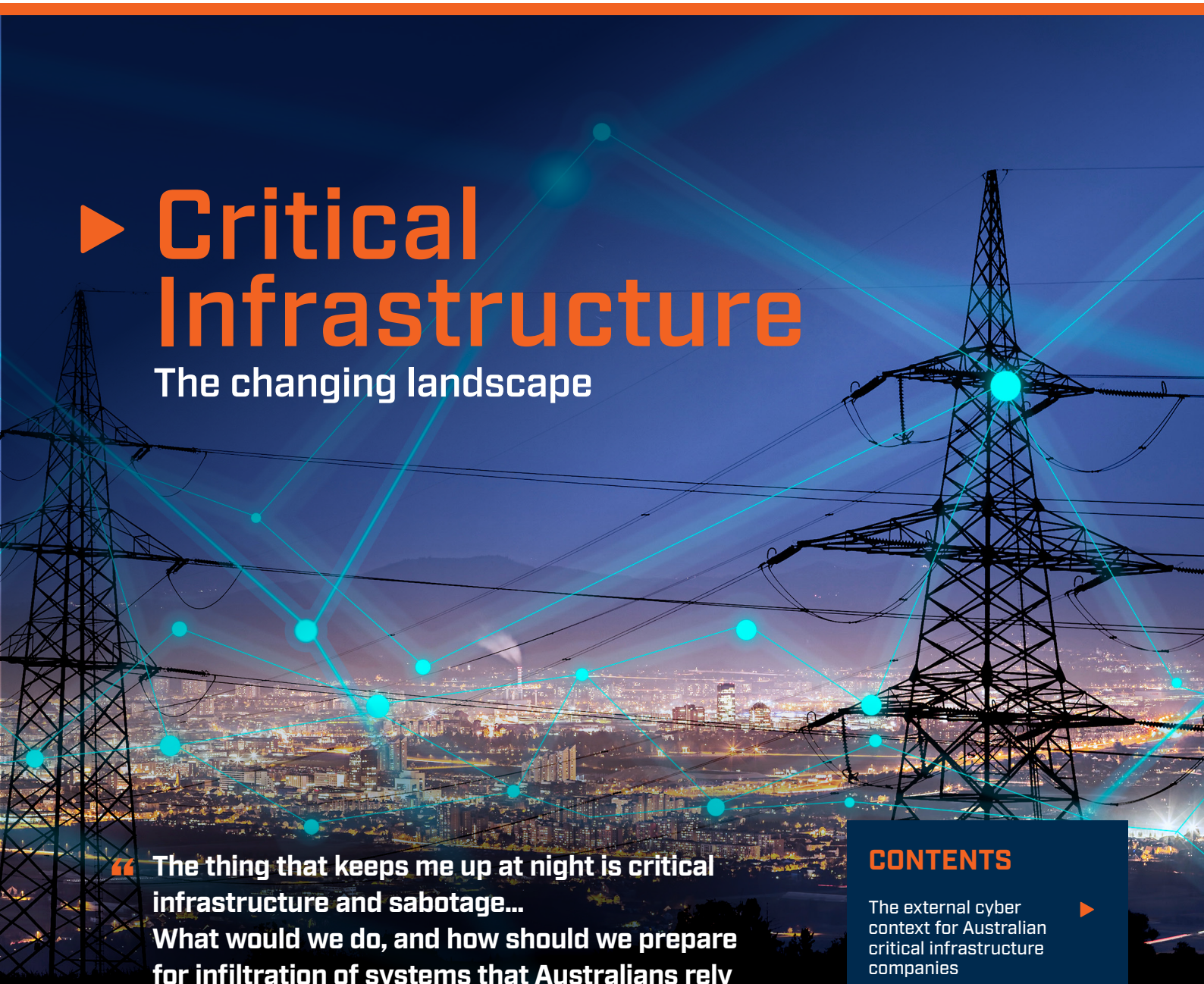
Huntsman®
Defence-Grade Cyber Security

FOR CRITICAL INFRASTRUCTURE

- Risk & Audit Team
- Executive Team
- Directors

Critical Infrastructure

The changing landscape



> "The thing that keeps me up at night is critical infrastructure and sabotage...
> What would we do, and how should we prepare for infiltration of systems that Australians rely on just to survive?
> How are we going to make sure that those systems are resilient and that, if they do come under cyberattack, we are able to repair and restore very quickly?"

Home Affairs Minister, Feb 2024

CONTENTS

The external cyber context for Australian critical infrastructure companies

Chillingly the quote on the previous page was made by Australia's Minister for Cyber Security. Allaying these fears is not the work of a moment. The remarks follow the expansion of critical infrastructure industry groupings, the commencement of the SOCI Act with its positive security obligations for those affected, and the ongoing enhancement of Critical Infrastructure Risk Management Planning and reporting responsibilities.

No doubt continuous improvement motivates your organisation, and the new perspectives on cyber and operational risk management are part of your strategic objectives – requiring an ever-evolving posture to deal with changing risks and the environment.

The threat landscape remains complex and volatile, especially as our use of technology expands. Security gaps begin to emerge in our operational systems and processes and the internet of things (IoT) continues to exacerbate the scope of the challenge. This and the connectedness of our economic and social activity has meant that global collectives from regulators to industry bodies are identifying frameworks and knowledge-bases to share resources and best practice guidance. For all cyber security stakeholders, forewarned is forearmed.

The MITRE ATT&CK® framework, for example, is a valuable global security resource that is regularly updated to forewarn security teams about a significant number of current potential cyber threats and how they might impact their businesses. With this knowledge, security teams can then increase their vigilance, to better manage the risks associated with each detected attack type.

Closer to home, the Australian Cyber Security Centre's (ACSC) Essential Eight (E8) Maturity Model combines eight crucial cyber security risk mitigation strategies to protect and measure the resilience and hence cyber maturity of an organisation. The controls include: • application control • patch applications • restrict Microsoft Office macros • user application hardening • restrict administrative privileges • patch operating systems • multi-factor authentication • regular backups.

With a preventative E8 security framework to measure the effectiveness of security controls, in combination with tools like the MITRE ATT&CK® matrix to reliably inform threat detection efforts, organisations can actively improve their cyber security risk management capabilities. This applies particularly to Critical Infrastructure organisations where compliance against cyber risk management frameworks can inform their cyber readiness.

The following diagram is designed to highlight the defence responses that your organisation should have in place to effectively intervene in a developing attack which, as can be seen, comprises multiple offensive activities. The diagram highlights the defensive efforts a cyber security team undertakes to counter each stage of a potential attack. It points to the importance of Attack Readiness to lessen the likelihood of a successful attack and an inventory of the current state of security control effectiveness. Importantly, this will better inform and guide any Response and Recovery efforts should they be required.

CRITICAL INFRASTRUCTURE INDUSTRY GROUPINGS

- **Communications**
- **Financial services and markets**
- **Data storage & processing**
- **Defence**
- **Higher education and research**
- **Energy**
- **Food and grocery**
- **Healthcare and medical**
- **Space technology**
- **Transport**
- **Water and sewerage**

CYBER SECURITY MARKERS

The key defence stages and points where Boards, Executive Management, Security and Risk Teams need visibility

READINESS | **RESPONSE & RECOVERY**

DETECTION

Defence Lifecycle

1 PREVENTION

Offence Lifecycle: Resource Development, Initial Access, Execution, Persistence

2 CONTAINMENT

3 RESPONSE

Offence Lifecycle: Privileged Escalation, Defence Evasion, Credential Access, Discovery, Lateral Movement

Offence Lifecycle: Collection, Command & Control, Exfiltration, Impact

4 RECOVERY

Offence Lifecycle: Reinstatement of operations (after an incident)

Cyber Report Visibility

	PREVENTION	CONTAINMENT	RESPONSE	RECOVERY
Board	**Monthly** Cyber Security Control Maturity	**Weekly/On-demand** Cyber Security Control Maturity Risk Escalation Report Incident Summary	**Weekly/On-demand** Cyber Security Control Maturity Computer Security Incident Response Team (CSIRT) Progress report Regulatory reporting assessment	**Monthly** Cyber Security Control Maturity CSIRT Report + Report for the regulator (if req.) Post Incident Review and Report Strategic & Governance Review
Executive Management	**Weekly/Monthly** Cyber Security Control Maturity	**Daily/Weekly/On-demand** Cyber Security Control Maturity Ongoing Incident Report	**Weekly/On-demand** Cyber Security Control Maturity CSIRT Progress report Disaster Recovery Plan (DRP) Implications report	**Monthly/On-demand** Cyber Security Control Maturity CSIRT Report + DRP Report Post Incident Analysis
Security/ Risk Teams	**Monthly** Cyber Security Control Maturity	**Daily/Weekly/On-demand** Cyber Security Control Maturity Regular Cyber-Risk Management Report	**Daily/Weekly/On-demand** Cyber Security Control Maturity Situational Awareness Report CSIRT Progress report DRP Implications report	**Monthly/On-demand** Cyber Security Control Maturity Post Incident Analysis & Report Performance Improvement Feedback

Software

Essential 8 Auditor OR **SmartCheck** + **Essential 8 Scorecard**

Enterprise SIEM OR **MSSP SIEM** + **Essential 8 Scorecard**

Huntsman®

If your concerns mirror those of the Minister, the onus is on Critical Infrastructure organisations and their leadership to expand their cyber security risk management to include early stage thinking. This preparation should include the maintenance of Cyber Risk Readiness activities as a key part of your broader Critical Infrastructure Risk Management Plans.

Cyber-attack readiness and having a true measure of your cyber resilience status

As directors and executive leaders continue to integrate cyber governance into their corporate governance and risk-management practices, we are often asked about how best to achieve these objectives given time pressures and skills shortages in the ever-changing cyber threat environment.

Like any organisational change, it is important to plan. You need to baseline your current situation and plan your objectives. As you integrate readiness into your cyber security strategy, you need confidence in the quality and reliability of the security information that is informing your decisions and the ultimate outcome. An evidence-based line of sight to your security controls, their effectiveness in mitigating any security gaps, and your resulting level of cyber resilience, will give you confidence about the state of your operational, reputational, and regulatory risks.

If you have invested in extensive digital transformation over the past few years, or are navigating the integration of generative AI tools into your business processes, the preparation, testing, and measurement of the effectiveness of your cyber risk controls has never been more important. Having an informed understanding of your readiness for a cyber security incident, and how it will be addressed, is the first step in managing your security objectives and outcomes.

> "**Critical Infrastructure:** those physical facilities, systems, assets, supply chains, information technologies and communication networks which, if destroyed, degraded compromised or rendered unavailable for an extended period, would **significantly** impact the social or economic wellbeing of Australia as a nation..., or affect Australia's ability to conduct national defence and ensure national security."
>
> Source: 2023 Critical Infrastructure Resilience Strategy

Snapshot: Cyber-Physical Systems and IoT across our Critical Infrastructure

Guarding your Cyber-Physical Systems (CPSs) requires a thorough understanding, by your Leadership Team and Directors, of the assets you hold, their vulnerability and riskiness at any point in time. Equally important are the mechanisms in place to protect these CPSs and how your incident management plans are regularly tested within your Business Continuity Plans.

The on-going adoption of technology to support business processes and efficiencies is increasing the attack surface and so too, the vulnerability of every organisation to potential attack. Maintaining the resilience of your enterprise and its operations in such a volatile threat environment is increasingly a team effort.

If you're surprised by the expansion in the number of Critical Infrastructure industries, it is worth considering a seemingly mundane example. John Deere is a traditional farming machinery company, and an increasingly significant player in food production, globally. The introduction of **cloud-based farm management systems** and other technical innovations is turning the organisation and its machinery into multi-point food-supply chain participants.

AI sensors on their machinery, a recent partnership with Starlink to build satellite-informed farm equipment, and their transition to an ag-tech behemoth introduces systemic risk to agrarian pursuits. Historical weather-related risks have now expanded beyond impacts on crops and livestock to the ability to operate digitised machinery, as seen when the Solar Storms of May 2024 **globally disrupted GPS-operated farming equipment**, interrupting vital systems and services in the critical food sector.

GUARDING YOUR CYBER-PHYSICAL SYSTEMS requires a true understanding within your Risk Teams, Executive, and Board, of:

- **The assets you hold**
- **The assets most at risk**
- **The mechanisms in place that are guarding these CPSs**
- **Ensuring your Business Continuity Plans evolve as the assets expand or contract**

Huntsman®

The SOCI Act, your CIRMP, and the looming deadline for specific critical infrastructure entities

The latest Security of Critical Infrastructure Act (SOCI Act) consultation closed on March 1st, 2024, with internal security and ICT teams now striving to report the status of their Critical Infrastructure Risk Management Program(s) (CIRMP) before the September 2024 deadline.

Short incident impact reporting time frames and annual CIRMP status reports are all part of the positive cyber security obligations Critical Infrastructure owners and operators are obliged to meet under this latest phase of the SOCI Act.

A regulator, the Cyber and Infrastructure Security Centre (CISC), has recently been established to supervise industry compliance. And while not intended as a major disruptor to business-as-usual activities, organisations that lack the staff and technical resources needed to improve their visibility and automate reporting, may find these new positive security obligations an added oversight burden. For those seeking more details about their CIRMP compliance obligations and guidance for the 2023/24 report, **see here**.

One of the fundamental additions to be included as part of the annual report is the selection of one (or more) of five designated cyber security frameworks. The risk management methods of the other CIRMP hazards to be reported on are not as specifically prescribed; although there is more than a passing similarity with operational risk management principles likely to impact some sectors in the near future.

Apparently, a recent **trial audit** by the regulator identified that a number of responsible entities still need to formalise their CIRMP reporting practices. The regulator notes that this might be acceptable in August 2024 but going forward, CIRMP compliance will increasingly become part of the corporate governance process. The interdependence across many of the risk hazards in the CIRMP will require that organisations develop more integrated systems and processes to manage their CIRMP compliance. Cyber security, risk and operational stakeholders will need to collaborate more closely so that CIRMP reports truly reflect the cyber maturity and overall operational resilience of the organisation.

Your board will have its first report to endorse before the 28th of September 2024 but following that, your annual requirement for continued risk management reporting must become a systematic part of BAU.

Although daunting when faced with limited people resources and an external skills shortage, the implementation of a cyber security framework and a CIRMP more generally is an important step for the critical infrastructure sector in lifting cyber security readiness. Maintaining the effectiveness of your cyber security and other hazard control efforts will help limit the risk of cyber-attacks, and mitigate any emerging threats that threaten to adversely impact business operations. At a cyber summit last year, the Minister for Home Affairs stated, "We know we cannot stop these cyber-attacks; what we can do is prepare for them so that when they occur we can bounce back better."

"Short incident impact reporting time frames and annual CIRMP status reports are all part of the positive cyber security obligations Critical Infrastructure owners and operators are obliged to meet under this latest phase of the SOCI Act"

So, how do you **measure the success of your CIRMP**, and are you **seeing other outputs** on a monthly basis at a leadership level, **that demonstrate effective cyber risk controls and cyber maturity?**

The security frameworks are of varying levels of complexity. One however – the ACSC's Essential Eight Maturity Model – embraces the common technical controls and is straightforward to deploy and manage.

Next steps

Regardless of whether your organisation is categorised as Critical Infrastructure under the SOCI Act, or you are third party supplier to a Critical Infrastructure provider, the provisions of the SOCI CIRMP will impact you. Make sure as part of your cyber security strategy that you have the latest Defence Stages in place to successfully manage contemporary cyber threat lifecycles and guard your 'crown jewels' and the risks that your suppliers might bring.

If, as a senior leader in your organisation you are not seeing appropriate levels of cyber risk reporting, and don't have certainty around what is in place to defend your organisation, consider Huntsman Security solutions to inform your cyber risk management and reporting obligations.