THE IMPACT OF AUSTRALIA'S SOCI ACT ON CYBER RESILIENCE

Security of Critical Infrastructure Act (SOCI) 2018

Honeywell

TABLE OF CONTENTS

SECURITY OF CRITICAL INFRASTRUCTURE

(SOCI) 2018

The Australian government has enacted legislation to help enhance cybersecurity by introducing systems to help mitigate and manage risks associated with people, processes and technology within vital infrastructure facilities, reducing potential damage and disruption.

LEGISLATIVE REQUIREMENTS

2018 SOCI LEGISLATION

OBJECTIVE

The framework for managing risks related to critical infrastructure includes several key components:

- Enhancing transparency around the ownership and operational control of critical infrastructure in Australia to better comprehend associated risks.
- Promoting cooperation and collaboration among all levels of government, regulators, and the owners and operators of critical infrastructure to identify and manage these risks
- Mandating that responsible entities for critical infrastructure assets recognize and address risks related to those assets
- Introducing heightened cybersecurity obligations for entities managing systems of national significance to boost their readiness and response capabilities regarding cybersecurity incidents.
- Establishing a regime for the Commonwealth to address severe cybersecurity incidents.

THE RISKS

A cybersecurity incident could significantly impact the availability of operational technology (OT) and critical control systems. This directly affects the safe and reliable operation of critical infrastructure assets, putting Australia's essential supply chain of services at risk.

Given the potential legal ramifications and the risk of greater physical, financial, and reputational damage, it is crucial to immediately focus on oversight and investment in cybersecurity, including OT cybersecurity.

Board Obligations: For all boards, cybersecurity and cyber resilience must be top priorities. If boards do not give cybersecurity and cyber resilience sufficient attention, it can create a foreseeable risk of harm to the company and expose directors to potential enforcement action by various government departments and agencies.

Fines/Penalties: In December 2022, responding to several significant cybersecurity and data breaches, the Australian government passed legislation to increase civil penalties. The highest penalties for non-compliance can be significant.. Further changes are under consideration, and the industry must be ready to respond

Reputational Damage: If attacks occur, a company's reputation can be difficult to repair. The impact can potentially extend to a drop in share price over one year or more and instill doubt among customers. Studies show that the average cost of a cyber incident is $100,000 USD per day.

SOCI REFORMS 2021, 2022 AND 2024

(SOCI) 2018

The Australian government has passed the following reforms to the initial 2018 legislation: the Security Legislation Amendment (Critical Infrastructure) Act 2021 (SLACI Act),the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (SLACIP Act) and the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024. These amendments now form part of the 2018 Act.

LEGISLATIVE REQUIREMENTS

2021/2022 SOCI PART 2/PART 2B

11 Sectors | 22 Asset Classes

See page 5 for full list of applicable sectors and asset classes.

OBLIGATIONS

Reporting critical cybersecurity incidents

If you are a responsible entity for a critical infrastructure asset and you become aware that a critical cybersecurity incident has occurred, or is occurring, and the incident has had, or is having, a significant impact on the availability of your asset, you must notify the Australian Cyber Security Centre (ACSC) within 12 hours after you become aware of the incident. If you make the report verbally, you must make a written record through the ACSC's website within 84 hours of verbally notifying the ACSC.

Reporting other cybersecurity incidents

If you are a responsible entity for a critical infrastructure asset and you become aware that a cybersecurity incident has occurred, is occurring, or is imminent, and the incident has had, is having, or is likely to have, a relevant impact on your asset you must notify the ACSC within 72 hours after you become aware of the incident. If you make the report verbally, you must make a written record through the ACSC website within 48 hours of verbally notifying the ACSC.

> **HOW DO YOU IDENTIFY AN ACTIVE OT CYBER THREAT AND DIFFERENTIATE FROM A TRADITIONAL EQUIPMENT FAILURE?**

SOCI MANDATES

The Security of Critical Infrastructure Act (SOCI) in Australia imposes several requirements on certain organizations to help protect national infrastructure.

KEY SOCI REQUIRMENTS	
Risk Management Program	• Develop and maintain a comprehensive risk management program that identifies and mitigates risks to critical infrastructure assets • Regularly review and update the risk management program to address evolving threats
Critical Infrastructure Asset Register	• Report and maintain an accurate register of critical infrastructure assets • Ensure that the register is up to date with details about ownership, control, and operational information
Mandatory Reporting Obligations	• Report cyber incidents and other security breaches to relevant government authorities within specified timeframes • Provide detailed information about the nature and impact of the incident, as well as the response measures taken
Government Assistance Measures	• Comply with directions and requests from government authorities during significant security incidents • Facilitate government intervention if necessary to manage and mitigate threats to critical infrastructure
Positive Security Obligations (PSOs)	• Implement and maintain security measures to protect critical infrastructure assets from cyber threats, physical attacks, and other security risks • Adhere to sector-specific security guidelines and standards issued by government authorities
Enhanced Cyber Security Obligations (ESCOs)	• For nationally significant entities, develop incident response plans, participate in cybersecurity exercises and undergo regular assessments
Compliance and Enforcement	• Undergo regular audits and assessments to ensure compliance with SOCI Act requirements • Address any non-compliance issues identified by regulatory authorities in a timely manner
Information Sharing and Collaboration	• Participate in information-sharing initiatives with government agencies and other critical infrastructure sectors • Collaborate with industry partners and stakeholders to enhance collective security and resilience

ROLES IN SOCI	
Board of Directors	Ultimate accountability and governance oversight
Chief Information Security Officer (CISO)	Accountable for implementing security measures and incident response
Risk Management and Compliance Officers	Responsible for the management of the Critical Infrastructure Risk Management Program (CIRMP)
CEO and Senior Management	Strategic direction and operational oversight
IT and OT Teams	Technical implementation and system monitoring

THE HONEYWELL SOLUTION

Honeywell's OT Cybersecurity Platform, comprising Cyber Insights and Cyber Watch, revolutionizes operational technology (OT) cybersecurity. Cyber Insights transforms OT cybersecurity, offering profound insights into a company's cybersecurity posture, asset detection and threat analytics, bolstering defences at a single-site manufacturing facility.

Cyber Watch, a milestone innovation, provides an enterprise-wide view through a centralized dashboard for near real- time monitoring and executive-level response coordination. The Governance Portal empowers the CISO to help ensure compliance with standards like SOCI, IEC 62443, NIS 2 and NERC CIP, meeting cybersecurity benchmarks.

Seamlessly integrated, these solutions are designed to offer trusted insights and risk management in a unified suite, transforming OT cybersecurity into a proactive, strategic asset.

HONEYWELL CYBER INSIGHTS AND CYBER WATCH
Revolutionizes Operational Technology (OT) Cybersecurity

Near real-time device discovery

Near real-time threat monitoring

Remote cyber and OT alarms

Compliance portal IEC / NIST

CRITICAL INFRASTRUCTURE RISK MANAGEMENT PROGRAM (CIRMP)

Part 2A of the SOCI Act (risk management program PSO) applies to 13 critical infrastructure asset classes.

LEGISLATIVE REQUIREMENTS

2023 SOCI PART 2A

*8 Sectors | 13 Asset Classes**

See page 5 for full list of applicable sectors and asset classes.

CRITICAL DATES

Within 6 months of an asset becoming a CI asset, a responsible entity must establish and maintain a process or system in the CIRMP to comply with *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023. 4*

OBJECTIVE

Cyber and information security hazards

A responsible entity must establish and maintain a process or system in the CIRMP to—as far as it is reasonably practicable to do so:

- Minimise or eliminate any material risk of a cyber and information security hazard occurring; and
- Mitigate the relevant impact of a cyber and information security hazard on the CI asset
- Within 6 months of an asset becoming a CI asset a responsible entity must establish and maintain a process or system in the CIRMP to comply with a framework listed in section 8 of *the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* **i.e. ISO, IEC 62443, NIST, Essential 8 or equivalent.**

> **HOW DO YOU QUANTIFY RISKS ASSOCIATED WITH YOUR OT ENVIRONMENT AND PROVIDE CONFIDENCE OF COMPLIANCE TO YOUR BOARD?**

HONEYWELL'S SOLUTION PORTFOLIO

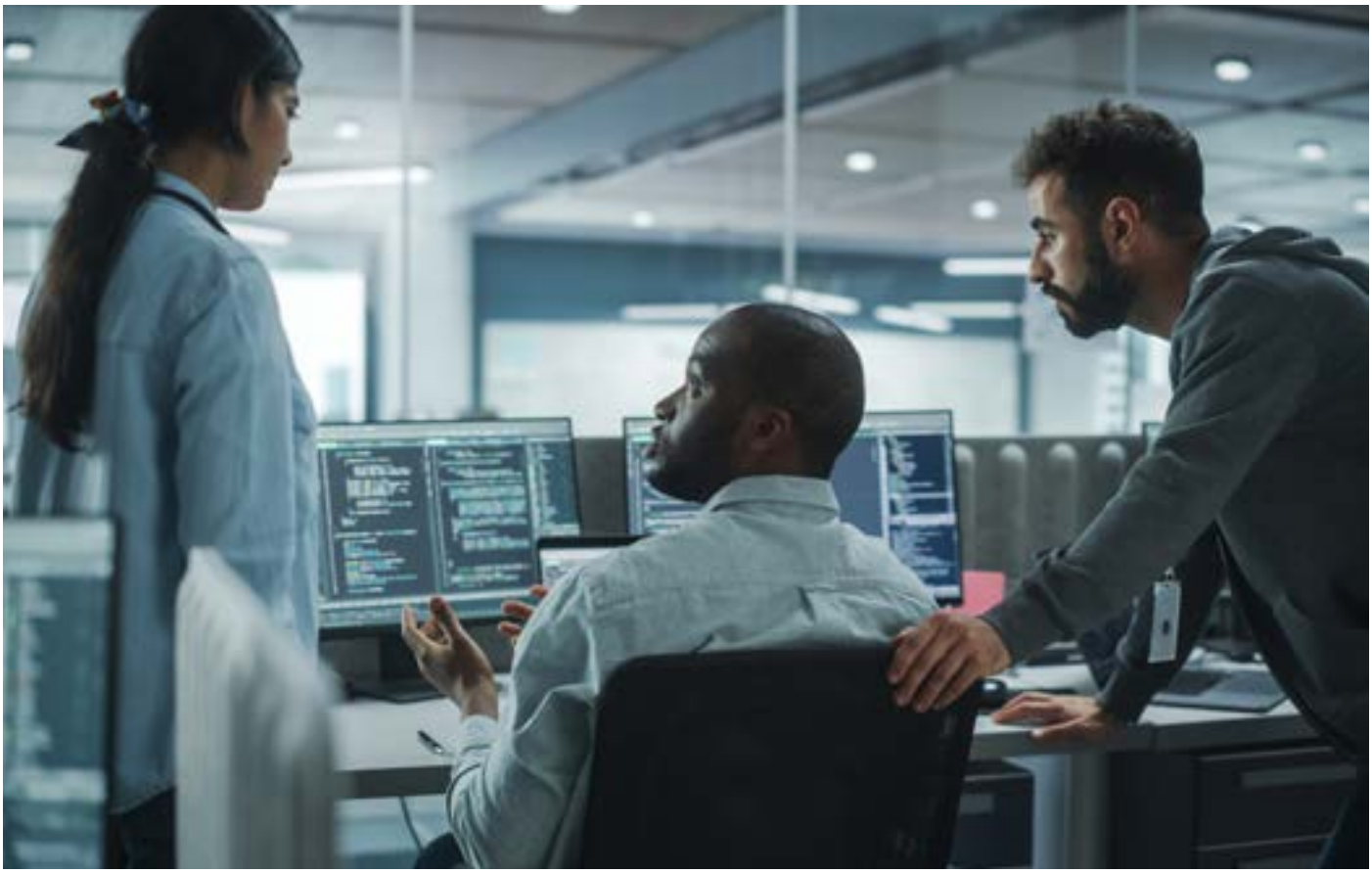
Honeywell's proven OT cybersecurity solutions offer advanced products and services designed to help identify and mitigate OT cybersecurity risks. Tailored to any maturity level, our solutions include cyber assessments, penetration testing, vulnerability studies and Cyber Insights for posture analysis. Cyber Watch provides near real-time monitoring, and the Governance Portal ensures compliance with IEC 62443, NERC CIP, NIS 2, SOCI and OTCC. We also provide rapid incident response and training programmes. These integrated solutions transform OT cybersecurity into a proactive, strategic asset for industrial organizations.

HONEYWELL MANAGED OT CYBER SERVICES

Monitor for signs of a cybersecurity breach

Proactive vulnerability and threat detection

Current updates and rapid incident response



WITHIN 6 MONTHS OF BECOMING A CI ASSET: ESTABLISH AND MAINTAIN SYSTEMS TO COMPLY WITH APPLICABLE CYBERSECURITY FRAMEWORKS:

NIST (National Institute of Standards and Technology):	**ISO 27001** (International Standards Organization)	**AESCSF** (Australian Energy Sector Cyber Security Framework)	**ESSENTIAL EIGHT MATURITY MODEL** (Maturitylevel one)	**C2M2** (Cybersecurity Capability Maturity Model)
Framework Core: The core component of the NIST CSF outlines five key functions: Identify, Protect, Detect, Respond, and Recover, ensuring a holistic approach to cybersecurity	**Information Security Management:** ISO 27001 provides a systematic approach to managing sensitive company information, ensuring its confidentiality, integrity, and availability	**Focus:** Primarily focuses on cryptographic security, specifically centered around the implementation of the Advanced Encryption Standard (AES) for protecting data at rest and in transit	**Key Strategies:** The Essential Eight includes application whitelisting, patching applications, configuring Microsoft Office macros, restricting administrative privileges, and multi- factor authentication	**The Cybersecurity Capability Maturity Model (C2M2)** is a free tool to help organizations evaluate their cybersecurity capabilities and optimize security investments. It uses a set of industry-vetted cybersecurity practices focused on both information technology (IT) and operations technology (OT) assets and environments

ARE YOU SUBJECT TO SOCI REGULATIONS?

WE'RE HERE TO HELP! TAKE THESE STEPS AND CONTACT YOUR HONEYWELL ACCOUNT MANAGER TODAY.

IMMEDIATE RECTIFICATION

- Register assets promptly
- Notify authorities about delays and corrective actions

INTERNAL REVIEW

- Assess and improve compliance processes
- Consult legal and compliance expertsand corrective actions

PREVENTATIVE MEASURES

- Implement a compliance calendar, regular training, risk assessment actions and enhanced monitoring systems

THE FOLLOWING ARE DETAILS OF THE CRITICAL INFRASTRUCUTRE SECTORS AND CRITICAL INFRASTUCTURE ASSET CLASSES DEFINED IN THE SECURITY OF CRITICAL INFRASTRUCTURE ACT 2018 (SOCI)

SECTOR	ASSET CLASSES
Communications	Critical telecommunications asset Critical broadcasting asset ** Critical domain name system **
Data storage or processing	Data storage or processing **
Defence industry	Critical defence industry asset
Energy	Critical electricity asset ** Critical gas asset ** Critical energy market operator asset ** Critical liquid fuel asset **
Financial services and markets	Critical banking asset Critical superannuation asset Critical insurance asset Critical financial market infrastructure asset **
Food and grocery	Critical food and grocery asset **
Health care and medical	Critical hospital
Higher education and research	Critical education asset
Space technology	Space technology
Transport	Critical port Critical freight infrastructure asset ** Critical freight services asset ** Critical public transport asset Critical aviation asset
Water and sewage	Critical water asset **

** Asset classes required to follow CIRMP – critical infrastructure risk management programme

** Critical financial market infrastructure assets - Payment systems only required to follow CIRMP

HOW HONEYWELL CAN SUPPORT

Honeywell provides a spectrum of OT cybersecurity solutions, from helping improve OT cybersecurity defences with vendor-agnostic solutions designed to assist organizations in identifying, prioritizing and reducing OT cyber risks and potential vulnerabilities.

SCHEDULE YOUR SOCI CONSULTATION

For more information

To learn more about Honeywell OT Cybersecurity, contact your Honeywell Account Manager.

Honeywell Connected Enterprise
715 Peachtree Street NE
Atlanta, Georgia 30308

THE FUTURE IS WHAT WE MAKE IT

Honeywell