Cyber Security and
Business Resiliency

Tech State of Play

Welcome

As businesses grow, so do their challenges—especially in today's digital world. Striking a balance between growth and security was a significant theme in our research. Based on insights from leaders like you, this report dives into the cyber security challenges and offers practical steps to help you build resilience and stay protected.

Cyber security isn't just an issue for the IT department. It's a major business concern impacting customer trust, operations, and your business's future. At Telstra, we know how important it is to stay competitive while keeping cyber threats at bay.

Insights are drawn from the Business Tech State of Play research study with 192 owners and decision makers from businesses with 100-499 employees. The research also surveyed 1,000 Australian businesses with less than 99 employees and 1,000 Australians about how they use technology when shopping and at work.

This report is here to help you gain better insight into what other organisations, like yours, are facing, gain better visibility of what is important to your customers and provide insight into how you can protect what you've worked so hard to build. You'll find ideas to help spot vulnerabilities, strengthen your team's understanding of security, and learn why having the right partner can make all the difference in safeguarding your business.

Steve Long
Mid Market Segment Executive,
Telstra Business

Business Tech State of Play Research Study →

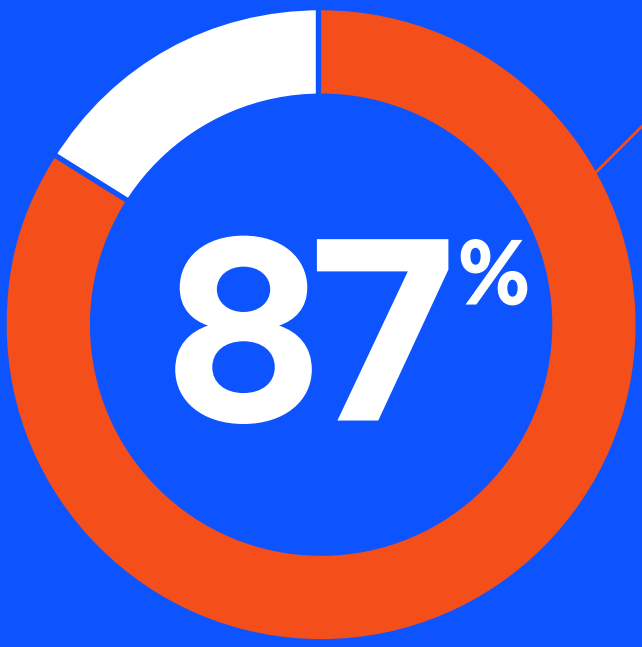
What's inside

Business insights for organisations with 100-499 employees taken from the Tech State of Play research.

Your customers' trust is one of your most valuable assets. Today, with increasing awareness about data privacy, any breach or lapse in security could significantly harm that trust.

According to our research, 87% of consumers surveyed say they would actively avoid engaging with a business if they believed their data would not be secure.

This statistic underscores the importance of cyber security as an operational concern and a key component of relationship management with your customers.

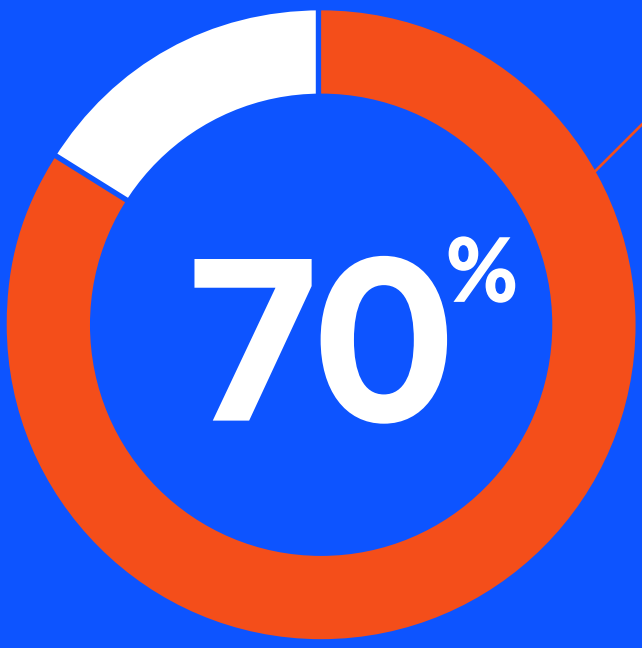


87% of consumers surveyed would avoid dealing with a business if they thought their personal data wouldn't be kept secure.

> Cyber security has kept the likes of me and many of my peers and colleagues up at night for many years. Now, with government intervention, there's this improved focus and cyber security is a bit of a shared portfolio across the business. Everyone must be well abreast of what's emanating out of the cyber security domain.
>
> Energy sector IT leader, 100-499 employees

As digitalisation becomes more embedded in every aspect of business, the scope of cyber risks has grown exponentially. A strong fear that business leaders expressed was the reputational damage to the organisation.

Seventy percent of business leaders interviewed are concerned about the impact a breach could have on how their business is perceived in the market.



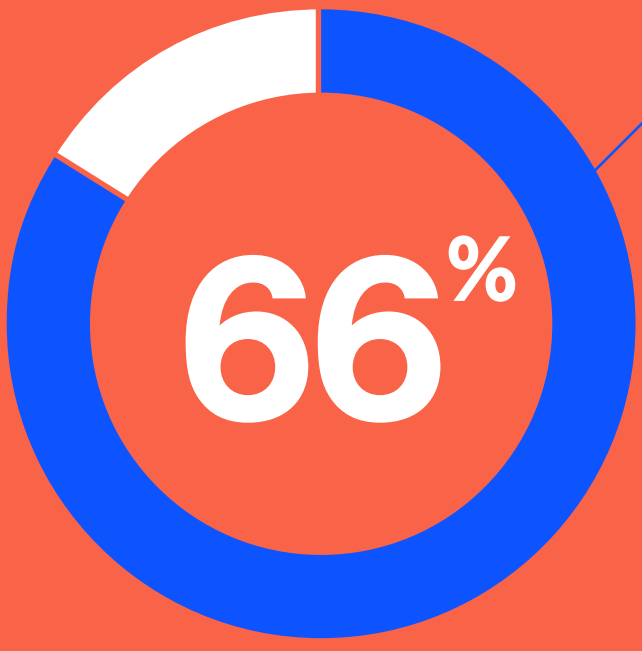
70% of business leaders surveyed are concerned about the impact a breach could have on business reputation.

Businesses that fail to protect sensitive customer data risk losing customers and facing possible regulatory fines and legal actions. Given these risks, it's no surprise that cyber security ranks as the top technology concern for business leaders today.

It is no longer sufficient to assume that basic protections will suffice—customers expect and demand robust security measures.

> Large scale issues have been visible to not just technology professionals, but the whole world. People can see how this can affect your banking, retail, supply chain, healthcare, anyone. People are starting to realise the importance of technology systems and computer systems and networks and stuff like that and how they need to protect it and have business continuity plans.
>
> Energy sector IT leader, 100-499 employees

Awareness of cyber threats has grown, yet many businesses still don't feel fully prepared. Our research found that 66% of business leaders find it challenging to keep up with the latest cyber security threats. This gap between awareness and action leaves businesses exposed.



66% of business leaders surveyed agree it's challenging to keep up with the latest cyber security threats.

The vast majority (97%) of business leaders surveyed have some form of cyber security controls in place. With most businesses reporting having on average six types of controls in place.

6 – The average number of cyber security protections in place according to businesses leaders surveyed.

The six types can vary considerably from business to business. However, the top 6 common approaches, as reported, included:

- Password management (64%)
- Cyber security software (58%)
- Staff training (58%)
- Automatic software updates (56%)
- And multi-factor authentication (52%).

It is much less common to have protection in place on staff-owned devices (42%) or have security drills for staff such as phishing tests (35%).

While it is tempting to celebrate the controls already in place, important gaps appear when we look across the full spectrum of protections that a business needs.

Looking beyond the average six protections in place, our research highlights that basic security measures aren't always in place. For example, half of the companies we surveyed (52%) use multi-factor authentication (MFA), a simple yet powerful tool to prevent unauthorised access.

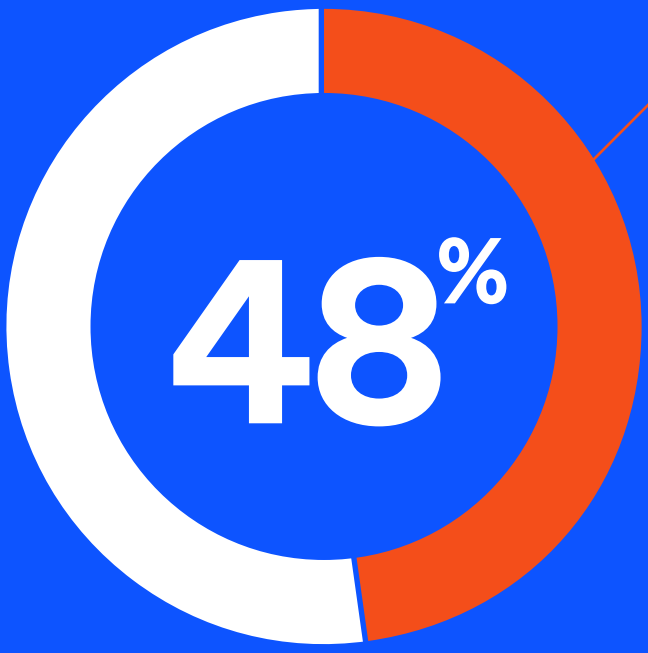
Businesses with 100 to 499 employees often have many devices and endpoints, meaning gaps like this can add unnecessary risk.

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

The basics	Password management processes and access controls.	64%
	Cyber security software on work computers and laptops (e.g., anti-virus software).	58%
	Staff training (e.g. security awareness training).	58%
	Automatic software updates.	56%
	Multi-factor authentication (MFA) set up on all systems where we can set it up.	52%
	Cyber security protection on work mobile devices (e.g., anti-virus software).	42%
	A back up policy that is documented and executed regularly.	40%
Potential gaps to assess	A policy on managing, securing and disposing of business and customer data.	46%
	Security solutions to protect email and collaboration tools.	44%
	A security policy relating to staff devices (mobiles or laptops) not owned by the business but used for work (i.e., BYOD).	41%
	Regular cyber security drills (e.g, phishing tests).	35%
	A cyber incident response plan that's documented and shared.	35%
	A process for that manages cyber security risks when staff are leaving our business.	31%
	External audits or expert assessments.	31%
	None of these.	3%

> For me the very first thing is password management, and the second thing is multi-factor authentication. These should be non-negotiable.
>
> Businesses are improving their focus around staff training and security awareness, and they have to. Even if you got your first line of defence as your password and your MFA, there are socially engineered attacks coming via email and phishing.
>
> Energy sector IT leader, 100-499 employees

Technology alone can't protect your business. Your employees are the first line of defence—and, unfortunately, they can also be your weakest link. Our research shows that only 1 in 2 business leaders feel confident that their employees fully understand how to protect sensitive data.



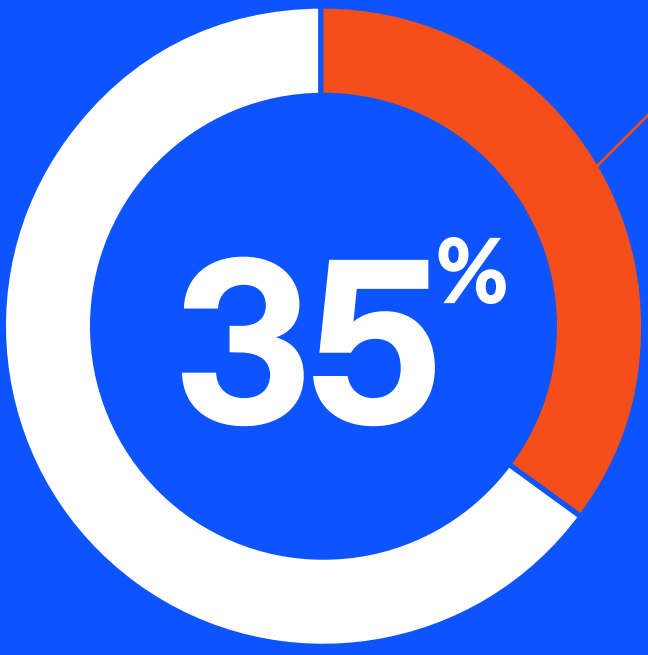
48% of business leaders surveyed are not confident that employees fully understand cyber threats and how to protect business data.

When the nature of cyber threats is constantly changing, static or dated security measures are a risk that can be mitigated.

Everyone—from entry-level employees to senior management—need to stay updated with best practices and emerging threats. Investing in regular and comprehensive staff training is an essential ongoing initiative to mitigate cyber risk.

Implementing cyber technology is not enough on its own —your people need to know how to recognise phishing attempts, handle data securely, and respond to breaches. Many organisations overlook this critical area.

Only 35% of business leaders surveyed identified having regular cyber drills (including phishing tests). With human factor being one of the primary targets for cybercriminals, this is a concern.



35% of businesses provide cyber security drills (e.g. phishing tests) regular phishing drills, according to our survey.

Our research suggests just under half (49%) of businesses surveyed manage IT 100% in-house. And when it comes to cyber security, 2 in 10 (22%) outsource this completely on an ongoing basis and around 3 in 10 (26%) get external help on an ad-hoc basis.

This data suggests that many businesses have realised that their internal teams may need more expertise or time to manage these threats.

> **With the recent hacking threats, cyber security is a major focus for our company. We have decided to outsource this to an external company to ensure we are covered properly.**
>
> Finance and Insurance sector leader, 140 employees

Cyber threats create a need to identify internal gaps, understand them, and safeguard the business from emerging and ongoing threats. Not all businesses have the resources to design and implement comprehensive strategies in-house.

That's where trusted partners can play a critical role. With deep expertise and range of cyber security solutions, Telstra can help businesses assess their current risk profile and develop a bespoke plan to cover their vulnerabilities.

Key takeaways

1 Heightened focus creates an opportunity to boost cyber protection.

Consumer expectations around data security are high, and our research highlights that business leaders feel strongly about protecting their organisation's reputation. Heightened focus on cyber security in organisations creates an opportunity to invest in the right protections because ultimately reputation is everything.

2 Closing gaps among basic protection types could be a quick win.

While businesses have various protections in place (6 on average) many are either reporting gaps or not realising gaps in what could be considered 'basic' cyber protections. Implementing relatively straightforward protections may allow your business to achieve quick wins.

3 Invest in staff training for a well-rounded cyber defence.

Cyber security is not just about technology—it's about people. If your business is one of the many that does not currently run staff training and phishing drills regularly, this could be a significant opportunity.

4 To stay ahead, businesses should seek support from expert partners.

Many businesses need access to additional expertise to manage ever-evolving cyber threats. Partnering with external specialists with scope and experience gives you access to knowledge and tools to stay ahead of potential risks and build a resilient business.

At Telstra Business, we help protect, grow and empower businesses through our people, partners and solutions, all underpinned by our secure and resilient network.

Helping businesses stay secure

Talk to your Territory Manager today about how we can help you close your security gaps and remove complexity.

Through a comprehensive security review we can provide insights, guidance and the solutions to ensure your business remains secure.

Our network of leading technology partners

Through best-in-class partnerships with leaders in global security and an extensive network of local technology partners, we're able to provide tailored support Australia-wide. Talk to your Territory Manager today, about how we can help your business stay ahead.

Explore more business insights and trends.

Read now →

Read now →

To explore any topic mentioned, talk to us today.

13 22 53

business.care@team.telstra.com