SPOTLIGHT ON AUSTRALIA'S CYBER SECURITY ACT 2024

Reviewing the Reporting Obligations under the Cyber Security Act 2024

A Spotlight on Mandatory Incident Reporting and Ransomware Reporting Guidance

StratisAdvisory

RISK | STRATEGY | CYBER COMPLIANCE MANAGEMENT

Cyber Security Act Overview

The Cyber Security Act 2024 officially became law on November 2024 applicable to Smart Devices or relevant connectable products, acquired in Australia, that can connect (directly or indirectly) to the internet or a network. The Act extends to every Territory outside Australia.

Cyber Security Act Objectives

- Mandatory minimum cybersecurity standards for smart devices.
- A "Limited Use" obligation for the National Cyber Security Coordinator to foster industry engagement with the government after cyber incidents.
- Establish the Cyber Incident Review Board (CIRB) to review major cyber incidents and advise on response and impact reduction.
- Mandatory reporting for certain businesses to disclose ransomware and cyber extortion payments.
- Encourage cyber incident reporting to the AU Government with protections on use and liability.
- Support consent-based, limited-purpose sharing of cyber incident data with State and Territory Governments (not admissible evidence).

Commencement Timeline

30 November 2024

Part 1: Preliminary, Objectives and Definitions

Part 4: Coordination of Significant Cyber Security Incidents

Part 6 and 7: Regulatory Powers and Miscellaneous

29 May 2025

Part 3: Ransomware Reporting Obligations

Part 5: Cyber Incident Review Board

***12 months after enacted into law**

Part 2: Security Standards for Smart Devices

Cyber Security Act Security Standards

Part 2: Security Standards for Smart Devices

- Manufacturers must produce devices in compliance with prescribed standards.
- Suppliers must comply with other obligations e.g. provide information with each product.
- Non-compliance with security standards must not be supplied in AU.
- Products supplied in AU must have a statement of compliance; a copy is retained for a specified period.

Applies to products ***manufactured or supplied*** after this Part commences. Non-compliance may trigger compliance, stop or recall notices. Some products or classes may be exempt under these rules.

Part 2 Division 3: Enforcement Mechanisms

The Secretary of the relevant Department is empowered to:

- Issue a Compliance Notice if an entity isn't meeting obligations.
- Escalate to a Stop Notice if compliance is not achieved.
- Issue a Recall Notice for persistent non-compliance.
- Publicly notify failures to comply with recall notices.

Entities have the right to:

- Internal review of enforcement decisions.
- Undergo independent audits.

Part 3: Ransomware Reporting

- Entities with an annual turnover of A$3 million (or certain responsible entities for critical infrastructure) must report ransomware payments within 72 hours to a designated Commonwealth body.
- Reports must contain detailed incident, demand, and payment information.
- Non-compliance attracts civil penalties (60 penalty units).

Part 4 Division 2: Voluntary Information Sharing

- Entities may provide details of significant cyber security incidents to the National Cyber Security Coordinator.
- Shared information enjoys protection: However, it is inadmissible against the reporting entity and may not be used for civil or regulatory enforcement.

Part 5: CIRB

Australian Government
Department of Home Affairs

- Conducts incident reviews and publishes public and protected reports.
- May ask or require entities to provide relevant documents.
- Recommendations are non-punitive but guide future resilience strategies.

Obligations of Reporting Entities

Term	Definition and Obligation
Smart Devices or relevant connectable products	Internet or network-connectable products intended for personal, domestic, or household use, e.g. Smart TV and watches, Home assistants, etc.
Significant Cyber Security Incident	An incident that materially risks AU's social/economic stability, national security, or is of serious concern to the public.
Smart Device Manufacturers and Suppliers	Must comply with mandatory security standards and provide compliance statements.
Reporting Entity	A business operating in the AU with annual turnover that exceeds the current turnover threshold must report ransomware payments within 72 hours via Australian Signals Directorate (ASD's) ReportCyber portal.
National Cyber Security Coordinator (NCSC)	Coordinates responses to significant incidents; receives voluntary reports.

- **Regulatory Compliance:** Entities must align cyber policies, contracts, and product documentation with new standards.
- **Incident Transparency:** Mandatory reporting increases visibility into ransomware threats and discourages payments.
- **Legal Protections:** "Limited use" provisions protect entities from enforcement actions based on shared incident data.
- **Market Accountability:** Public notices for non-compliance may affect consumer trust and brand reputation.
- **Cross-Sector Collaboration:** CIRB and NCSC foster industry-government cooperation for systemic resilience.

Discover what Stratis Advisory can do for you

Cybersecurity Program

Information systems documentation is typically disparate, involves multiple inputs from various third-party vendors performing a specific function, technically focused vs. operational execution, and fragmented without identified ownership across various functions. Stratis can consolidate your information systems and support your chief information security officer (CISO) with developing and maintaining a sustainable risk-based enterprise-wide cybersecurity program.

Cybersecurity Risk Assessment

Beyond Service and Organization Controls (SOC) audit(s), penetration testing, and PCI Security Standard assessments, dedicated risk assessments help you understand the inherent risks in information technology systems, processes, and programs. Stratis can execute your cybersecurity risk assessment to identify broader risk identification and control mitigation across key information systems.

Outsourced Regulatory Monitoring Program

Operating domestically or globally, industry guidance and laws and regulations are evolving and expanding, specifically those on beneficial ownership reporting, data privacy and breach reporting, cybersecurity program implementation, and third-party risk management. Stratis can develop and execute a customized outsourced regulatory monitoring program based on your operating model, markets, customers, and risk tolerance to proactively address relevant changes that impact your business.

Stratis Advisory | 1.415.352.1060 | www.stratisadvisory.com | info@stratisadvisory.com