Spotlight on Australia's Security of Critical Infrastructure (SOCI) Act

May 20, 2021 08:08 BST

Spotlight on Australia's Security of Critical Infrastructure (SOCI) Act

Since April 2021, organisations operating in any of Australia's 11 critical infrastructure sectors are required to more significantly contribute to the Australian government's vision for a "more secure online world for Australians", where Critical Infrastructure Owners and potentially Directors risk fines of up to $44,400 or a prison sentence of up to two years for non-compliance.

Following the *Commonwealth Government of Australia's 2020 Cyber Security Strategy* to respond to the ever evolving threat to Australia's critical

infrastructure, the Department of Home Affairs introduced an updated Security of Critical Infrastructure (SOCI) Act that progress reforms to protect critical infrastructure and systems of national significance, and entered into force in April 2021.

As a result, organisations that supply food or groceries to critical supermarkets; are critical to the transport of goods by road, rail, river or sea; offer data processing services to government; are hospitals with an intensive care unit owners, or otherwise own or operate assets in one of the 11 designated critical infrastructure sectors (CIS) are now subject to:

- **Positive security obligations**, including risk management and mandatory cyber incident reporting,
- **Enhanced cyber security obligations**, such as exercises to build cyber preparedness and vulnerability assessments and remediation, and
- **Government assistance**, i.e. at the receiving end of information gathering, action and intervention directions by Ministers where an ongoing or imminent cyber incident puts Australian lives at risk.

What does this mean?

Practically, this means if you operate in any of the below sectors you need to act:

- Communications

- Data Storage and Processing
- Defence
- Financial Services and Markets
- Higher Education and Research
- Energy
- Food and Grocery
- Health care and Medical
- Space technology
- Transport
- Water and Sewerage

What are organisations expected to do?

You will have to take on additional responsibilities to:

- Identify current and previous cyber incidents, evaluate their impact and report

- Ensure that your risk management program is up to date and effective
- Have systems and procedures in place to prepare and deliver annual reports
- Prepare to participate in supervised cyber security exercises
- Prepare to participate in supervised vulnerability assessments
- Comply with ownership and operations reporting responsibilities

What steps should organisations take now?

The multitude of obligations across different pieces of legislation can often seem overwhelming, particularly when organisations lack the financial, human and availability resources or a structured approach to plan their response.

Outsourcing these resources is an option for organisations who need help assessing, managing and developing their cyber resilience posture. It is important that you work with somebody who understands your business concerns and aims to help you protect your software and personal data and ensure it's safe and secure.

Where organisations believe government assistance would be insufficient to meet their obligations, they should consider reaching out to a cyber security organisation who has international reach to assist with ensuring their organisation is meeting regulatory obligations.

Key takeaways:

- Through the Security of Critical Infrastructure (SOCI) Act, the Australian government is driving Critical Infrastructure Sectors to improve cyber resilience.

- Better cyber risk management and incident response capabilities are needed to enable organisations to react swiftly and consistently to cyber-attacks.

- Organisations across any of Australia's 11 critical infrastructure sectors need to act now to ensure compliance to the Act, or face penalties.

Shutterstock ID: 1458781236

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970