

Cyber Security for Startups and Small Business



Why do cyber security now?

Your business operations will involve digital and/or internet connected tools and processes. It is critical that you protect your organisation and people from a cyber security breach, particularly when you have staff working remotely.

Managing your cyber risk can be challenging, but it is essential because it reduces costs and manages risk to reputation if you are compromised.

It is also now a legal requirement for businesses within critical infrastructure supply chains to establish, maintain, and comply with a risk management program, including cyber security obligations, through the [Security Legislation Amendment Act 2022](#).

Where to start?

- **Australian Government's Australian Cyber Security Centre:** Step-by-step Guides and where to report a cyber crime. www.cyber.gov.au/small-business
- **CyberCheck.me:** partnership between the WA AustCyber Innovation Hub and the ECU Security Research Institute (ECUSRI), provides comprehensive cyber guides. Selected councils also provide small businesses with access to a free one hour – 1 on 1 cyber security consultation. www.cybercheck.me

Securing your digital footprint

1. Have business continuity plans and incident response procedures written down and know who you'll switch to if your internet and/or cloud service provider experiences outages.
2. Turn on automatic updates for your operating system (e.g. Microsoft Windows) to ensure as much malicious software is blocked.
3. Ensure your business and all staff have updated the apps used by your business to the latest versions (should be done regularly).
4. Ensure you have a procedure in place for regular backups of data and systems and keep backups for 6 months.
5. Implement Multi Factor Authentication (MFA) as mandatory practice including, where possible, replacing the use of platforms/software that do not have an option for MFA.
6. Ensure your staff know how to keep your organisation cyber secure.

Enable your team to support the security of your organisation's digital footprint

- Ensure staff understand how to safely connect remotely to company infrastructure
 - Use a reputable VPN. Require staff to be using it whenever possible and keep it updated. It should be used at home and in all public places.
 - A good article on reputable VPNs is available at: au.pcmag.com/vpn/138/the-best-vpn-services
 - Help staff ensure they have changed the default password on their home router.
 - A good instructional video is available at: www.youtube.com/watch?v=CCWS6qQ1k5k.
- Use a reputable password manager. If possible, have a company-wide licence so you can monitor usage and require staff to use it at all times.
 - If you can, take the opportunity to go password free and up your ante on MFA at the same time. A highly innovative Australian company providing technology to support this is **Forticode** (www.forticode.com).
- If in doubt, don't click! Ensure your team has a basic understanding of of cyber security, including being alert to scams and malicious links in emails (phishing).
 - **Cyber Aware** (www.cyberaware.com) – provide cyber 101 training designed for Australians by Australians.
 - Stay across the latest scams by subscribing to the **ACSC** alert service : www.cyber.gov.au/acsc/register/individuals-and-families
 - Report it if you've received an SMS or email you think is a scam to **Scamwatch** (www.scamwatch.gov.au)
 - Use Australian company **Mailguard** (www.mailguard.com.au) to stop malicious emails reaching your team in the first place.

Australian Cyber Companies

Cyber security management can be challenging for small businesses that don't have technical support or expertise. Australia has great cyber security companies known as Managed Security Services Providers or MSSPs who specialise in this. A selection of companies who already have SME customers are listed below, but you can also search for MSSPs through your favourite browser.

- **CyberCX** (www.cybercx.com.au) – a group of 13 MSSPs that span Australia and New Zealand.
- **KineticIT** (www.kineticit.com.au) – is an MSSP with offices nationally and in New Zealand.
- **ParaFlare** (www.paraflare.com) – provide real-time managed detection of cyber attacks and incident response.
- **Red Piranha** (www.redpiranha.net) – a national MSSP providing services from Australia into Asia.
- **Triskele Labs** (www.triskelelabs.com) – provide a security team as a service, as well as other key services to ensure you have holistic management of cyber risks.

More broadly, it is important to have a good understanding of your digital assets and how well protected they are from malicious interference, including access management and protecting your website. You can speak to your MSSP about this – and there are Australian companies who specialise in monitoring and responding to cyber breaches, including for small business:

- **Assetnote** (www.assetnote.io) – provide a software solution that automatically maps your external assets and monitors them for changes and security issues to help prevent serious breaches.
- **Cogito Group** (www.cogitogroup.net) – provide a range of solutions and services including security assessments, identity management and authentication.
- **Ionize** (www.ionize.com.au) – provide a range of services including accredited security assessments and guided implementation of actions to improve your organisation's cyber security.
- **Kasada** (www.kasada.io) – provide a software solution that prevents malicious automated attacks on your website and other digital infrastructure.
- **Hactive.io** (www.hactive.io) – provide accredited security assessments. In addition to a wide range of other services, they also offer a software solution that continuously tests your digital infrastructure for vulnerability to attack.
- **RightCrowd** (www.rightcrowd.com) – provide advanced physical access management which also integrates tracking of your digital assets to know whether they are on or offsite.
- **Slipstream** (www.slipstreamcyber.com) – provide a range of services from their Cyber Security Operations Centre in Perth. They optimise client security and resilience through data-driven intelligence.

- **ES2** (www.es2.com.au) is a leading Australian based company specialising in Cyber Security, Business and Cloud Solutions for all sized organisations within the public and private sectors, with its Head Office in Perth
- **Tannhauser** (www.tannhauser.com.au) is a locally owned and operated Perth, WA consultancy providing cyber security, risk and resiliency services
- **Yira Yarkiny** (yirayarkiny.com.au) Yira Yarkiny Group is a 100% Indigenous owned and operated company with a focus on security services. Yira Yarkiny provides end to end security services with a large focus on Cyber Security.

Understand your organisation's cyber readiness with a tool that's easy to use and won't take up much time:

- **Cynch** Security's Cyber Fitness online platform is specifically built for Australian micro and small business. They've also published a workbook that can help you record decisions on how you'll make things available remotely. cynch.com.au

If your company sends and receives volumes of information like a medical centre, accountancy or legal firm, consider putting in place practices that clearly communicate to staff, clients and customers the level of sensitivity around information:

- **JanusNET** (www.janusnet.com) is an Australian company that provides an online tool that marks your documents and emails with the right classification, like 'commercial in confidence' and helps to prevent data loss.

Australia's cyber security industry has over 500 companies developing and delivering products and services across the 50+ cyber security capability types in the global market. The companies listed in this fact sheet are a snapshot of those that have rapidly deployable solutions – there are many more available. Visit AustCyber's website or contact us for more information.

AustCyber's mission is to support the development of a vibrant and globally competitive Australian cyber security sector and in doing so, enhance Australia's future economic growth in a digitally enabled global economy. We are one of six industry-led, federally-funded Industry Growth Centres that operate as small private sector, non profit entities. Industry Growth Centres are an initiative that aims to drive innovation, productivity and competitiveness by focusing on areas of competitive strength and strategic priority.



Western
Australia
Innovation Hub