AustCyber
Australian Cyber Security Growth Network

Cyber security for startups and small businesses with remote working

Why do cyber security now?

Some, if not all, of your business and its operations involve digital and/or internet connected tools and processes. Having the means to manage cyber risks in your organisation, and ensure your suppliers and partners are not exposing you to unnecessary cyber risk, is always important.

Finding the time and resource to do it can be challenging, but even more so during a crisis. When you have staff working remotely, it's critical that you protect your organisation and people from cyber attack.

This is because it reduces cost and manages risk to reputation if you are compromised. In a crisis, it also ensures that as your organisation recovers, you're ready to grow in ways that are more trusted and assured.

Where to start?

Have a good understanding about where your organisation's cyber readiness is at by using 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 your decisions on how you'll make things available remotely.

Read up on authoritative practical advice. This factsheet complies a list of actions from these to help you act quickly, with the assurance you're on the right track.

- Small business advice from the Australian Government's Australian Cyber Security Centre: *www.cyber.gov.au/small-business*
- Small business advice from the Australian Government's Stay Smart Online program: *www.staysmartonline.gov.au/protect-your-business*

Here are some useful articles on business sustainment more broadly:

- What to focus on now: *www.smartcompany.com.au/business-advice/strategy/covid-19-business-survival/*
- For startups moving to remote working: *www.ribit.net/blog/top-5-tips-for-startups-moving-to-work-remotely-during-covid-19/*

Securing your digital footprint

There are a range of cyber security and IT related things your business should be working to have in place, regardless of operating circumstances. These become more important if you have a distributed workforce, including team members working from home.

- 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.
- Turn on automatic updates for your operating system (e.g. Microsoft Windows) to ensure as much malicious software is blocked.
- Ensure your business and all staff have updated the apps used by your business to the latest versions (should be done regularly).
- Ensure you have a procedure in place for regular backups of data and systems.
- 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.

It can be challenging for small businesses that don't have technical support or the expertise within the team to get these things done and done well. Australia has great cyber security companies who specialise in this area – known as Managed Security Services Providers or MSSPs. 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.

A great way to check if your MSSP is ensuring they've configured the security of your software and IT infrastructure appropriately, is to ask them if they are using **Detexian** (*www.detexian.com*) – an Australian cyber security company that has developed a tool to monitor unauthorised changes in software configurations and systems access.

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 these areas, including for small business needs:

- **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.hacktive.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.au*) - provide a range of services from their Cyber Security Operations Centre in Perth. They optimise client security and resilience through data-driven intelligence.

If you're a company involved in sending and receiving volumes of information/data like a medical centre, accountancy or legal firm, consider putting in place practices that clearly communicate between staff and clients/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.

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

- Ensure staff understand how to connect remotely to company infrastructure securely.
  - 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: *https://au.pcmag.com/vpn/138/the-best-vpn-services-for-2020* (If you want to know who AustCyber uses, email us at *info@austcyber.com*).
  - Help staff to ensure they have changed the default password on their home router.
    - A good article on how to do this, including instructional videos, is available at: *www.techradar.com/au/broadband/how-to-change-your-router-password*.
- 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 business has a basic understanding of the what and how 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 COVID-19 scams at: *www.staysmartonline.gov.au/alert-service/covid-19-scam-messages-targeting-australians*
  - Report it if you've received an SMS or email you think is a scam to Scamwatch (*www.scamwatch.gov.au*) to verify what you're seeing is real or malicious.
  - Use Australian company **Mailguard** (*www.mailguard.com.au*) to stop malicious emails reaching your team in the first place through their software that integrates with your email software.

For specific information on the financial relief packages made available by Australian governments, visit:

National:

- Business.gov.au: 'Coronavirus information and support for business' – https://www.business.gov.au/risk-management/emergency-management/coronavirus-information-and-support-for-business
- Australian Treasury: 'Support for Businesses' – https://treasury.gov.au/coronavirus/businesses

State and territories:

- ACT: 'Treasury: COVID-19 Economic Survival Package' – https://apps.treasury.act.gov.au/budget/covid-19-economic-survival-package
- NSW: '$2.3 billion health boost and economic stimulus' – https://www.nsw.gov.au/news-and-events/news/health-boost-and-economic-stimulus
- NT: 'Trade, Business and Innovation: Jobs Rescue and Recovery' – https://business.nt.gov.au/support-for-business/recovery
- QLD: 'Immediate Industry Recovery Package' – https://www.qld.gov.au/about/industry-recovery
- SA: 'Unprecedented response and economic stimulus to drive SA jobs, economy in wake of bushfires, coronavirus' – https://www.premier.sa.gov.au/news/media-releases/news/unprecedented-response-and-economic-stimulus-to-drive-sa-jobs,-economy-in-wake-of-bushfires,-coronavirus2
- TAS: 'Tasmanian Support & Stimulus Package' – http://www.premier.tas.gov.au/documents/FACT_SHEETS_-_STIMULUS_PACKAGES_Final-V2.0.pdf
- VIC: 'Economic Survival Package To Support Businesses And Jobs' – https://www.premier.vic.gov.au/economic-survival-package-to-support-businesses-and-jobs
- WA: 'Coronavirus: COVID-19: Western Australian Government response' – https://www.wa.gov.au/organisation/department-of-the-premier-and-cabinet/coronavirus-covid-19-western-australian-government-response

By Australian banks:

https://www.ausbanking.org.au/banks-small-business-relief-package/

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.

AustCyber
Australian Cyber Security Growth Network