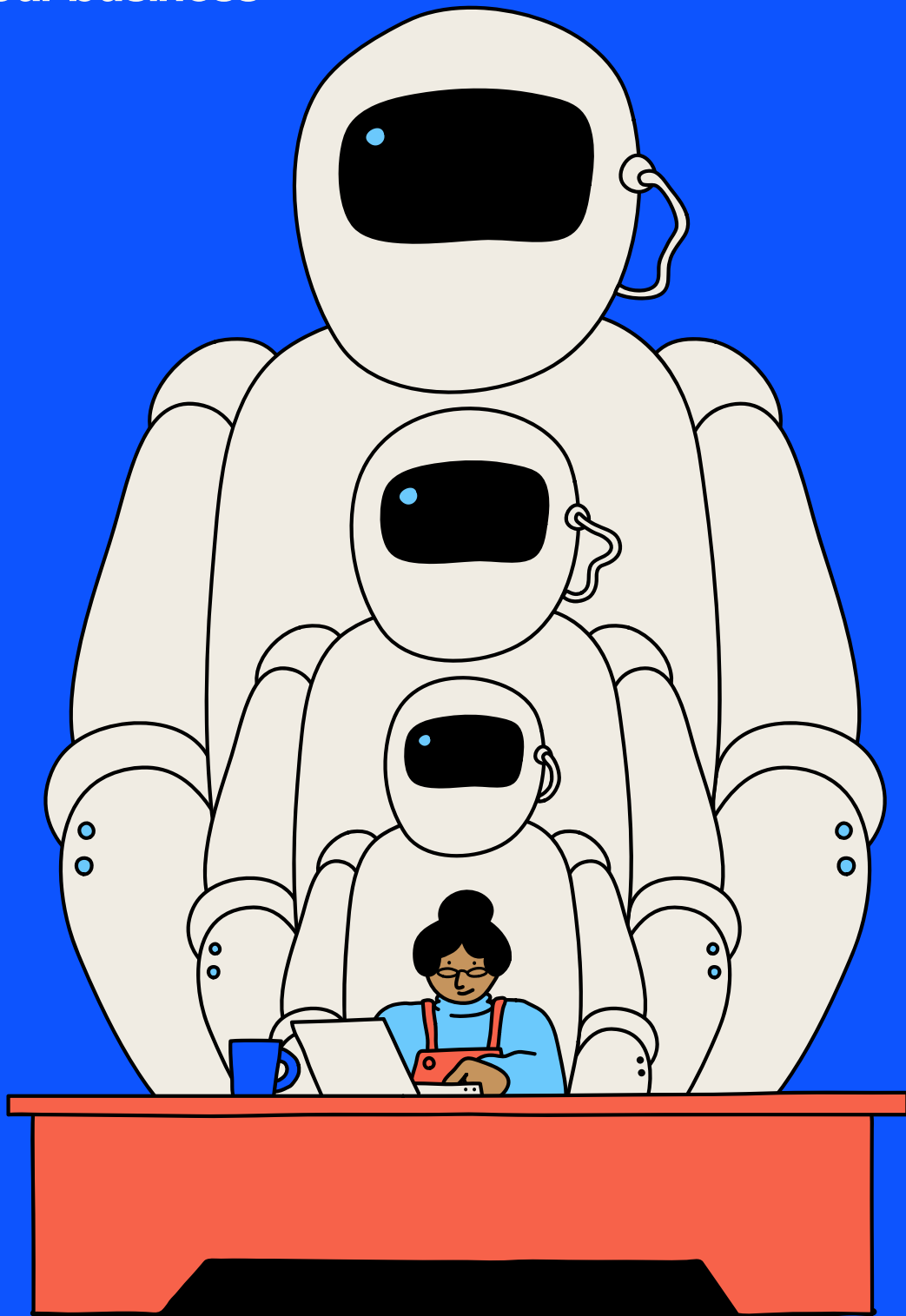


Tech State of Play

Cyber security
and your business



What's inside

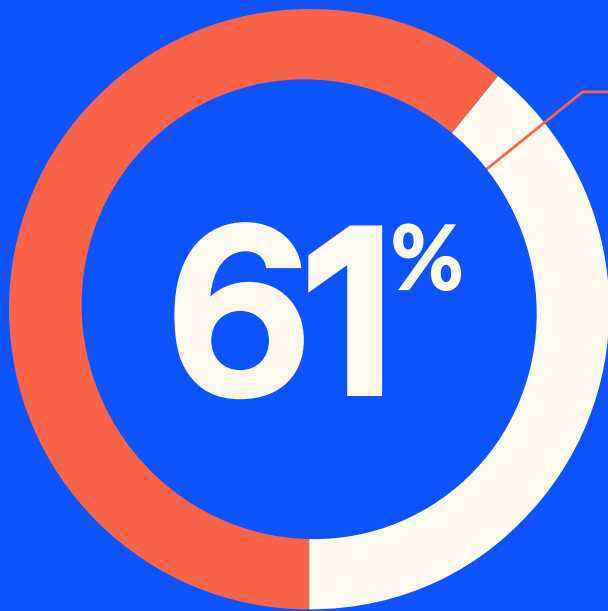
Cyber security is important to your customers	3
Check if you're under protected	5
Invest in staff training to boost security	10
Key takeaways	12
Prioritising your technology choices	13
How we can help	14

Insights in this report are taken from the **Business Tech State of Play** research study which surveyed 1,000 leaders from small and medium businesses (SMBs).

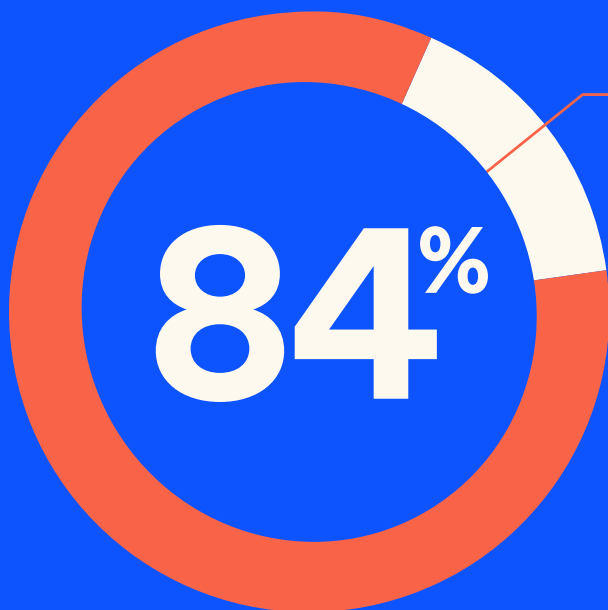
If you're anxious about cyber security risks, you're not alone. As more business functions become digitised, concern about the risks to data and privacy increase.

The majority (69%) of SMBs agree it's challenging to keep across the latest cyber security threats that could impact their business.

Almost half of SMBs think cyber attacks would have a limited impact on their customers because they don't keep sensitive customer information. But cyber criminals can be after data as simple as names and email addresses.



61% of SMBs are concerned about the risks to data and privacy that come with a greater digital presence.



84% of consumers expect that businesses will keep any personal data they provide secure.

Your business has its own risk profile that should inform your cyber security decisions. Are you on top of the cyber security basics? Easily implemented measures such as multi-factor authentication, password management and automatic software updates can go a long way to help make your business cyber resilient.

Mobile device protection is also crucial when so many of us rely on our mobile phones or tablets for doing work on the go. Yet the majority of SMBs do not have cyber security protection (e.g., anti-virus software) on work mobile devices.

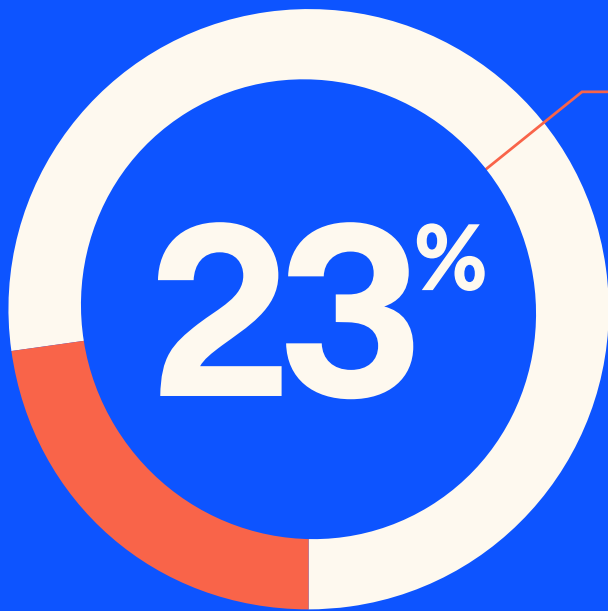
**Almost
half of SMBs
do not have
basic security
measures
in place.**

Check if you're under protected

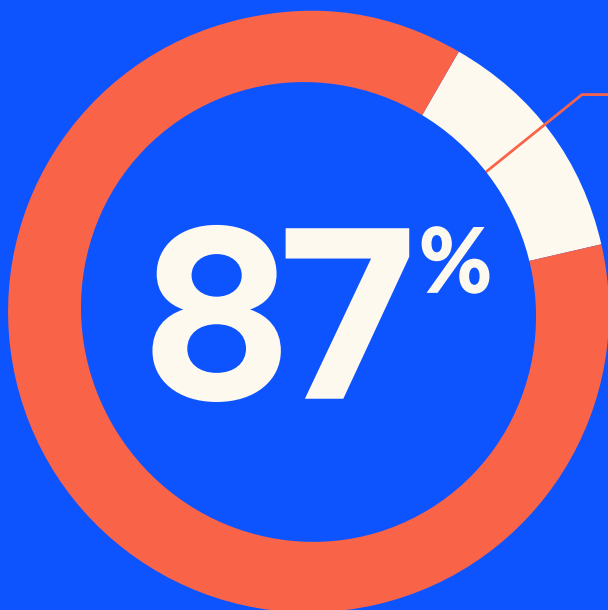
Percent of SMBs with different cyber security protection measures in place

Question: Which of the following, if any, do you have in place to protect your business from cyber security threats?

	% of SMBs
Automatic software updates	54%
Password management processes and access controls	51%
Cyber security software on work computers and laptops (e.g. anti-virus software)	50%
Cyber security protection on work mobile devices (e.g. anti-virus software)	38%
Multi-factor authentication (MFA) set up on all systems where we can set it up	36%
A back up policy that is documented and executed regularly	33%
Security solutions to protect email and collaboration tools	32%
Staff training (e.g. security awareness training)	29%
A policy on managing, securing and disposing of business and customer data	23%
A security policy relating to staff devices (mobiles or laptops) not owned by the business but used for work (i.e. BYOD)	20%
Regular cyber security drills (e.g. phishing tests)	14%
A process that manages cyber security risks when staff are leaving our business	13%
A cyber incident response plan that's documented and shared	12%
External audits or expert assessments	12%
None of these	11%



Only 23% of SMBs have a policy on managing, securing, and disposing of business and customer data.



87% of consumers would avoid dealing with a business if they thought their personal data wouldn't be kept secure.

“Security concerns and fixes are a continual focus and cost the company a lot of time and money on a continual basis.”

**CULTURAL AND RECREATIONAL
SERVICES SECTOR BUSINESS OWNER,
90 EMPLOYEES**

A cyber security breach could have significant impacts on your business reputation. But many SMB leaders aren't confident employees fully understand threats and how to keep business and customer data secure. Only 1 in 3 are investing in cyber security awareness training for staff.

Clear policies relating to cyber security, solutions to protect the devices that staff are using and training to help staff be vigilant are all important ways you can help protect your business.



Only 53% of SMBs are confident their employees fully understand cyber security threats and how to keep business and customer data secure.

Key takeaways

1

Check any obligations under regulations such as the Privacy Act in relation to any customer data you might collect. Don't assume it's not sensitive data.

2

Proactively review how you're protecting your business from cyber security threats. Prioritise *getting the basics right* and get expert help if you're not sure what else to do.

3

Ensure your staff are on top of security. Consider the devices used in your business and invest in appropriate staff training such as the free *Cyber Wardens program*.



Cyber security trends and tips for your business.

It can be hard to know what to prioritise, especially when time is at a premium. By staying focused on customer expectations, the needs of your staff and potential risks to your business, you can identify what's important for you.

Being clear about how you want to use technology and the outcomes you expect to see, can help you develop a clear plan.

Ask yourself

- 1** What's not working as well as it could?
- 2** What are other businesses like ours doing?
- 3** What changes around us do we need to adapt to?

With Telstra, you're only one hello away from a real-life tech expert. We offer a range of solutions to help you do business better online.

Bolster your business with cyber security

Make cyber safety a priority with a risk management plan that includes cyber security tools built for business.

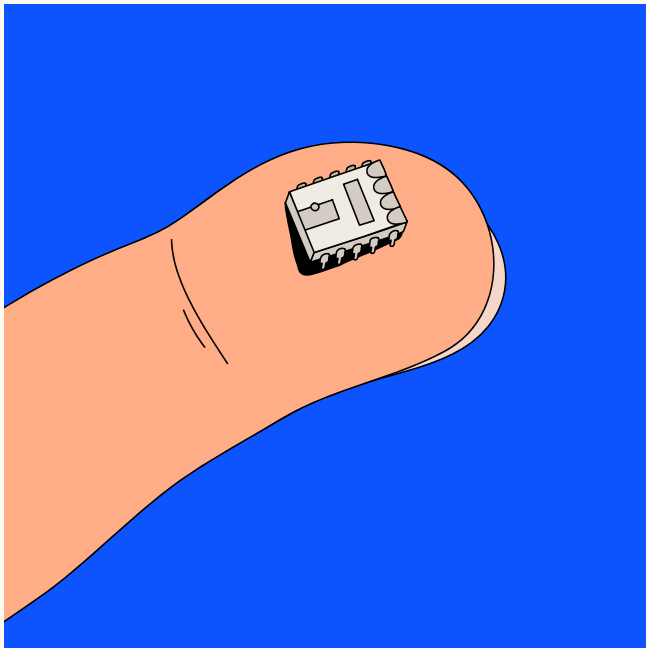
→ **Explore cyber security tools**

Professional service and advice

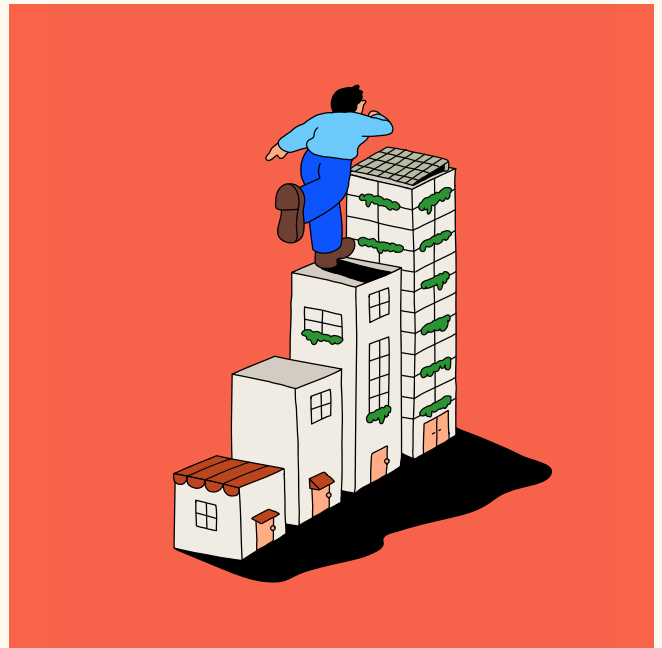
Get strategic advice and holistic technology solutions by visiting your Telstra Business Technology Centre or requesting a call back.

→ **Find my Telstra Business Technology Centre**

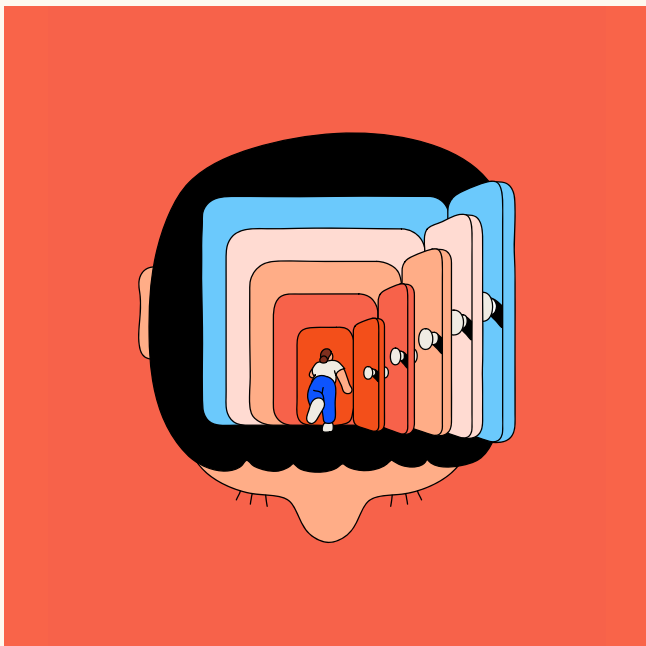
Explore more business insights and trends



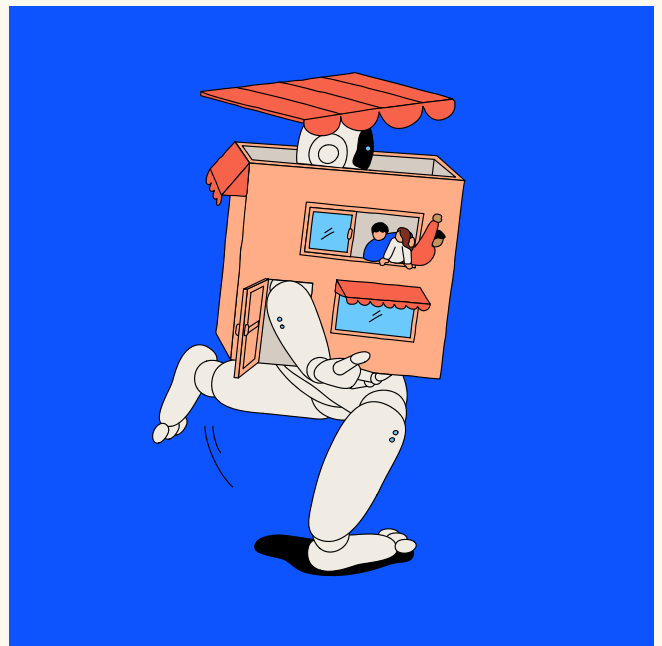
→ Insights to power your business today and tomorrow



→ Evolve with your customers



→ Ideas for unlocking goliath productivity



→ Put AI to work for your business