

Cyber Security Act 2024: Legislative Updates and What You Need to Know - blueAPACHE

Canonical: <https://www.blueapache.com/blog/cyber-security-act-updates>

Details:

2025

Australia's Notifiable Data Breaches scheme, in place since February 2018, requires covered organisations and agencies to notify the OAIC and affected individuals of eligible breaches likely to cause serious harm. It does not require notification of every incident involving personal information. In November 2023 the Cyber Security Legislative Package was formed. The 2023-2030 Australian Cyber Security Strategy is the roadmap to realise the Australian Government's vision of becoming world leader in cyber security by 2030. As part of this strategy, on the 29 November 2024, the Cyber Security Act 2024 received Royal Assent and became Law.

What You Need to Know

Security Standards for Smart Devices: The Act establishes a framework for mandatory standards for relevant connectable products, with manufacturer and supplier duties and statements of compliance. Check the applicable rules, covered product categories and commencement arrangements; the framework should not be read as an identical obligation for every smart device.

The regulator may then conduct testing to verify the statement of compliance and if there is a failure to comply the regulator may publish a notice in the public domain which could cause reputational damage.

Mandatory Ransomware Payment Reporting: Part 3 applies where the statutory incident, demand and payment conditions are met. Reporting business entities include relevant businesses operating in Australia above the prescribed annual-turnover threshold, and responsible entities for critical infrastructure assets covered by Part 2B of the Security of Critical Infrastructure Act. The rules prescribe a \$3 million threshold, with a calculation for a business carried on for only part of the previous financial year.

The reporting business entity must report within 72 hours of making the payment or becoming aware that another entity made it on its behalf, as applicable. A third-party incident does not by itself impose this payment-reporting duty on every payer. See sections 26–27 of the Act and Home Affairs reporting guidance.

Limited Use for the National Cyber Security Coordinator: Part 4 restricts the purposes for which protected incident information may be used or disclosed. Permitted incident-response uses, exceptions and evidence-admissibility rules apply. These protections are not blanket secrecy or immunity from investigation; refer to sections 38–42 of the Act for the relevant conditions.

Cyber Incident Review Board: The establishment of an Independent Statutory Advisory Body that will conduct no-fault, post-incident reviews of significant cyber security incidents in Australia to make recommendations to the government on actions to prevent, detect, respond to or minimise the impact of similar cyber security incidents in the future.

How to Protect Your Organisation

Regular Cyber Risk Assessments: Identify vulnerabilities through comprehensive assessments to stay ahead of potential threats and ensure mitigation strategies are up to date.

Strong Incident Response Plans: A clear, tested incident response strategy can turn a potential crisis into a manageable situation, reducing both impact and cost.

Keep Software and Systems Updated: Regularly update all software and systems to protect against known vulnerabilities. This includes applying patches and updates as soon as they are available.

Threat Intelligence: Ensure the collection, analysis, and application of information about potential and existing cyber threats. This helps organisations anticipate, detect, and respond to cyber threats more effectively.

****Understand your 3rd party – and Supply Chain Risks: ****Third-party relationships may provide threat actors with an easier pathway into an organisation's systems and networks. Vetting those supply chain partner's cyber security resiliency and capability, including through their assurance of identity and access management, governance and risk management, and information asset management, will help understand any partner / supplier weaknesses and potential risk vectors.

What Happens If You Don't Act

Failing to meet legislated expectations can expose your organisation to regulatory and legal risks, with potential fines and severe reputational damage. Customers and stakeholders expect robust data protection, and any failure in this area can significantly tarnish your brand's credibility. It is important to recognise that any information contained in this document, or the links shared are general in nature and does not constitute legal advice. Readers are encouraged to obtain legal advice that applies to their particular circumstances.

How we can Support You

At blueAPACHE, we support our clients by helping to build a robust risk management framework which addresses their security risks and supports controls to protect their key assets, thereby enhancing their cyber resilience. We help our clients with scenario-based simulations to assess response processes and recovery with gaps identified for improvement and remediation. Our published ISO/IEC 27001 certification relates to the information security management system within its certified scope. It is not certification of every emPOWER product, a guarantee of the highest security standard, or proof of a customer's compliance. Our vCISO (Virtual Chief Information Security Officer) capability provides a cost-effective, strategic oversight tailored to your organisation's needs. This service supports governance and risk planning; compliance depends on the obligations and controls that apply to your organisation. For further assistance or to discuss your cybersecurity needs, please reach out to us here .

When did the Cyber Security Act 2024 receive Royal Assent and become law in Australia?

The Cyber Security Act 2024 received Royal Assent and became law on 29 November 2024, as part of the Cyber Security Legislative Package formed in November 2023.

What is the 2023-2030 Australian Cyber Security Strategy?

The 2023-2030 Australian Cyber Security Strategy is the roadmap to realise the Australian Government's vision of becoming a world leader in cyber security by 2030. The Cyber Security Act 2024 is part of this strategy.

What are the cyber security standards requirements for smart devices under the Cyber Security Act 2024?

The Act establishes a framework for mandatory standards for relevant connectable products, including manufacturer and supplier duties and statements of compliance. Product coverage and commencement depend on the applicable rules; check those requirements for the product concerned.

What are the mandatory ransomware payment reporting requirements under the Cyber Security Act 2024?

Where Part 3's incident, demand and payment conditions apply, a reporting business entity must report within 72 hours of making a ransomware payment or becoming aware of a payment made on its behalf. Covered entities include relevant Australian businesses above the prescribed turnover threshold and specified critical-infrastructure responsible entities. The rules prescribe \$3 million, with a part-year calculation. Sections 26–27 govern the scope and trigger.

What is the 'limited use' obligation for the National Cyber Security Coordinator under the Cyber Security Act 2024?

Part 4 limits the purposes for which protected incident information may be used or disclosed by the National Cyber Security Coordinator and other recipients. Incident-response uses, exceptions and admissibility protections apply under sections 38–42. It is not a blanket promise that information can never reach law enforcement or regulators.

What is the Cyber Incident Review Board established under the Cyber Security Act 2024?

The Cyber Incident Review Board is an Independent Statutory Advisory Body established to conduct no-fault, post-incident reviews of significant cyber security incidents in Australia. It makes recommendations to the government on actions to prevent, detect, respond to, or minimise the impact of similar cyber security incidents in the future.

What are the consequences of failing to meet the Cyber Security Act 2024's legislated expectations?

Failing to meet legislated expectations can expose an organisation to regulatory and legal risks, including potential fines and severe reputational damage, and can significantly tarnish a brand's credibility due to customer and stakeholder expectations of robust data protection.

How do you support clients in complying with the Cyber Security Act 2024?

We offer risk-management support, scenario-based exercises and vCISO services to help customers assess controls, response and governance. Our ISO/IEC 27001 certification concerns the certified management-system scope, not automatic compliance of every service or customer. Applicable obligations and agreed responsibilities need to be assessed for each organisation.

What data breach reporting scheme has been in place in Australia since before the Cyber Security Act 2024, and what does it require?

The Notifiable Data Breaches scheme has operated since February 2018. Covered organisations and agencies must notify the OAIC and affected individuals of eligible breaches likely to result in serious harm; not every personal-information incident is automatically notifiable.