CYBER SECURITY COOPERATIVE RESEARCH CENTRE

CSIRO DATA 61

CyberCX

Small but stronger

Lifting SME cyber security in South Australia

Prepared by CSCRC, CSIRO's Data61, CyberCX

cybersecuritycrc.org.au

This project was a collaboration between the CSCRC, CSIRO's Data61 and CyberCX

With the support of the Government of South Australia and the ACSC

Project team

Dr Stephenie Andal

Anne-Louise Brown

Dr Marthie Grobler

Regine Richelle

ACKNOWLEDGEMENTS

Thank you to the Government of South Australia, especially Premier Steven Marshall, for its valuable support on this project. Thank you also to CyberCX and CSIRO's Data61 for their dedication and hard work to deliver this collaborative research project. And finally, the CSCRC thanks the six South Australian SMEs who participated in this pilot project, giving so generously of their time, to make this pilot project happen. This report is based on a more comprehensive report, ***South Australia Pilot Project: SME Cyber Security Uplift.***

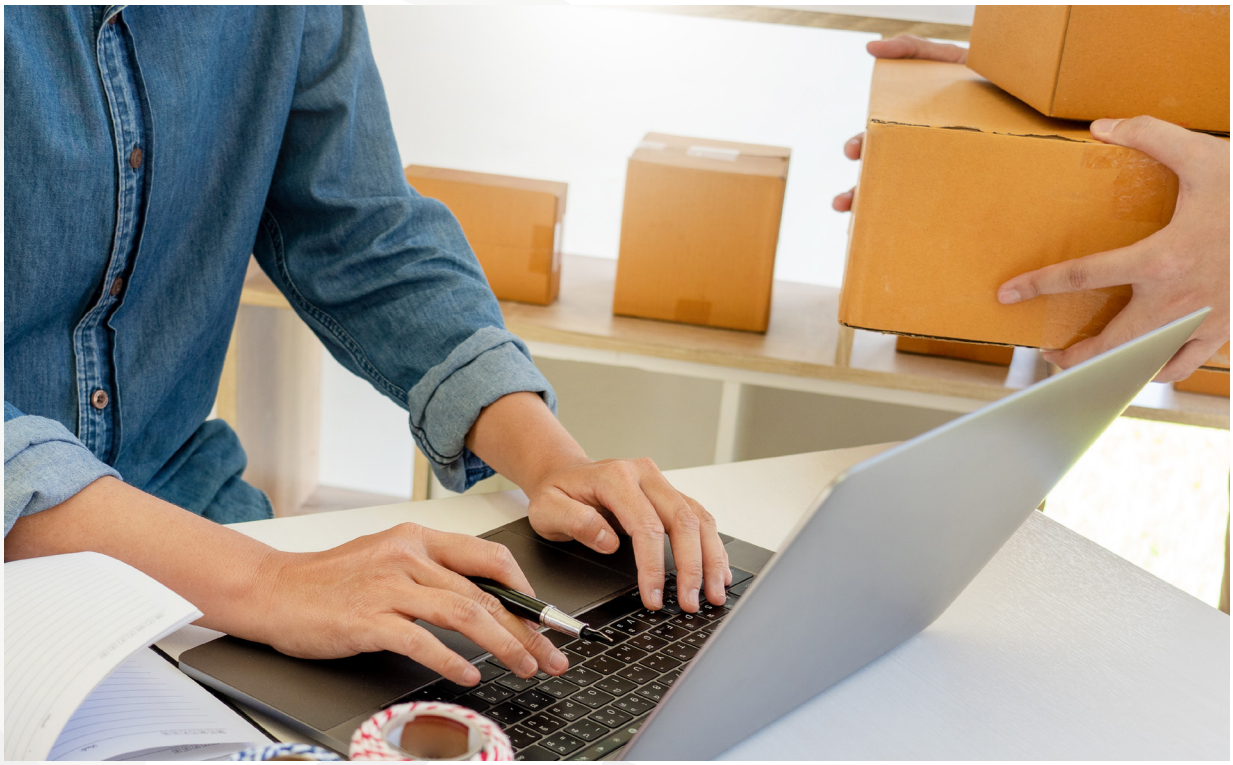
PROJECT OVERVIEW

Small and medium enterprises (SMEs) are the lifeblood of Australia's economy, comprising more than 90 per cent of the economy. The Australian Bureau of Statistics (ABS, 2019) reports SMEs specifically contributed to the national economy through employment (44% of private-sector employment in selected industries), industry value added (34%) and gross domestic product (35%).

However, when it comes to cyber security uplift, the SME sector – which is diverse in size and scope – faces a myriad of challenges. Namely, investment of money, time and resources often present significant barriers to SME cyber uplift. In addition, SMEs are inundated with cyber security how-to guides and written advice, which can be overwhelming and confusing. Hence, this project takes a different approach: focusing on practical cyber security implementation and integration. This project was borne of the desire to create meaningful change, identifying the common strengths and weaknesses of SMEs as it comes to cyber security and establishing simple and cost-effective solutions to bolster cyber security.

The Cyber Security Cooperative Research Centre (CSCRC), in collaboration with CyberCX and CSIRO's Data61, and supported by the Government of South Australia and the Australian Cyber Security Centre (ACSC), invited six Adelaide-based SMEs to participate in the pilot project. Cyber security maturity assessments were completed via targeted consultations with the six SMEs by CyberCX and an observer from CSIRO's Data61, with the data analysed by CSIRO's Data61. This report presents the high-level findings of the pilot project, along with possible future focused initiatives and strategies to achieve SME cyber security uplift, as well as offering practical advice to SMEs about how to bolster their cyber security posture.

The pilot learnings have been analysed and formulated into a comprehensive analysis report and blueprint that will help inform the Government of South Australia, as well as other governments and government departments, in the implementation of scalable and practical initiatives to support SME cyber security uplift. The blueprint is designed in a way that it can be implemented cross-jurisdictionally and is intended as a resource to help policy makers prioritise areas of importance for SME cyber security uplift.



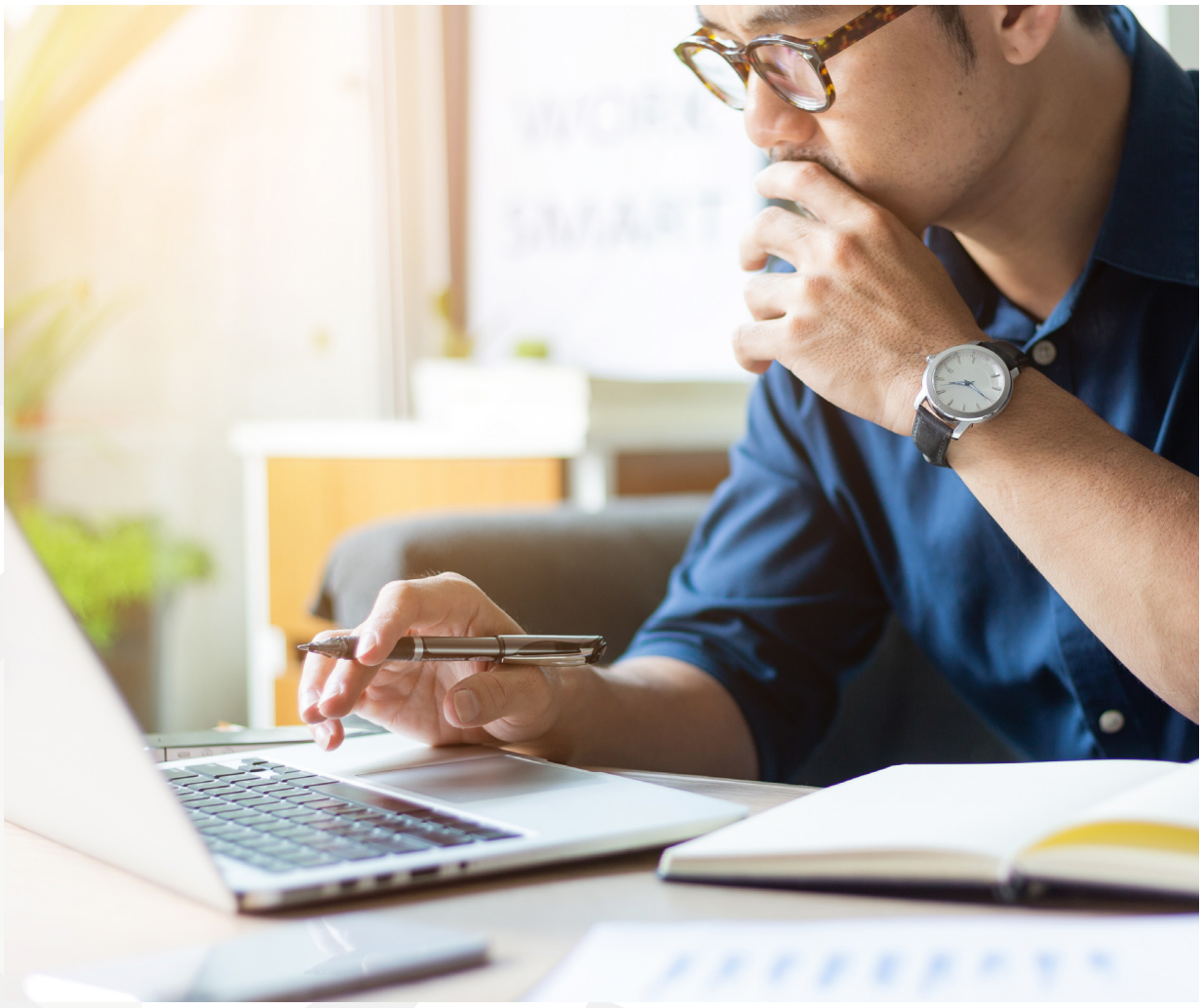
METHODOLOGY

This collaborative pilot project between the CSCRC, CyberCX and CSIRO's Data61 was aimed at improving the security of six South Australian SMEs and to foster better understanding of the challenges these organisations face in implementing and maintaining cyber security. The findings build on existing guides to create practical and implementable cyber security uplift solutions for Australian SMEs and will assist governments to formulate targeted SME cyber uplift initiatives.

The baseline cyber security of the SMEs was mapped to the ACSC's Information Security Manual's Cyber Security Principles. To manage the uplift process, a gap assessment was conducted to map the state of the participating SMEs' cyber resilience based on the principles.

While all SMEs expressed a desire for cyber security uplift, the depth of desire was commensurate with their level of cyber security maturity. The lower the cumulative cyber security maturity score, the stronger their emphasis on the need for cyber security hardening. SMEs with a higher maturity still reported specific areas in which they wished to improve their cyber security maturity as they grew their business to work with more sensitive information.

The key reasons driving the desire for cyber uplift among the SMEs were to improve service delivery for clients, to enhance business reach to larger, potentially international clients, and to acquire Defence Industry Security Program (DISP) membership. Some of the SMEs were comfortable with their current cyber position, reflecting their maturity.



SME PARTICIPANT SNAPSHOT

The number of staff employed by the participating SMEs varied between 12 and 52, with various combinations of permanent employees and contractors.

Half the SMEs reported they primarily use cloud software as a service (SaaS) for critical business operations.

Two SMEs reported they use hybrid infrastructure, with most of their data stored on premise and on selected cloud services.

One SME reported they stored all information and data on premise.

Half the SMEs reported they were dependent on their managed service providers (MSPs) to assist in delivering critical business objectives, while others indicated they relied on a cyber security consultancy firm or had in-house services.

One SME reported employing university students to assist in delivering critical business objectives, supported by permanent staff who focus on ICT infrastructure management.

The majority of SMEs were receptive in terms of discussing recommendations and advice about how to bolster their cyber security practices.

One SME was hesitant when discussing budget while others were more forthcoming and direct.

KEY FINDINGS

Cyber is considered as an add-on and is not built-in to business operations. Most SMEs only have a very basic cyber security plan and tend to address cyber security problems and incidents as they arise. SMEs are focused on advancing in their own fields and less inclined to be early adopters of new technologies outside this focus.

SMEs manage cyber budgets in an ad hoc fashion. The combination of limited dedicated cyber security resources, ad hoc information environments, and the absence of well-defined processes is a persistent concern. Most SMEs indicated they need guidance in terms of adequate cyber security budget, as this is not fully formalised or managed as a strict percentage of overall budget.

A trusted network is not established in the supply chain. There is a worrying lack of maturity in a trusted network in supply chain management. The majority of the SMEs acknowledged that separation of responsibilities for cyber security with key suppliers is something they do not address at all, although they prioritise information classification and management.

Physical assets are better secured than digital assets. SMEs all have adequate measures in place for physical access control, although there were varied responses in password management, access control and application control. All SMEs had basic anti-virus controls in place but opted for entry level solutions with basic detection capabilities.

Regulatory and legislative obligations are unclear. There is a specific need for guidance in terms of legislation and regulations that need to be adhered to from an SME perspective. With the exception of industry-specific expectations, SMEs are unclear of what level of cyber security maturity is expected.

Incident preparedness is very poorly developed. Half of the SMEs acknowledged they were poorly prepared for cyber attacks, with either no processes in place or basic undocumented processes being followed. SMEs face financial and resourcing barriers to undertake full incident investigation and recovery, in addition to not having the correct measures in place to mitigate the initial vulnerabilities.

BYOD poses a considerable risk. Many SMEs embrace a culture of bring your own device (BYOD) but do not have the necessary checks in place to ensure these devices do not introduce security vulnerabilities into systems and networks.

Cyber security maturity varies significantly between SMEs. SMEs with lower cyber maturity showed a stronger desire for cyber security uplift, while SMEs with a higher cyber security maturity showed a desire to maintain their maturity and expand their business operations. SMEs were more advanced in governance-related aspects, and less mature in protection-related aspects.

FUTURE FOCUS: SME CYBER SECURITY UPLIFT

The findings from this pilot will help form the basis of future approaches to SME cyber security uplift by providing understanding of the current cyber maturity landscape of SMEs and identifying key target areas for improvement. Future approaches must be driven by effective policy making, with this pilot helping signpost possible initiatives and strategies that could be adopted to effect nation-wide cyber security uplift. These policy approaches and resulting public guidance and advice would help guide SMEs when enhancing their existing mechanisms through the implementation of stronger cyber security measures.

Recommendations for policy makers

- Implement a co-designed approach to cyber security campaigns aimed at SMEs to support general awareness and the need for SME cyber security maturity. These might be co-designed with industry to ensure widespread industry uptake.
- Establishing new **funding models and incentivisation packages** to support SME cyber security uplift.
- Establishing new **programs and initiatives** to embed a **cyber secure attitude** across the economy and foster cyber maturity.
- Together with the business community, the co-design and development of a **SME community engagement system** to provide support and access to relevant cyber security information which will facilitate SME cyber maturity uplift.
- Ongoing, timely and clear guidance concerning **specific legislative and policy requirements for SMEs.**

Public guidance – key messaging

- Cyber security should be elevated to the board as a **strategic business and risk consideration**, not siloed within the IT department.
- Cyber security is integral to **ongoing organisational integrity**, and not considered as a one-off, 'tick box' exercise.
- Cyber security requires **proactive and considered investment** to elevate maturity.
- More transparency concerning **vendor offerings** will enable broader SME product take-up and drive cyber security uplift.
- Cyber security must be a shared responsibility within organisations to drive an economy-wide **cyber safe culture change**.

Blueprint for SME Cyber Security Uplift

Five common weaknesses identified across SMEs

There were five key areas of weakness identified across SMEs as it came to cyber security maturity:

- Cyber security considerations remain add-ons for most SMEs.
- Due to limiting factors including cost and resourcing, most SMEs have only basic cyber security plans, poorly developed incident preparedness, are ill-prepared for BYOD risks and cyber security budget management remains ad hoc.
- Effective management of supply chain risks and vulnerabilities is not yet established, due to lack of cyber security maturity.
- SMEs need greater certainty regarding the minimum cyber security maturity they should achieve, which could be addressed via regulatory or legislative means.
- Physical assets are better secured than digital assets, given their tangibility.

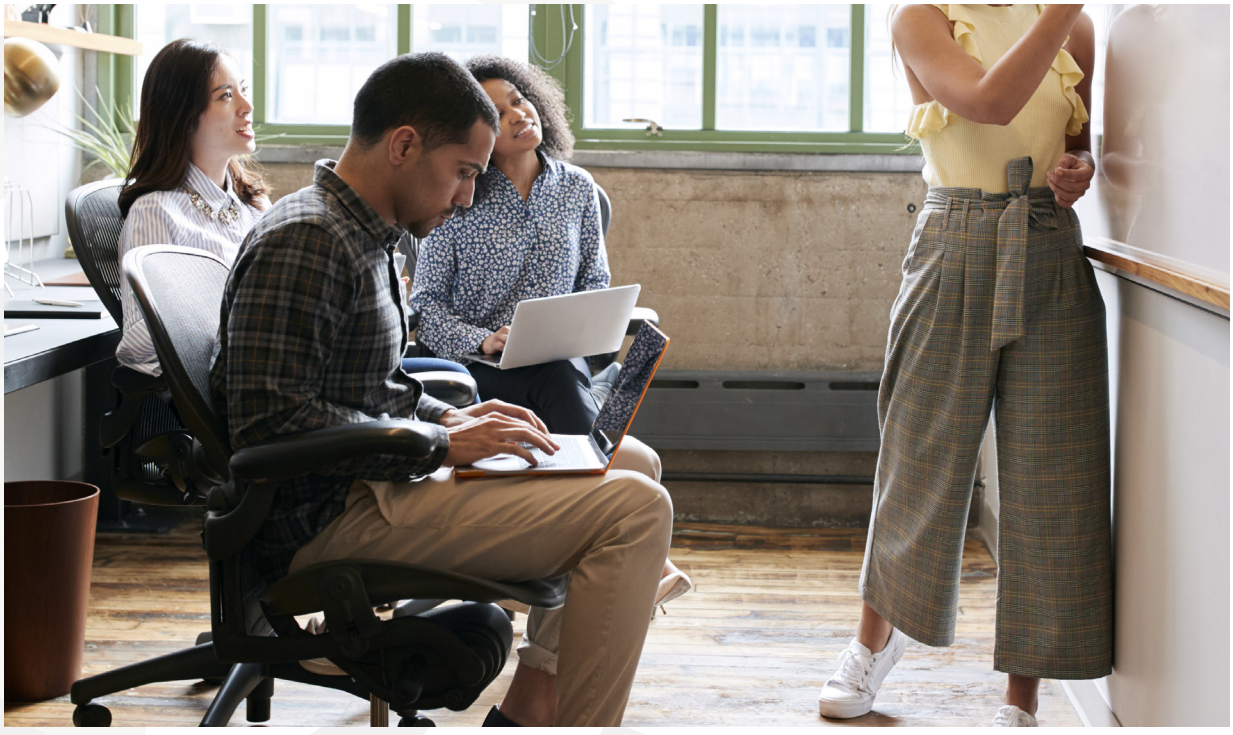
Engagement strategies that worked for the SMEs

- **Transparency is key**. Offering transparent advice to SMEs with a cooperative approach that builds on government advice about how they might improve their cyber security builds trust.
- SMEs are looking for **reliable and trustworthy resources**. SMEs are wary about vendor offerings and unsure about what solutions to choose. They require ongoing access to vendor-agnostic approaches to uplift their cyber security posture.
- SMEs need access to **cyber security basics**. Many SMEs need greater awareness of some of the key building blocks of cyber security, including the need for strong passwords, the value of patching to keep systems safe, and that people are at the heart of cyber security and need to be adequately trained and aware of the risks.
- Cyber security is **a journey**. Many SMEs are operating under time and resource constraints. Recognising these factors and assisting SMEs on their path to cyber security maturity is a more effective approach than overwhelming SMEs with information.
- SMEs are hungry for **industry best practice benchmarks** to get a better sense of where they have 'gaps' in their cyber security protocols.
- Assisting SMEs with **securing data** is invaluable. Many SMEs hold sensitive information and IP and need practical advice about simple and effective ways to secure data and minimise risk.

Next steps

The blueprint provides practical steps for SMEs to implement to drive cyber security uplift across their business. These include:

1. **Embed a cyber secure attitude.** Shift thinking. Embed cyber security in everything that touches technology.
2. **Embrace cyber security development.** Cyber security development is an incremental process, a journey towards maturity. It is not a one-off investment.
3. **Embody good cyber behaviour.** Good cyber security behaviour is integral to organisational integrity. Cyber security is not just a tick box exercise.
4. **Earn trust in the cyber ecosystem.** Cyber security has no boundaries. One organisation's behaviour will affect the cyber security of another organisation in the ecosystem.
5. **Encourage cyber security camaraderie.** Shared cyber security intelligence and decision making enhances communicable cyber capabilities.
6. **Eliminate ad hoc cyber planning.** Cyber security matures with good planning and proper budgeting. Methodical planning leads to better governance.
7. **Enforce good cyber hygiene.** Put practices and steps in place that employees can easily follow to maintain system health and improve online security.
8. **Empower whole-of-organisation cyber thinking.** Cyber security should permeate throughout the whole organisation. It stretches beyond the traditional IT boundaries. Everyone owns cyber security from the CEO down.
9. **Escape the cyber blame game.** Encourage people to report cyber mistakes and suspicious behaviour. Reward open communication and avoid naming and shaming within the organisation.
10. **Exercise common cyber sense.** Stop. Think. Think again. React. Think cyber security and be cyber safe before you act.



QUICK WINS

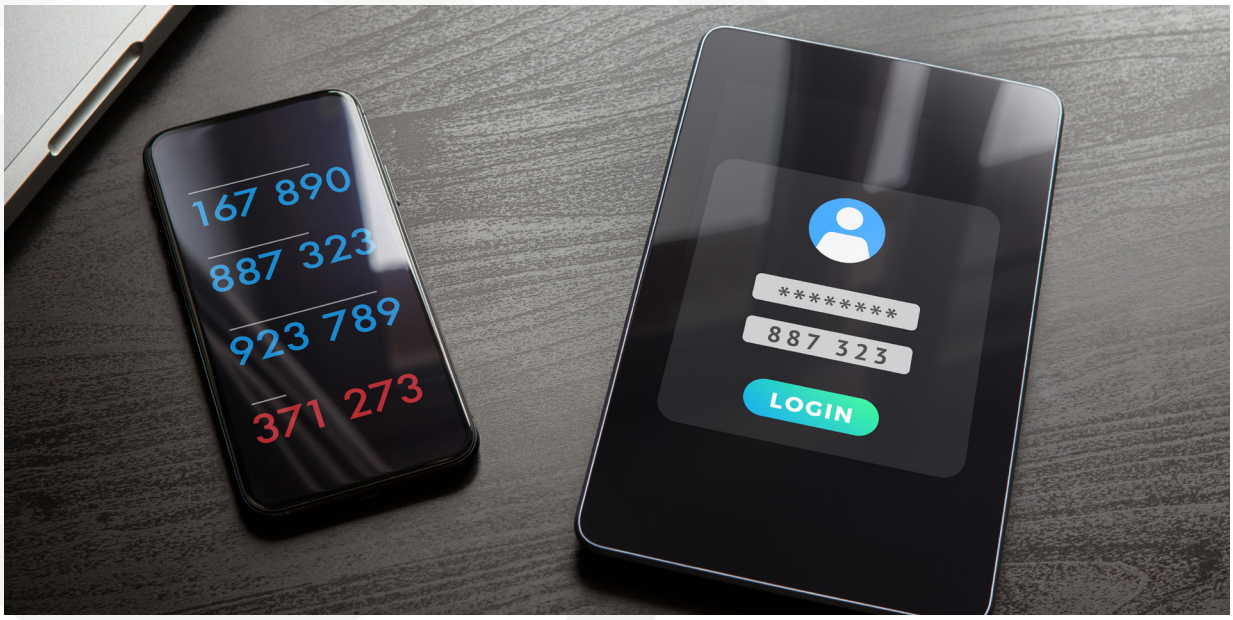
Protecting your digital assets is vital. For many SMEs these assets are essential to running the business and getting paid.

There are steps you can take to guide cyber security uplift. They are practical, foundational steps for building stronger cyber security practices.

Given resourcing and time constraints, you can take these steps individually or as a whole, helping improve the overall cyber posture of your business.

SME cyber steps:

- You need to know what to protect and why you are protecting it. It is vital that you take the time to do a high-level risk assessment and gap analysis, which will help you gain full awareness of your digital environment(s). This can be done internally or via a third-party cyber security provider. Key considerations should include:
  - **Knowing the value of your data:** Map out your key valuable data - the data that is essential to running your business, who has access, where it is stored (internally and across the globe), who is protecting it and how well it is protected.
  - **Personnel:** Know who is in your business and has access to your data. Develop a personnel security process with verification and background checks of personnel and third-party contractors. This should include requirements for prospective employees to submit a national police check.
  - **Supply chains:** Identify and make a list of suppliers as they can often be a way into your systems. Supply chain management helps lift visibility of potential third-party cyber security risks.
  - **Device management:** Develop specific BYOD governance and policy to help you manage the use of personal devices that are used to undertake work-related tasks.
- **Improving end-user account and device security.** Important steps to take include:
  - Making sure you use strong passwords.
  - Implementing multi-factor authentication (MFA) where possible and practical for both employees and contractors - especially on key systems.
  - Using password storage vaults.



QUICK WINS cont.

- **Restrict access** to critical data and systems as well as physical access to servers so that only employees who need access to carry out their roles have access to the right systems. Key to this is knowing who has the keys to the castle – make sure administrative privileges (i.e. authorisation to configure network and device settings) are only provided to those who really need them.
- Subscribe to a trusted source of **threat and vulnerability intelligence** and register with the ACSC's Partnership Program, which enables organisations to draw on technical expertise and awareness to get insights and support on relevant cyber security threats.
- **Review your business continuity processes** in case a cyber incident should occur. This could include:
  - Developing a cyber incident response process, reviewed and updated annually.
  - Regularly assessing the adequacy of data backups and storage.
  - Documenting critical processes and recovery steps for essential systems in the event of a cyber incident and the establishment of clear roles and responsibilities.
  - Making sure you have a physical list of key staff members and their contact details held offsite.
- Ensure **adequate cyber security training** is provided to all staff, on a regular basis, especially when new cyber security procedures or processes are implemented.
- If budget allows, consider undertaking annual **penetration testing** of platforms to help pinpoint cyber weaknesses for all connected systems that you operate. A penetration test, also known as ethical hacking, is a process that checks your internet facing sites and your key digital systems for exploitable vulnerabilities.

CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE