CyberWardens.

Your Cyber-Smart Guide

Navigating the next five years of cyber security for small business

cyberwardens.com.au

An initiative of COSBOA

Foreword

Small businesses make up more than 97% of all Australian businesses. They employ millions of people, support local communities and keep our economy moving every day.

They are also increasingly exposed to cyber risk.

Cyber security is no longer something only large organisations need to think about. Cyber criminals are looking for easy ways in, and small businesses can be attractive targets because they are often busy, time poor and connected to customers, suppliers, payment systems and online platforms.

A florist with a customer database, a bookkeeper with access to payroll information, or a small manufacturer that works with larger organisations all hold information and access that is worth protecting. Even a sole trader can be connected to a much bigger digital network.

At the same time, new technology is creating real opportunities. AI and other digital tools are changing how small businesses operate, serve customers and manage day-to-day tasks. These tools can help businesses save time and work more efficiently, but they also need to be used with the right safeguards in place.

That is why Cyber Wardens has developed this guide. It is designed to help Australian small businesses build practical cyber habits, strengthen their confidence and make informed decisions about the tools they use.

We have drawn on expert advice and real conversations with people who work closely with small businesses every day. The guidance in these pages is practical, accessible and focused on what small business owners and their teams can actually do.

Read it, share it with your team, and choose one action to take next. Small changes, done consistently, can make a meaningful difference.

Skye Cappuccio,
Chief Executive Officer
Council of Small Business Organisations Australia (COSBOA)

The next five years
What is coming and why it matters

Small businesses are operating in a connected and fast-moving environment, where more systems are online, more tasks are automated, and new tools are changing how businesses work, communicate and serve customers.

That brings real opportunity, but it also brings risks that small businesses need to understand and manage.

The good news is that improving cyber security does not have to be complicated or expensive. Many of the most effective cyber defences come down to everyday habits, clear processes and making cyber security part of how the business runs. For many small businesses, the hardest part is finding the time and making it a priority among all the other demands of running a business.

Human error continues to be the main cause of cyber incidents in Australia. When people work quickly, juggle competing tasks and make decisions without the right checks in place, mistakes can happen easily. As AI tools make it easier to create, share and automate work, those everyday decisions will matter even more.

Cyber criminals are also becoming more organised. They look for easy ways to access information, money or systems, and small businesses can be an attractive target. A small business may be connected to larger customers, suppliers, government contracts or payment platforms, which can make it part of a much bigger digital network. At the same time, small businesses do not necessarily have the same cyber protections in place as larger organisations, making them a low-hanging fruit for cyber criminals.

The National Cyber Security Strategy sets out a pathway to strengthen Australia's cyber resilience. For small businesses, resilience is built through practical decisions made every day: using strong passwords, turning on multi-factor authentication, checking requests before acting, backing up important information and helping staff know what to look out for.

This guide brings together five expert perspectives on the issues that will shape the next five years for Australian small businesses. Each section is designed to be practical, accessible and grounded in the realities of running a small business.

The next five years

Skilled people	Building cyber awareness and capability across your team, so that the humans in your business become your strongest defence rather than your greatest vulnerability.
Secure foundations	Getting the non-negotiable basics right, consistently and without overcomplicating them.
Smart adoption	Using AI and new technology safely and confidently, as a genuine business advantage rather than an unmanaged risk.
Connected networks	Understanding your place in the broader supply chain and taking responsibility for your share of the risk.
Global opportunity	Using strong cyber security as an enabler of growth, trust, and access to new markets.

CyberWardens.

Connected networks and secure foundations

Lieutenant General Michelle McGuinness CSC
National Cyber Security Coordinator

Lieutenant General Michelle McGuinness CSC is Australia's National Cyber Security Coordinator. In this role, she leads the Australian Government's response to significant cyber incidents and helps drive the national agenda to strengthen Australia's cyber resilience.

> *"The basics matter, and the basics work."*

Small businesses are not peripheral to national cyber security: they are connected at every level

For small businesses, LTGEN McGuinness's message is direct: cyber security is now part of running a business. It cannot sit only with IT support, and it cannot wait until something goes wrong.

"The biggest shift is that cyber security is no longer a technical issue sitting with IT or technical offices," LTGEN McGuinness says. "It is a core business responsibility."

That shift matters because small businesses are more connected than many realise. They rely on suppliers, software providers, payment systems, cloud platforms and customer databases. A weakness in one business can create a pathway into another, particularly when that business is part of a larger supply chain or service network.

LTGEN McGuinness says many small businesses still underestimate "that they are an attractive target for cyber criminals and that they have a key role in the broader ecosystem."

The starting point is understanding what your business relies on, who has access to your systems and what protections are already in place.Cyber security also needs to be part of the way people work. Staff do not need to become technical experts, but they do need to know how to spot warning signs, question unusual requests and respond quickly when something feels wrong.

"Cyber capability is not about turning everyone into technical experts," LTGEN McGuinness says. "It's about building a human firewall."

Secure foundations are essential. LTGEN McGuinness points to the Australian Signals Directorate's Essential Eight as one of the clearest guides for reducing cyber risk. Small businesses can use it as a practical benchmark, and ask their IT provider what protections are already in place, where the gaps are and what should beprioritised next.

Supply chain security is another clear focus. Many small businesses rely on external providers for software, payments, websites, payroll, marketing platforms and customer management tools. These services help businesses operate, but they can also introduce risk if security is not understood.

Small businesses should feel confident asking suppliers practical questions. How is our data stored and protected? Who can access it? What happens if there is a cyber incident? How will you let us know?

These are reasonable business questions, and they are increasingly part of working with trusted partners. As LTGEN McGuinness explains, "Cyber security is no longer confined to a single organisation. It is a shared responsibility across connected networks."

Reporting cyber incidents also matters. When a business reports an incident, it helps build a clearer national picture of what cyber criminals are doing and who they are targeting. Reporting is not about blame. It helps government and industry understand the threat environment and provide better support to others.

LTGEN McGuinness's advice is practical and reassuring. Cyber security does not have to be perfect to make a difference. It needs to be taken seriously, built into everyday operations and supported by simple actions that are used consistently.

3 things to do:

1

Check your cyber foundations.

Use the Australian Signals Directorate's Essential Eight guidance and ask your IT provider which protections are already in place.

2

Ask better questions of your suppliers.

Find out how your data is stored, protected and managed, and what will happen if they experience a cyber incident.

3

Know where to get help.

Visit cyber.gov.au to access free guidance from ASD's Australian Cyber Security Centre, sign up for alerts and understand how to report an incident.

CyberWardens.

Skilled people and global opportunity

Kersti Eesmaa, Vertical Scope Group

Kersti Eesmaa is the Chief Operating Officer of Vertical Scope Group and a leading voice on cyber workforce development in Australia. Formerly the Ambassador of Estonia to Australia, Kersti brings a unique international perspective to the risks facing Australian small businesses and a frank view of what it takes to build genuine cyber capability.

> *"The question small businesses often ask is, 'Why would anybody be interested in us?' That mindset needs to change."*

Why 'It won't happen to me' is the most dangerous assumption in business

Kersti is adamant that a critical need for small businesses is to understand that they are part of a much wider digital network. Even a sole trader can hold valuable data, use shared software, or provide services to a larger organisation.

"The criminals work pretty much like SMEs," Kersti says. "They all want to get the best return on the investment."

That means cyber criminals are often simply looking for the easiest way in. A small business with customer data, supplier access, payment information or poorly configured systems can become part of the pathway.

Kersti says one of the most common assumptions she hears from small businesses is, "Why would anybody be interested in us?" But that mindset can leave businesses exposed. A bakery with VIP delivery addresses, a GP with patients' medical records, or a contractor connected to a larger client all hold information that could be useful to someone.

Her advice is to start by understanding what your business has that others might value. That includes customer records, financial information, supplier relationships, account access and the systems you rely on to keep trading.

Kersti is also clear that small businesses do not need to turn everyone into cyber specialists. For many businesses, the first step is making sure the everyday technology they already use is set up properly.

"Cyber is not some magic, hacking, hoodie kind of complicated stuff," she says. "When you do cyber well, then you do IT well."

That is especially important for small teams, where IT and cyber security are often added to someone's existing job. If a business cannot afford a full-time IT person or managed service provider, Kersti says it may still be worth getting expert help to configure systems properly and show staff how to use them safely.

Training also matters. Kersti recommends making cyber awareness a regular habit, even if it starts with a short annual session. Practical exercises, such as phishing drills, can help staff understand how easily a mistake can happen and what to do differently next time.

"Repetition is the only way that people learn," she says.

Kersti also believes small businesses need to get more comfortable talking about cyber incidents. In her view, sharing real stories about what went wrong, what was missed and how a business recovered can be more powerful than generic warnings.

There is also a global opportunity in getting this right. Strong cyber security can help small businesses build trust, work with larger partners and compete in new markets. But Kersti cautions that going global can also increase exposure, especially when working in regions with different cyber risks or weaker security standards.

Her message is practical: cyber security should be treated as part of business continuity. It belongs alongside insurance, tax and compliance as one of the things a business does to keep operating.

3 things to do

1. **Map your data.**
   Identify what information your business holds that could be valuable to a criminal, including customer details, payment information, supplier access and login credentials.
2. **Check your supply chain exposure.**
   Think about who you work with, what systems you share and whether the people supporting your IT understand cyber security.
3. **Make cyber training a habit.**
   Commit to at least one cyber awareness activity each year for every person in your business, even if it starts with 20 minutes of practical training.

CyberWardens.

Secure foundations and connected networks

Adam Selwood, Cynch Security

Adam Selwood is the co-founder of Cynch Security, a platform purpose-built to make cyber security accessible and manageable for small businesses. With a background in both cyber risk and small business operations, Adam has worked with hundreds of small business owners to understand where the real gaps are and what ‘good enough’ cyber security actually looks like in practice.

> *“Good enough security is what we call cyber fitness. You’ve been working on it consistently. It’s something you’re actively managing, and you have the confidence that it’s under control.”*

Cyber fitness over cyber perfection

For Adam, the biggest shift ahead is the speed at which cyber risk is changing. Attacks are faster, technology is moving quickly, and customers, partners and government agencies are asking more of the businesses they work with.

“Small businesses are going to get hit from both sides,” Adam says. “Things are going to change with technology and security more rapidly, and the expectations that you’re keeping up with that are going to grow.”

That can feel intimidating, but Adam’s advice is deliberately practical. The goal is not cyber perfection. It is building what he calls cyber fitness. Just as physical fitness comes from regular habits over time, cyber fitness comes from taking small, consistent steps. It might be checking who has access to your systems, turning on multi-factor authentication, reviewing your backups, or spending time each quarter looking at what has changed in your business.

“You just need to take one step after another,” Adam says. “It’s far more important that you’re at least doing something.”

One of the biggest things small businesses underestimate is their external footprint. Any business with a website, email, social media account, online booking tool or payment system is visible online. That visibility can help customers find you, but it can also give cyber criminals information they can use.

Adam says many businesses are surprised by what can be found quickly from the outside, including the tools and platforms they use. Once a business understands what is visible, it can make better decisions about what needs to be protected.

Connected networks are also changing the expectations on small businesses. A business that wants to supply to a larger company, supermarket, government agency or critical infrastructure provider may increasingly be asked to answer cyber security questions before a contract is approved.

Adam says this often appears late in the process, when a business has already pitched, negotiated and nearly secured the work. Then a security questionnaire lands, filled with unfamiliar language and requirements.

“You will hit a wall as a small business trying to grow and sell to a larger organisation if you’re not in a position to overcome that compliance burden,” he says.

The best way to prepare is to start early. Small businesses should look at their current risks, review supplier and client contracts for cyber clauses, and consider what questions they may need to answer in the future. Even going through the process of getting a cyber insurance quote can help, because it prompts a business to check what protections are already in place.

Adam’s message is that cyber security can be an enabler, not just a cost. Businesses that understand their risks and build steady habits are better placed to adopt new tools, pursue larger contracts and respond if something goes wrong.

Good security needs to be active, regular and understood by the people running the business.

3 things to do

1

Think about what your business holds, who has access and what would cause real disruption if it disappeared or was exposed.

Review your contracts.

2

Check supplier, client and insurance documents for cyber security clauses or obligations you may have overlooked.

Build a regular rhythm.

3

Set aside time each quarter to ask what has changed, what needs attention and what simple cyber actions you can complete next.

CyberWardens.

Skilled people and smart adoption

Stephen Zappia, Revium

Stephen Zappia is the Chief Operating Officer at Revium, a technology consultancy helping businesses navigate digital transformation. Working closely with small and mid-sized businesses, Stephen brings a practical view of how AI is reshaping the way businesses work, and why human judgement still matters.

> *"Cyber security is not just a compliance burden. It is the way you build trust with your clients and customers, and more trust equals more success."*

People and technology: you need both, and you always will

Stephen Zappia has watched the AI conversation unfold inside small businesses over the past few years. The tools are genuinely powerful and the opportunity is real, but so is the risk if businesses use new tools without clear thinking, safe habits and the right checks in place.

"With new tools come new risks," Stephen says. "The old adage of remaining vigilant doesn't change."

One of his biggest concerns is overconfidence. AI can help people do things they may not have had the skills or time to do before, from drafting emails and reports to analysing information or building simple tools. That can be valuable, but it can also create risk when people trust the output without knowing how to assess it.

"Just because the AI is speaking with confidence, that does not mean that it's actually doing the right thing," Stephen says.

That is why Stephen believes curiosity and learning will be essential skills for small business teams over the next five years. People need to be open to new information, willing to question their assumptions and comfortable learning as technology changes.

He encourages businesses to build a culture where experimentation is supported, but not uncontrolled. Staff should have the right tools, clear guidance and safe spaces to test new technology without exposing business data or creating unnecessary risk.

Stephen describes three common approaches to AI adoption. Some people avoid it completely, like an ostrich burying its head in the sand. Others rush at every new tool without thinking through the risks, like a magpie going for shiny objects. The better approach is to stay aware, like a hawk, experiment with purpose and adopt the tools that genuinely serve the business.

"You want to have a bird's eye view of what's going on," he says. "You do want to swoop, but you only want to swoop when there's something that actually seems like it serves you or your business."

A practical first step is building a business knowledge base. Many small businesses hold valuable information in people's heads: how processes work, where files live, who does what and what customers expect. When that knowledge is not documented, the business becomes more vulnerable if someone leaves, gets sick or is unavailable.

Stephen recommends getting that knowledge into a shared, searchable system. It helps staff work more consistently, reduces silos and gives AI tools better information to work with when they are used safely.

Smart AI adoption also means protecting business information. Stephen recommends turning off model training where possible, avoiding personal accounts for work tasks, using de-identified or fake data when experimenting, and making sure a human reviews anything before it is sent, published or used to make decisions.

This is especially important with tools that can now create software, websites or applications quickly. Stephen warns that something built quickly still needs proper review before it is used in a business.

"If there's no governance over it, if there's no checks and balances, and if you don't know what you're looking for, you may actually end up releasing something that has some pretty negative consequences," he says.

His message is not to avoid AI. It is to use it deliberately. The small businesses that do this well will combine fit-for-purpose technology with capable people who know when to question, check and ask for help.

3 things to do

1. **Build a business knowledge base.**
   Capture key processes, customer knowledge and operational information in a shared system so it is not sitting in one person's head.
2. **Set rules for AI use.**
   Decide which tools your team can use, what information must not be entered, and when human review is required.
3. **Train your team to question outputs.**
   Encourage staff to check AI-generated content, verify unusual requests and think carefully before trusting what they receive online.

CyberWardens.

Skilled people, secure foundations and connected networks

Madeleine Opitz, Cyber Wardens Program Lead

Madeleine Opitz leads the Cyber Wardens program, which has trained tens of thousands of Australian small businesses to build cyber confidence from the ground up. Working at the intersection of education, behaviour change and small business culture, Madeleine has helped people without a technical background build the practical habits that protect their business every day.

> *"Real change starts with education. Actual education that helps people understand why it matters and what they personally can do about it."*

What 55,000 Australians taught us about cyber security

Ask most small business owners who is responsible for cyber security in their business, and they will point to one person. Usually themselves, sometimes a bookkeeper, occasionally whoever set up the Wi-Fi. It is a reasonable instinct, but it creates a fragile system. A staff member who clicks a phishing link or re-uses a password across accounts can undo everything else your business has put in place. Cyber security only works when it is shared.

"It only takes one weak link in the chain," Madeleine says. "And that chain runs through every single person in your business." Not everyone needs to be a cyber expert. But everyone needs to know the basics:how to spot a suspicious email, why MFA and strong, unique passwords matter and what to do if something feels wrong.

After building a community of over 55,000 people and a network of over 100 partner organisations, one pattern is clear: you are far more likely to take action on cyber security when you hear about it from someone you already trust. Not a stranger, not a generic campaign, but your industry association, your accountant or a fellow business owner who has already been through it.

"When someone hears about Cyber Wardens from a person they respect, they come in with confidence," she says. "That recommendation does a lot of the work before we even get started." This is why the partner network has been so central to the program.

In every session Madeleine runs, she asks the same question: how many of you have multi-factor authentication turned on across all your accounts? The hands that go up are rarely a majority. These are not outliers. They are business owners like you, with staff, customers and financial data sitting in systems that are one compromised password away from a serious incident. Before you tell yourself you have the basics covered, check. Really check. Because the gap between thinking you are protected and actually being protected is where most incidents begin.

If you are still working through the fundamentals, that is not a reflection of how smart or capable you are. It is a reflection of how stretched you are, and how quickly the digital landscape has shifted around you.

"Every time we run a session and someone says 'I didn't know that,' that's not a failure," Madeleine says. "That's exactly what we're there for."

What ultimately makes the difference is culture. A one-off training session does not change behaviour. A policy document sitting in a shared drive does not either. What works is when cyber security becomes part of how a business operates day to day: in onboarding, in team conversations, in the questions people ask before they click, share or download. It stops being an afterthought and becomes a core business practice, sitting alongside OH&S and compliance as something the whole team owns.

The businesses that get this right are the ones where someone kept the conversation going.

3 things to do

1

Share the basics with your team and networks.

Do not assume everyone already knows what to look for. A short conversation about phishing, passwords or MFA is worth having with every person who touches your business systems, including casual staff and contractors.

2

Enrol in Cyber Wardens training.

Visit cyberwardens.com.au to access free training designed for small businesses. Start with the Foundations course and work through it together as a team, not just as a solo exercise.

3

Make cyber a standing agenda item.

It does not need to be long. Five minutes in a team meeting to flag anything unusual, share a reminder or check in on a simple action is enough to keep it front of mind and part of how your business runs.

Looking ahead: what does a cyber-smart business look like in 2031?

By 2031, a cyber-smart small business will be prepared, confident and able to make good decisions as technology, threats and customer expectations continue to change.

Lieutenant General Michelle McGuinness, National Cyber Security Coordinator

"A cyber-smart small business will have strong security foundations, skilled and cyber-aware people, and a culture where cyber security is embedded into everyday operations. It will be confident in its use of technology, connected through trusted networks, and positioned to compete in domestic and global markets."

Kersti Eesmaa, Vertical Scope Group

"Cyber is never perfect. It is about managing the risk of cyber, not getting it 100 per cent right. For small businesses, cyber needs to become part of doing business, like insurance, workers' compensation or tax."

Adam Selwood, Cynch Security

"A cyber-smart small business will be adopting technology like it's going out of fashion. The brakes are on the car, they have the confidence, and they have the answers to the questions their stakeholders are asking. Most importantly, they can prove it."

Stephen Zappia, Revium

"Appropriate security measures that combine fit-for-purpose technology with capable people should be the vision everyone is trying to achieve. If you just focus on the technology, or you just focus on the people, you will be left behind. It has got to be both."

Madeleine Opitz, Cyber Wardens Program Lead

"A cyber-smart small business is one where cyber confidence is shared across the team. Someone knows the basics, keeps the conversation going and helps people act quickly when something does not feel right."

Together, these perspectives point to the same future: cyber-smart businesses will be the ones that build strong foundations, use technology thoughtfully, train their people and treat cyber security as part of everyday business.

Start here!

The cyber-smart checklist: your action plan for the next 12 months

Stronger cyber security is built through small, practical steps that become part of the way your business runs. Start with the actions that are free, simple and most likely to reduce your risk. Then build a regular rhythm so cyber security is always top of mind.

Do it this week — Free actions that take less than an hour

- [ ] **Turn on multi-factor authentication:** Set up multi-factor authentication, also known as MFA, on your key business accounts. Start with email, banking, cloud storage, accounting software and any platform that stores customer or payment information. MFA makes it much harder for someone to access your account, even if they have your password.
- [ ] **Update your software and devices:** Check that your business devices, apps and operating systems are up to date. Updates often include security fixes that close known gaps cyber criminals can use to get in.
- [ ] **Start Cyber Wardens training:** Visit cyberwardens.com.au and complete the Foundations training. It takes about 10 minutes and explains the basics in plain language.

Do it this month — Low-cost or free actions that take a few hours

- [ ] **Map your data:** Write down what information your business collects, stores and shares. This could include customer details, payment information, staff records, supplier contacts, passwords, booking information or business files.
- [ ] **Check who has access:** Look at who can access your business systems and whether they still need that access. Remove old staff accounts, check shared logins and make sure admin access is only given to the people who really need it.
- [ ] **Review your contracts:** Read your supplier, client and insurance documents for cyber security clauses. You may already have obligations around data protection, reporting incidents or meeting certain security standards.

Do it this year — Ongoing actions that become habit

- [ ] **Create a regular cyber check-in:** Set aside time each quarter to ask: what has changed, what needs attention and what can we fix now? Keep it short and practical. The value is in doing it regularly.
- [ ] **Run a short awareness session:** Hold at least one cyber awareness session with your team each year. Twenty minutes on spotting phishing emails, checking unusual requests or using MFA can help build safer habits.
- [ ] **Practice what you would do in an incident:** Talk through a simple scenario with your team. What would you do if you could not access your email? Who would you call if your website went down? What would happen if a staff member clicked a suspicious link? Knowing the first few steps can reduce panic when something goes wrong.

Cyber security is not a one-off task. It is a set of habits that help protect your business, your customers and your reputation over time.

CyberWardens.

Contributors

Cyber Wardens gratefully acknowledges the expert contributors whose insights and generosity shaped this guide.

- Lieutenant General Michelle McGuinness, National Cyber Security Coordinator
- Kersti Eesmaa, COO, Vertical Scope Group
- Adam Selwood, Co-founder, Cynch Security
- Stephen Zappia, COO, Revium
- Madeleine Opitz, Program Lead, Cyber Wardens

Mindset. Skillset. Toolkit.

Your cyber smart future starts now.

A Cyber Wardens Publication | 2026

Produced in partnership with COSBOA

Share this guide with a fellow small business owner.