awareness: The team shares its expertise, making each member aware of requirements and processes across the business. HR and Operations might be unaware of ECSO, likewise cyber security and Legal may be unfamiliar with Work Health and Safety requirements.

Learning / Working methods: The team learns to work together, what methods, training and communications are needed in or outside the team to manage situations and implement decisions.

Skills shortage: The team can identify missing skills or knowledge. "I don't know" is a good answer in an exercise; it shows that something or someone is missing. The team can include additional, and permanent, internal or specialist external resources to cover the gap.

Process integration: The team will have multiple security and safety processes, they might even be contradictory. These should be compared, integrated and the implications understood.

Risk assessment: The team's wide skills, expertise and knowledge gained from exercises make it best

placed to understand and quantify the business's material risks, vulnerabilities and consequences; "If this likely incident happens, our business closes for two weeks."

Written plans: The team's most important outputs are its written Incident Action Plans, making a playbook of the needed actions and communications for the team and the business.

These pragmatic plans must also be included in a more detailed 'Risk Management Program' (RMP). This is a mandatory requirement for organisations subject to Australian CI. Briefly, it covers physical, cyber, personnel and supply chain security plans as well as a risk assessment and reasoning for each documented critical asset.

These are your business survival plans; regulatory compliance is secondary. Anyone in or beyond the response team must be able to understand them and physically access them in case the network is down.

Finally, the exercises and outputs need to be repeated and constantly revised.

- Appoint a cross-function response team
- Run simulations to identify skills and knowledge gaps
- Fill skills and knowledge gaps (internally or externally)
- Input to board-level risk assessment
- Document pragmatic Risk Management / Action Plans
- Constantly revise and update

Understand the threat landscape

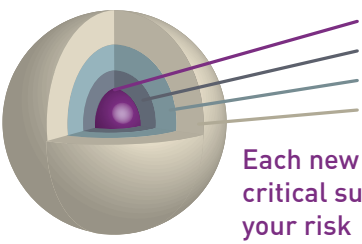
The number of entry points to your business has widened through things like operational technology, working from home, IoT, your connected supply chain and so on. Meanwhile, state actors and criminals have been improving their techniques and reach, especially in their ability to steal valuable information or cripple systems. In parallel, the number of natural hazards we face has grown in severity and breadth of impact - disruptive events such as flooding, bush fires and pandemics. All three have recently altered the way we do business. We also cannot ignore internal events such as perimeter controls and inattention to equipment maintenance schedules, for example.

It's clear that your security planning needs to embrace cyber, physical and natural risks. It means a holistic approach. A piecemeal approach to protecting your critical assets is doomed to fail. All your specialists and maybe some outsiders need to work together to maximise the protection needed by your business and its many stakeholders.

Assessing risk

Every business is different but an approach to identifying and quantifying your own risk can benefit from a common approach. This has to include internal IT misuse risk as well as that created by your partners and suppliers. This is covered in more detail in the *Know your partners and suppliers* chapter. A chain is only as strong as its weakest link so, in this sense, all potential threats to your

sources of supply need to be included. Do you need to establish alternative sources? How would your business survive a significant supply chain failure?



Each new participant in your critical supply chain increases your risk

A growing threat comes from the way in which an increasing number of your physical resources are becoming networked with IT and communication systems - your own and those of your suppliers who may require cloud-based access to your network for monitoring and maintenance of their installed equipment or services.

The *Assess risks and scope* chapter takes a deeper dive into this topic.

Threat categorisation

Threats can be intentional or unintentional. An unintentional threat could be an automated process or AI that goes wrong or plugging an unknown USB into a connected device. The remainder are natural events and other hazards.

Intentional threats are the ones most commonly discussed, certainly in the area of cyber security. The attacks may be carried out by inanimate programs, but they are definitely human-driven by state actors, criminals, influential organisations and individuals. Beyond cyber, lie deliberate

physical breaches such as interruption of critical supplies such as energy or raw materials. These may be driven by military or terrorist action.

Unintentional threats are usually the result of negligence or ignorance. This is why all employees need to be made aware of the need for vigilance and given a clear understanding of the risks and profound consequences that could result from a single accidental lapse. This could range from clicking on an unknown link to losing an access pass and failing report it. Any connected business partner could become an access point for malware. Exercise strong physical and digital access controls on everyone connected with your business.

The bottom line

The board of a business is responsible for all business risks. Maximising the security and safety of your critical assets and their resilience involves addressing the risks to your most precious assets. In doing this, you are helping yourself, your business, your partners and Australia itself.

- Know adversaries/threats/weaknesses
- Be clear about their motivations to attack
- Identify and protect the processes, information, and items that are most valuable to your business – your critical assets.
- Know where their threats lie
- Have systems in place for detecting and dealing with physical / cyber breaches
- Have an awareness and training plan to protect against human error

Assess risks and scope

The assessment of major risk is core to most organisations' normal business practices, although some concentrate purely on commercial risk or take a piecemeal approach.

Before you can assess and quantify a specific risk you should understand the scope of risk. For each major aspect of your business, factor elements such as:

- **Size and complexity**
- **Nature of business**
- **Profile and reputation**

These set the base level or scope of your risk. Large and complex businesses and organisations face higher risk because of the interrelationship of risk factors. A simple equipment failure can lead to a cascade failure in a complex system. The nature of your business, your profile and reputation can make you more or less of a criminal target. This base level gives you some idea of the likelihood of each threat or hazard you face.

If you are securing an Australian CI asset, the base level is automatically higher and you are simply more likely to be a target. Because it's CI, you also have to manage a greater level of complexity, which itself can increase risk. Every business needs to balance the costs of any action or inaction against the likelihood of loss, damage, or failure to supply. Most companies can secure themselves adequately at reasonable cost. However, if they are subject to greater risk, their costs will be disproportionately higher:

Australian CI legislation mandates the development of a Risk Management Program for affected businesses. Even if you don't have, own or operate any Australian CI, your business would benefit from a similar plan. The approach is:

- **Discover your critical assets and who owns them**
- **Assess the value to the business**
- **Assess the costs of protecting them**
- **Make, document and communicate your risk decisions**

Discover

First, you have to find out what you have, where it is and who is responsible for it. The starting point is any named critical asset and all critical assets which are part of a class of assets. These vary for each sector and can cover everything from specific equipment such as a distribution subsystem, to individual databases, monitoring and control systems, key people, or whole buildings.

Don't stop there. Look at related critical assets, whether they are part of Australian CI or not. Then make sure they are fully documented as to ownership and purpose. This audit process is essential and doing it thoroughly can save effort and avoid harm in the long term.

Assess the value

Every company is different, but the value of any asset is not purely monetary but also based on the consequences to your business if it is unavailable for any reason. It may impact other assets found in your discovery process. This assessment allows you to create a documented set of priorities for risk assessment and for the scale of effort you put in to secure it. The priority for a critical CI asset is clearly highest, and mandated, because of its impact on the Commonwealth. Even so, limiting this exercise to only CI assets introduces a vulnerability by failing to spot interdependencies.

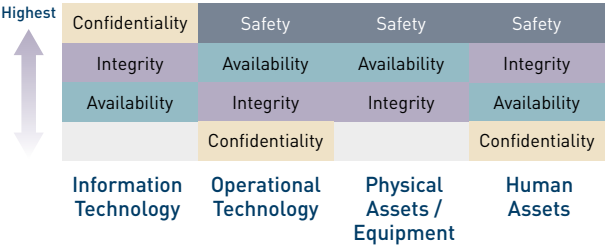
Assess the costs/risks

This is the core of this process. Your CI leader, response team and your desktop exercises will be invaluable. The assessment of risk scope, the audit of your assets (prioritising your CI assets), is the starting point.

Cyber security assessment principles available in standards such as ISO27001, IEC624423 or NIST CSF, provide frameworks that are also adaptable to physical assets and infrastructure. The priorities are driven by whatever can affect an asset's availability, integrity, reliability, safety and confidentiality. Given how pervasive IT and OT are,

and most businesses' dependency on them, this is often a good base point.

Cyber security priorities across CI assets



Desktop exercises should provide a risk assessment based on the likelihood of a threat, incident or hazard occurring. It will also reveal the vulnerability of an asset to those eventualities. The exercises should assess the cost and impact of the consequences, and asses what actions could be taken to prevent their occurrence and those costs. This is a full risk management assessment.

A desktop exercise in practice

An example might be a natural gas plant, declared as a SoNS. It has an effective maintenance management program with physical redundancy. The team decides that the primary vulnerabilities are cyber security related and models a malicious attack through partner access to billing systems and links from the IT systems to the OT systems causing a failure in monitoring. It assesses the time taken to restore the systems and the costs. Against this it can assess a plan that limits partner access, limits IT to OT links and checks analogue readings against digital readings.

An additional, valuable, step is to test the assessment and plan with penetration testing, both cyber and physical.

Document and Communicate Decisions

The final stage is that you must document the assessments and costs, and any subsequent preventative or remedial plans in a way that can be clearly understood by non-specialists. And communicate and feedback everything to all those likely to be affected by those plans, making clear the priorities and especially where low cost and easily implemented solutions provide quick wins.

- Discover your critical assets including people, processes, and data and who is responsible
- Assess potential loss and how at risk you are
- Apply security controls where they are most needed (physical and cyber)
- Document and communicate your decisions to the company/organisation
- Feedback into the review process

Create an organisation-wide culture

The preceding chapters will have given you an idea of the breadth and scope of effort needed to secure your critical assets and of your extra responsibility and obligations if you're securing Australian CI. Your board will be included, you'll have a (CI or overall) security leader and a company-wide response and risk assessment team. All asset/risk owners and anyone with security in their job title should be involved.

When considering security, some organisations look at employees solely as a risk factor. This is a lost opportunity. A good security strategy or plan will look at them as a potential front line of defence. However, you cannot secure your critical assets or Australian CI without the active, willing and informed involvement of the company and everyone within it.

It's not easy, in the battle between getting work done 'on time' and getting work done 'securely', 'on time' tends to win. This can lead to a conflict between your planning, be it maintenance management programs, IT or OT cyber security policies or location access guidelines, and reality. This will reveal itself in everything from lax maintenance, the refusal to adopt an unwieldy password policy, to tailgating through a control barrier.

You can't just hope for 'buy-in'; you need to include the whole company in your critical asset or CI security efforts from the start, so that everyone sees the RMP as part of the company culture and accepts it because it makes sense.

Inclusive critical asset security

Your RMP or plan could fail at the first hurdle if it's designed solely by your response team or security specialists. While the team will prioritise business continuity, resilience, safety and security (cyber or otherwise), it is essential to include a wider team from different departments across the company, with specialist security or even external guidance that can:

- **Provide a practical view of how people do their jobs, what information and IT or OT systems they depend on**
- **Set realistic requirements for everyday controls such as system/physical access and password policies**
- **Look at how to alter departmental processes to provide protection against common threats or hazards (unwanted intruders, ransomware, CEO fraud etc.)**

This inclusion can bring external skills into the company and, make them relevant to different departments. It is important that the recommendations are seen to be fed back into policy making. Doing so can create a team of knowledgeable inside evangelists – champions or trusted peers who can significantly assist your security leader in making any necessary cultural and behavioural changes.

These changes start with awareness, education and training.

Awareness

Management, specifically your overall security leader, is responsible for creating and maintaining company-wide awareness of the importance of securing your critical assets or Australian CI and the consequences of not doing so. Messages about its importance must be seen to come from the top of the company. But they don't need to be delivered in a completely top-down way. Your response team's communication manager, and your marketing department may have the skills needed to promote awareness through internal mailings, promotions, or gamification, for example. Your local respected evangelists or champions can reinforce these messages and even create their own.

Education and training

Education can explain why securing your critical assets or Australian CI is important, and the principles behind it. Training gives your people the necessary skills to secure the assets. They are not the same thing.

Both are equally important but might be provided to different groups. Education may be more appropriate to those who contribute to the processes; the expanded team mentioned above. They are the people who need to know the reasons for a policy in order to extrapolate from it to deal with unforeseen situations. Training should aim to get the whole company to adopt a standard set of behaviours. Neither should be seen as a one off, box ticking exercise imposed by your HR or Corporate Policy department. Experience shows that a continuous approach works best.

Company-wide

Company-wide has to mean everyone. No-one is exempt. Your initiatives will fail if the most senior managers and asset owners don't take part. That means being seen to support the development process, supporting the awareness, taking part (visibly) in the education and training and, ultimately, following the policies.

Continual improvement

This is critical and this THIN**GUIDE** has a chapter dedicated to the topic of 'review process', the essence of which is that awareness, education and training have to be ongoing because threats and hazards vary and develop. Your CI security leader, response team and the extended team will see these changes and will have to change your policies, plans and RMP to match their evolving views, assessments and experience.

Measurement

Measure improvements. Document them. This could start with just the number of people being trained. Some organisations create online tests to create an ongoing score for security familiarity.

- Involve people from across the company in critical asset/Australian CI security
- Actively encourage local evangelism and take feedback
- Develop and deliver awareness, education, and training as separate items
- Constantly assess, review and revise

Keep on top of laws and regulations

The legal landscape shifts periodically to reflect the rapidly deteriorating global security climate, both physical and digital. In Australia, this has been addressed by reviews of the original SOCI (2018) Act and the resulting SLACI and SLACIP Amendments.

The new rules and regulations will remain under continuous review and their details will inevitably change as new Critical Infrastructure threats to Australia and its citizens emerge.

Public and private businesses are at the forefront of this battle to defeat criminal and state actors, especially cybercriminals, and to protect the Commonwealth from natural or man-made problems.

These new laws and regulations, and others you may be familiar with, such as local state regulations and the Privacy law which dates back to 2001, represent a starting point for recognising threats and planning your responses.

Your team's knowledge of your business sector will be far more detailed than any legislator's and it's important that you take responsibility to operate in the spirit of the law as well as conforming to its explicit requirements when laying out the security policies for your organisation and its suppliers.

Here are just a few of the laws and regulations that relate most closely to Critical Infrastructure:

SOCI, SLACI and SLACIP Acts

These three acts are at the heart of protecting your and Australia's Critical Infrastructure. You can read the minute detail of these Acts in many Government sources or from many leading consultancies.

The broad detail is that SOCI (Security of Critical Infrastructure) focused on just four sectors: Electricity; Gas; Water and Ports. SLACI and SLACIP widen the catchment to eleven sectors.

SLACI introduced two new measures: an obligation to report cyber incidents; and a requirement to report ownership and operational information relating to critical infrastructure assets.

SLACIP requires responsible entities to create and maintain a critical infrastructure RMP and a framework of "enhanced cyber security obligations" that must be complied with by operators of Australia's most important CI assets referred to as Systems of National Significance (SoNS).

Failure to conform to the new requirements can result in significant fines – up to 200 penalty units for CI entities and 1000 for corporations.

Quite apart from the obligations, this is about reputation, doing what is right, defending and maintaining the safety of all Australians.

Examples of local regulations (the SLACIP Act may supersede them):

IPART Operators Licence Conditions: Independent Pricing and Regulatory Tribunal – NSW

OVIC's VPDSF 2: Office of the Victorian Information Commissioner

VAGO: Victorian Auditor General Office Audit Compliance

Privacy Act 1988

This law is under review at the time of writing, concurrently with the formation of an Online Privacy Bill, which addresses the privacy challenges posed by social media and other online platforms.

The resulting Privacy Act will have been informed by the outcomes of the Online Privacy Bill. The Act is supported by the Privacy Regulation 2013 and the Privacy (Credit Reporting) Code 2014. Its 13 Australian Privacy Principles (APPs) apply to government agencies and private sector organisations with an annual turnover of $3 million or more.

Cybercrime Act 2001

Cybercrime is criminal activity where a computer or network is integral to, or the target of, an offence. Some of its laws have been inserted into the Criminal Code Act 1995, the key offences being unauthorised access to and modification or impairment of data held in a computer or other device, and unauthorised impairment of electronic communications.

The provisions are regularly updated to ensure that law enforcement officers have the powers necessary to search for and obtain electronic evidence. Other Acts cover Telecommunications and Surveillance devices.

These obligations, and more, are complex. If in doubt, seek expert advice.

Standards

Hundreds of standards apply to security, ranging from management frameworks to the specifics of a piece of technology. Increasingly, production equipment, maintenance scheduling and building security systems are networked and digitally-driven.

If you are obliged to use any security standards and you are unfamiliar with them, it is well worth obtaining specialist advice.

ISO 27000 series

This offers a rigorous and comprehensive family of standards for protecting and preserving your information under the principles of confidentiality, integrity and availability. ISO 27000 is the most important document when it comes to cyber security. It is also a good source for templates which can help in CI documentation.

It acts as an excellent starting point for the adoption of ISO 27001, which covers IT and OT Operations, Human Resources, Supplier Relationships, Compliance and Physical Security – all key elements of your CI.

A business with ISO 27001 accreditation shows itself to be a cyber security aware and trustworthy trading partner.

If you start with ISO 27001, adapting to the requirements of the other standards (ISO 27031, 32, 35, etc.) should be a relatively smooth process.

IEC64423 series

The IEC 62443 series aims to secure industrial automation and control systems (IACS) throughout their lifecycle. It currently includes nine standards, technical reports and technical specifications.

Remember: security-aware suppliers and customers will be checking your credentials too.

- Know why regulations, codes of practice and standards are merely a starting point for an effective security strategy
- Make sure your security and non-security professionals are familiar with the requirements defined by Australian and recognised international regulations. e.g. ISO/IEC 27001
- Make sure they are aware of other legislation, standards and obligations specific to your company or organisation and your industry
- Make sure all your third-party contracts include a requirement for compliance with relevant standards
- Understand your statutory requirements and those of the stakeholders

Know your partners and supply chain

For a security strategy to be effective, it has to include any person, organisation or object that exchanges data with your IT and OT system or has physical access to your workplaces. Each represents a potential security vulnerability. Just as important, you need to consider the continuity of supply of essential materials and services in the event of a more widespread disaster such as the Covid pandemic or global semiconductor shortage.

Each of your business partners or suppliers faces similar risks. You need to ensure that their security and resilience measures match your own needs so that they don't become a chink in your armour. This applies to existing relationships as well as new ones. For larger organisations, this could mean thousands or tens of thousands of cascaded organisations.

Assess stakeholders

Stakeholders include everyone who interacts digitally or physically with your organisation. They could be website visitors who provide personal information. They may not carry responsibility but you still bear responsibility towards them. They will include anyone, typically suppliers, contractors and customers, who exchanges data with your system or who has physical access to your premises, including off-site workplaces. Your suppliers and contractors will agree to bear responsibility for participants in their own supply chain. Security of your critical assets is not just a cyber issue. It

even comes down to the people who service your physical equipment or deliver your parcels. No-one should be exempt from your scrutiny.

You will need to determine the level of access they have, whether it is appropriate and, according to that assessment, find out whether their security regime is sufficiently robust to protect you. Do they have a genuine awareness of, and experience in, CI security? And, if not, can they prove their cyber security credentials? You need to know who you can trust. Run an Australian National Police Check or background checks based on the AusCheck Scheme on your suppliers and contractors. Also, check their certification such as ISO/IEC 27001 and include a check on the certifying authority. They are not all equal. When it comes to CI security, you need partners who understand the requirements and who are willing to cooperate fully. This is not a box-ticking exercise.

Just as you protect your digital perimeter, so you need to protect your physical perimeter. Think of all the ways this could be threatened and put the necessary access controls in place.

Security requirements

Before you can embark on any security discussion with your stakeholders, you need to be unambiguously clear about your own supply and security requirements. Extract just the relevant requirements for each type of stakeholder to ensure that their access is appropriate to their function and no more. While an IT service provider might be happy to work with your full requirements, a small or medium business that interacts only

with your purchasing department will work with the relevant subset.

You will need to take a view on what you mandate for all your suppliers (and contractors and customers) and what you're prepared to slim down for special cases.

Responsibilities

The responsibility for maintaining good CI security lies with all parts of your business ecosystem. You and your stakeholders have to feel mutually secure. You will provide updates to requirements and new discoveries that affect them and they will reciprocate with reports of relevant incidents and actions taken. Ideally, you need to include your security expectations in your commercial contracts. These will include aspects such as what to do in the event of a failure to supply or security breach or what should be done with shared information or materials during the execution of a contract or at its termination.

If all these steps are covered conscientiously, you will be able to conduct business more confidently in a spirit of partnership with the stakeholders who would then be part of your extended CI security regime.

- Assess all relevant stakeholders
- Know which ones to trust
- Agree requirements, responsibilities, and service level agreements
- Control cyber system and physical access

Know how to get good advice

Unless you are exceedingly fortunate, you will find that your internal CI security expertise doesn't completely cover your requirements. You will have to find one or more external sources of help. It is vital that the people and organisations you choose will be valued and accepted as an integral part of your security team.

To stand the greatest chance of finding such help, you need to be clear about your requirements and know how to assess the prospective delivery partners. You will also need to check they will be able to deliver on expectations.

Identify your capability gaps

Once your security team has determined your needs, it will have identified the relevant skills and experience from inside the company. It will then have to recruit/train internally or draw on external services to compensate for any gaps. Given the breadth of critical asset security, few consultants or consultancies can cover all the ground.

To avoid overlaps and unnecessary complexity, it is important to be very clear about what you want to achieve through third parties. Only then are you ready to prepare your RFP (Request for Proposal) and go searching.

Find help

Many CI security specialists would probably claim to be exactly what you need. It is highly likely that more than a few are cyber security specialists flying the CI banner. It might help to hire someone with appropriate expertise to help you identify likely prospects. The Australian Cyber Security Centre is a rich source of helpful information and connections including a section devoted to organisations and critical infrastructure **bit.ly/CGI-ACSC**. The Australian Government's Cyber and Infrastructure Security Centre is also a valuable source of guidance. **bit.ly/CGI-CISCRES**

Look for expertise in:

- **Intimate knowledge of your industry sector**
- **Understanding of your CI technology solutions**
- **Creating security policies and strategies**
- **Risk management**
- **Assurance on effective security implementation**
- **Designing, implementing and managing/monitoring secure IT and physical systems**
- **Incident response to help you through a data breach**
- **Legal obligations**
- **Crisis management to help you respond to an incident**
- **Media handling to help you protect your company's reputation in a crisis**
- **Testing whether your systems can be penetrated**

- **Education and training that specialises in CI and critical asset security**
- **And many more...**

Assess prospects

Shortlist prospective consultancies according to a number of criteria:

Relevance: Do they understand your industry and your niche within it?

Location: Are their services delivered, and assets contained, within Australia?

Experience: How much relevant practical experience of your type of need do they have?

Staffing: How qualified and experienced are the staff they will deploy?

Certifications: Are their certification sources credible?

Independence: Are they vendor-independent?

Reputation: Find evidence of customer satisfaction from independent reviews, customer satisfaction ratings, industry reputation and published works.

Your RFP response evaluation will lead to a shortlist. Then you will need to ask them face-to-face to fill in any gaps. Their behaviour at this stage will tell you whether they are sufficiently open-minded and collaborative to work with you in a spirit of partnership.

Implementation

Having selected the right partner(s) from your shortlist, they need to become part of your team as quickly as possible. This means creating and agreeing plans, expectations and performance measures so that you can periodically measure the value they're delivering.

The details are up to your CI security leader, but they should include behavioural as well as technical measures. You need to know whether they're delivering the promised value and you also need to know if they are genuinely working as part of your CI team.

Remember that an important by-product for your company is the knowledge transfer that is bound to take place in a collaborative relationship.

- Determine what needs you cannot satisfy internally
- Specify exactly what you need from third parties
- Seek authoritative help from the CI community
- Shortlist and select suppliers that pass your assessment criteria
- Ensure they integrate with the teams and leadership
- Monitor their performance and collaborate for continual improvement

Document everything

Some companies find security documentation onerous and do it solely to comply with regulation. This is a mistake. It makes far more sense to consider documentation as a way of enabling compliance, communication and securing commitment. If you are responsible for Australian CI assets, you need to follow the obligatory documentation requirements, detailed below. The same documentation will be just as valuable in securing your own critical assets.

Within the broad terms above, you'll find six types of documentation:

Planning	**Training**	**Evidence**
Action	**Reporting**	**Contractual / legal**

Planning: Documents used for planning/strategy will be the most complete. They must include the full audit of critical assets; including ownership, physical location; and who should have access. The documents have to also explain the reasoning behind any needed actions such as the risk assessment for each asset and the steps needed to protect them. Each should reference, summarise or point to an action plan. These documents may be used to show compliance, communicate the plan and get commitment to the plan, both inside and, if necessary, outside your organisation.

Action Plans: They can be anything; a remedial equipment service policy, a cyber security password policy, or a building evacuation plan. They must communicate clear, concise and pragmatic measurable actions.

Training: To secure CI, everyone – from board level to field engineer – needs to be involved and trained. This should vary from simple guidance on action plans, to training programs that include some of the reasoning behind the actions. This both communicates and builds commitment.

Reporting: You cannot show progress nor compliance unless you measure and report it. Your strategic planning documents must also include these progress reports. Keep reports and reporting to the minimum needed to comply at any level and communicate the outcomes of your planning with KPIs for management and employees.

Evidence: "If it isn't documented it didn't happen." Whatever 'it' is – a certification, a training schedule, the entire published Australian CI RMP, or an incident – with no record of it, you can't show what happened or, indeed, that you would even know that it had happened. This is compliance proof, not just for Australian CI but also proof of best efforts and best practice in insurance claims. It is also the basis for improving your processes.

Contractual/legal: The *Know your partners and suppliers* chapter makes it clear that your contracts and legal agreements with your suppliers must reflect your needs. These may be congruent with Australian CI, both for supply and security behaviour. They, in turn, ensure that these needs

are reflected all the way down the supply chain.

The agreements then need to be audited and registered as part of your critical asset security. The same goes for agreements with the people responsible for the assets and carrying out your organisation's plans. This also applies to your officers or appointed executives.

What documents are required?

The exact details of documentation of the types mentioned will vary by business type. However, if you have, or are, an Australian CI asset or a SoNS you are obliged to produce a written RMP and an annual report.

RMP (Risk Management Program): As part of creating a Government-mandated template for a RMP, the CISC publishes regular updates. **bit.ly/CGI-CISCRMP** Independent sources provide various sector-specific Risk Management/ Assessment templates, but this is an area where it may be worth seeking expert advice.

The contents of the RMP are set out and subject to a set of rules. It must cover how you intend to manage material risk to critical assets from four main hazards: physical and natural, cyber and Information security, personnel, and supply chain. It must show the assets and their ownership, the risk assessment, and the actions taken or being taken to prevent or mitigate the risk.

The RMP is the summary, and distillation of the documented activities this guide has suggested – having a CI security leader, appointing and training a team to manage incidents, performing

an asset audit and risk assessment (documented), assessing your supply chain and partner risk, and communicating and reviewing your decisions.

Take a bottom-to-top approach, where individual detailed assessments or plans (cyber security for OT and IT, personnel strategy and equipment maintenance etc.) are distilled and aggregated, but the originals referenced and easily accessible. Your RMP, including reasoning and actions taken, can be understood and demonstrable to non-specialists.

Annual report: An annual report on the progress of your RMP is mandatory. However, that alone is not evidence that you have secured your critical assets. It should be a summary of all the monthly, or even weekly progress reports on each action plan, which are seen at every board meeting.

ISO/IEC 27001: This is not mandatory but if you're under Australian CI, you cannot operate without conforming to it.

Finally, your documentation should comply, communicate, and help build commitment. It has to have a defined review and re-approval date to ensure that it remains current. And it absolutely must be in a form that's available where it's needed.

- Create a legible practical CI security program
- Create a plan that can be measured
- Create materials that educate and train staff
- Report on progress at every board meeting
- Document all activities

Create a review process

By now, your security plan should be robust enough to deal with most types of everyday attack, hazard and even user error. The details will change over time as the threats against your critical assets change and as you learn and document better ways to increase your protection. CI security risk reviews should become a permanent agenda item of board meetings.

Your risk management plan determines all the primary areas of board level attention and direction – the 'why?' of the security strategy. They also address the 'what?' – the elements for which managers and digitally- or physically-connected business partners will be responsible. Finally, operational details will be defined at the 'how?' level. The framework itself will endure with little or no change because it was forged from a strategic, rather than an operational, perspective.

Your original goals and decisions will spread down towards everyone in the organisation. Each person will be responsible for minimising risk to critical assets in their area of activity. Reports will flow back up, triggering local actions and summary reports that form part of the board's monthly discussions of new risks, the effectiveness of existing remedies and the bottom-line impacts.

At a strategic level, CI security management is similar to any other major business activity. Perhaps the main difference is that recognised Australian CI organisations are legislated to

act on real-time intelligence from authorised outside sources such as the Australian Cyber and Infrastructure Security Centre (CISC). In any event, outside intelligence is vitally important to your security planning.

Your plan

Tackling security cannot be a one-off exercise. Prioritise the rollout of your actions according to the risks being tackled. Work on short, medium and long term (1-, 3- and 5-year) plans. Make sure they harmonise with existing security activities and plans. Each action will have a meaningful measure so that its progress or completion can be reported coherently.

At a high level, a 'framework' approach – where the whys, whats and hows are clearly identified – gives everyone involved the chance to understand and participate in the risk management plan's creation. By being involved, the participants acquire a sense of ownership and commitment to making their parts work. This approach can then be overlaid on an industry best practice framework, such as ISO27001, for a more detailed prescriptive implementation plan. At all times, progress will be clear and remaining gaps identifiable by matching progress to the framework.

For each of your critical assets that fall under the Australian CI regulations, you will be obliged to establish, maintain, and comply with an RMP to manage the material risk of a hazard occurring, which could have a relevant impact. The Government's Cyber and Infrastructure Centre offers a good starting point for understanding the requirements. **bit.ly/CGI-CISCRMP**

Review and measure

Revisiting your plans to test your original assumptions, measuring progress towards your goals, ensuring that budgets are being used wisely and that you have the necessary resources are just some of the reasons why it is so essential to conduct reviews. Material for review should be relevant to its audience. While the board might review summary feedback monthly, others inside and outside the organisation will be reporting on their security activities as required by the plan, sometimes on an hourly or daily basis. It is also important that the Board knows how ROI is being tracked. A board-level investment effectiveness measurement report is just as crucial as an operational control effectiveness report.

Some companies will employ internal audit teams to independently monitor the effectiveness of the security strategy. Given that your main thrust is to empower and encourage everyone involved, any such audit should be seen by all as 'checking that the plans are working' and that continual improvement is being sought.

Who drives the plan?

The main driving force will always be the company leadership team, which will include your chosen overall security or CI security leader. However, everyone who is digitally or physically connected to your business must be asked to conform to the obligations the CI security plan places upon them.

Operationally, it is clear that some people are better at looking at things objectively and communicating

their findings clearly. These rare individuals need to be identified and offered the extra responsibility. They would be providing a valuable service to both their colleagues and their managers.

Why get involved?

Every person involved in the company's CI security efforts will want to know "Why should I bother?" and "What's in it for me?" The simple answer is that their cumulative efforts will help your organisation to survive and thrive, protect its critical assets, maintain its reputation and ensure that stakeholder assets, especially those belonging to its customers, are safe and secure. Your risk management plans will ensure that everyone knows exactly what is expected of them.

- This CI process and Risk Management Program must constantly change, plan accordingly
- Make your plan visible – involve everyone who impacts your risk, inside and outside the organisation
- Ensure you have built in a bottom-to-top reviewing and reporting mechanism
- Make security part of your culture and motivate people to participate

Embrace the future

Apart from critical assets, customer service is core to your business. This means keeping up with technical and process innovations and doing it securely and according to your values. Three critical areas are access, responsiveness and productivity vs. safety.

Access

Customers and partners want 24/7 access to their data and your services through any device anywhere. To stay relevant, grow market share, meet customer expectations and maintain control of PR objectives, your business will need to embrace emerging technologies Unfortunately, this increases the risk of unauthorised access to your data at rest and in transit. Users of external cloud-based services may also face data sovereignty issues. Homomorphic encryption promises total security of data in transit.

Digital touchpoints including smart meters, AR, VR, wearables, voice and motion will extend today's more conventional platforms and interactions. IoT and 5G will be at the fore in these developments.

Responsiveness

Customers expect rapid responses, personalised to their needs. Response speed comes from high-bandwidth communications and putting processing and data close to the customer. 5G and cloud/edge processing and data will accelerate this. AI- and

ML-assisted automation facilitates decision-making speed and organisational responses.

Quantum computing promises even greater improvements in data handling and decision-making speeds while Influence Engineering uses behavioural science learnings to enhance human/machine interactions. Unfortunately, cybercriminals will deploy the same type of software.

Productivity vs. Safety

Organisations that adopt effective new technologies and working practices will edge ahead. We've already seen a move to agile thinking, remote working and shared digital workspaces. Expect AI to augment software engineering as it learns and improves. AI also plays a major role in operations automation and human decision-making. IoT and IIoT provide the glue between the physical and digital worlds. All these changes bring serious security questions in their wake.

Opportunities

Providing your organisation's risk appetite and security program embraces your chosen new processes and technologies, it will give you the confidence to be bold while gaining competitive advantage.

- Identify the business opportunities presented by emerging technologies
- Add security strategies as appropriate
- Be proactive. Seize the opportunities. Move forward with confidence.

Afterword

We hope you find this THIN**GUIDE** to Securing Australian Critical Infrastructure informative, and it provides a handy framework and playbook for your business. You will have noticed the emphasis has been put on cyber security and that we, the Australian Information Security Association (AISA) have endorsed this guide.

At AISA we understand that securing critical infrastructure is bigger than just cyber security or information security and support CGI's recommendations. Cyber security is a challenge that we as a business community are facing collectively and we must help each other navigate by sharing experiences and best practice solutions.

Damien Manuel,
Chair, Australian Information Security Association

AISA Australian Information Security Association

For more information please visit
www.aisa.org.au

You may also like to read CGI's Guide to Cyber Security for Business at
bit.ly/CGI-CS2

CGI

THIN **GUIDE**

endorsed by: