ACSC Australian Cyber Security Centre

What you should do

Given the cyber threat landscape over the past year, the ACSC continues to recommend all Australian organisations prioritise implementation of the Essential Eight Maturity Model and, in particular, consider the following six actions:

Report all cybercrime and cyber security incidents, via ReportCyber. This is the central place to report a cyber security incident, cybercrime, or a cyber security vulnerability. The ACSC website (cyber.gov.au) provides extensive advice, guidance and information on a range of cyber security matters. The website also provides additional assistance and referral pathways depending on the nature of the incident or cybercrime. The ACSC encourages the reporting of cyber security matters to assist the ACSC in understanding the Australian cyber threat environment.

Become an ACSC Partner. Australian organisations who partner with the ACSC receive threat insights, advisories and advice to enhance their situational awareness. Cyber security professionals in our partner organisations also receive collaboration opportunities across industry and the Australian Government.

Know your networks. The ACSC encourages all users to understand and review their networks to establish where valuable or sensitive information and infrastructure is located, and apply appropriate cyber security measures proportionate to the risk of compromise.

Patch within 48 hours where an exploit exists. Malicious cyber actors monitor reporting of security vulnerabilities and use automated tools to regularly scan for and exploit network vulnerabilities. This means that organisations can no longer follow monthly patch update cycles, and should prioritise patching to protect their networks from cyber security incidents. Ensure patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Where this is not possible, it is important that organisations have robust cyber incident detection and response plans in place. For organisations that cannot patch their internet-facing services in a very timely manner, adopting trustworthy Software as a Service (SaaS) or Platform as a Service (PaaS) cloud approaches to internet-facing services, which immediately apply patches on the customer's behalf, may assist.

Evaluate risks associated with cyber supply chains. The ACSC encourages organisations to follow the ACSC's advice on cyber supply chain risk mitigation.

Prepare for a cyber security incident by having incident response, business continuity and disaster recovery plans in place, and testing them. An incident response plan enables organisations to respond decisively to a cyber security incident, limit its impact and support recovery. Testing the incident response, business continuity and disaster recovery plans, including through cyber security exercises involving restoration of systems, software and important data from backups, provides an opportunity to review and improve in a controlled environment.