

A stressful year ahead: Top threats to Australian small businesses in 2024.

Cyber security remains a top concern for small businesses amid rising pressure across the economy.

1 February 2024: As work gets underway in 2024, the Australian small business community faces a dynamic and evolving threat landscape in the digital realm. Cyber security has never been more critical, as businesses battle high interest rates, soaring energy prices and workforce shortages.

New research from the Council of Small Business Organisations of Australia (COSBOA) and the [Cyber Wardens](#) program has revealed the top 10 concerns for small businesses in 2024.

A survey of more than 2,000 small businesses asked owners, CEOs and employees what factors they thought posed a threat to their businesses over the next 12 months. The results demonstrated the mounting pressure on small businesses as they fight to survive a cost-of-operating crisis.

Cyber security came in at number three, after energy prices and the cost of staff, and is clearly weighing on the minds of small businesses. But it is down from being the number two concern last year as cost issues take precedence.

More than half (51 per cent) of small businesses believed cyber security threats posed a medium or high risk to their business. While 18 per cent of small businesses saw cyber security threats as a high risk, this increased for specific groups, including owners, CEOs and founders (22 per cent), small businesses delivering sales and services online (26 per cent), and those in the business (26 per cent) and IT sectors (33 per cent).

However, four in 10 small businesses also said they had no or low confidence in how to prepare for a cyber incident (37 per cent) or how to recover from a cyber incident if it occurred (40 per cent).

“We know that 2024 will be another challenging year for small business with economic headwinds ahead,” COSBOA CEO Luke Achterstraat said.

“This new data reveals the real challenges facing small business with 54 per cent of respondents worried about energy prices and 52 per cent worried about the cost of staff.

“It is important for small businesses to remain aware of the increasingly acute risk of cyber attacks. Investing in cyber security training and tools is essential to help protect your small business, staff and clients.

“Our Cyber Wardens program can help give small business owners the skills to help mitigate the risks, reducing one of the many worries they are facing.”

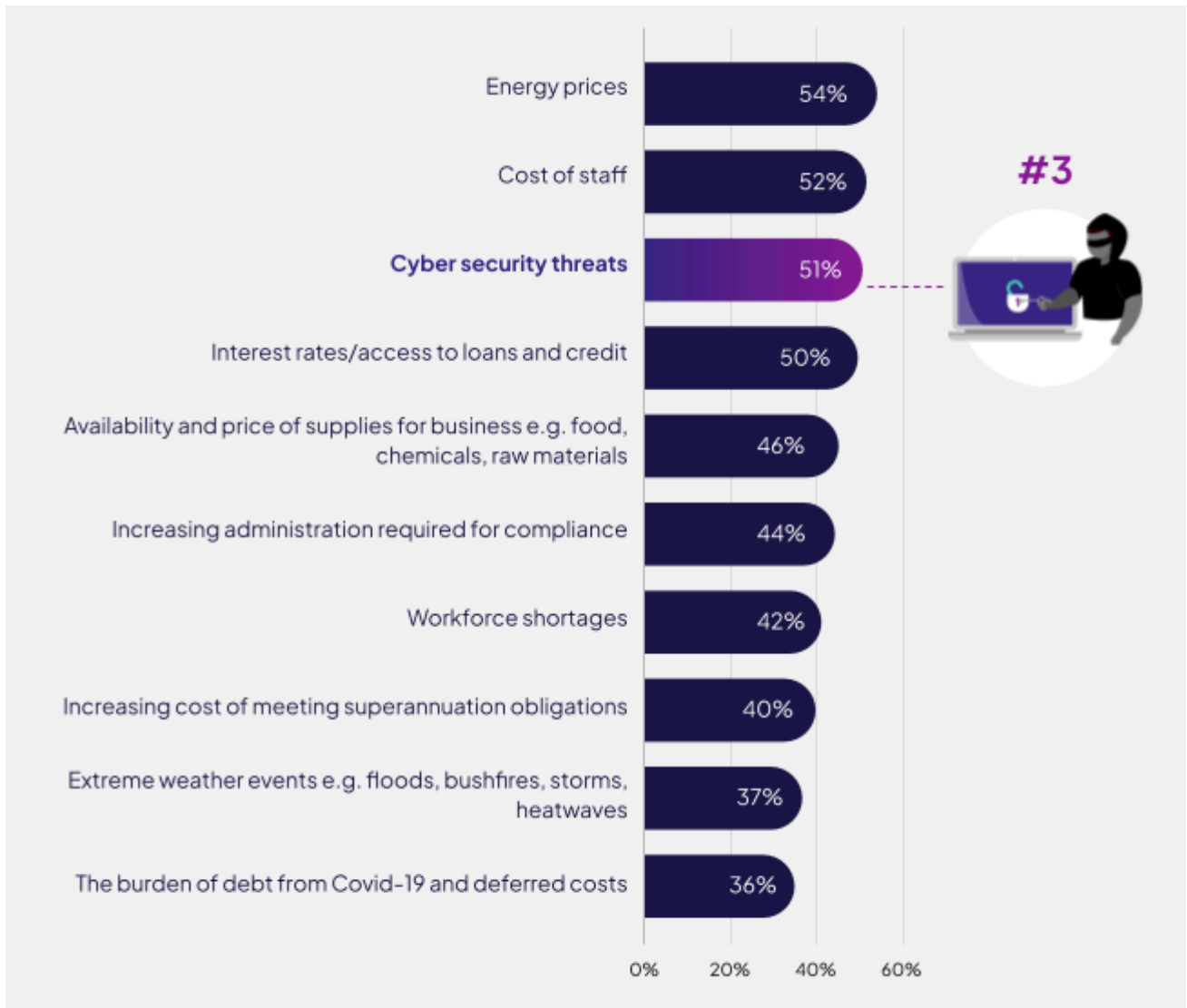


Table: percentage of small businesses that perceived these ‘threats’ as a medium or high risk to their business in the next five years.

Size matters

Compared to micro and mid-size small businesses, sole traders were more likely to say they had no or low confidence in their knowledge of how to fight a cyber attack (49 per cent) or where to get help when a cyber incident occurred (38 per cent).

Small businesses in their first year of operating were also less prepared, with more than five in 10 (54 per cent) having no or low confidence about how to recover from a cyber incident. Small businesses in their first year of operating were also much more likely to report that cyber security had never been discussed in their workplace (44 per cent, compared to 27 per cent of small businesses generally).

Almost half (49 per cent) of sole traders thought it was too time-consuming for small businesses to practise cyber security on top of everything else and more than four in 10 (44 per cent) believed it was more important for medium and larger businesses to practise cyber security than it was for small businesses.

The extent to which small businesses were concerned about the risk of cyber attacks varied depending on the type of business. The survey revealed that while nearly six in 10 'scale up' or growing small businesses (58 per cent) were concerned about cyber attacks, only four in 10 'side hustle' small businesses (40 per cent) had the same concerns. Similarly, 'start-up' and 'scale-up' small businesses were more likely to be talking about cyber security at least twice a year (83 per cent and 80 per cent, respectively) compared to home-based businesses (59 per cent).

"Cyber security is important for every small business — that includes sole traders, side hustles and micro businesses. It doesn't matter whether you work in the office or from home, whether you're growing or shrinking, you still need to take steps to protect your business," Mr Achterstraat said.

"The latest Australian Signals Directorate's (ASD) [Annual Cyber Threat Report](#) revealed the average cost of cyber crime per incident had risen by 14 per cent to \$46,000 for small businesses. That would be terminal for most small businesses.

"Together, we can strengthen the cyber security skills of Australian small businesses and protect our economic backbone."

Cyber Wardens urges small businesses to take proactive steps to protect themselves, their customers and their futures.

The free, Australian Government-funded Cyber Wardens program provides training to small business owners and employees on how to digitally safeguard their businesses. This includes essential upskilling on the fundamentals of multi-factor authentication, password management, device updates and backups.

According to Scamwatch, Australians lost more than \$429 million to scams in 2023, with phishing, false billing, online shopping scams, and identity theft being the most commonly reported scams.

Last year the ACCC reported the number of businesses losing money to scams had increased by 73 per cent.

For more information, please visit www.cyberwardens.com.au

ENDS

Background

About Cyber Wardens

At Cyber Wardens, we are on a mission to ensure Australian small businesses operate in a cyber-safe environment.

By bolstering the cyber capabilities of people who work in small businesses, we make it easier for small businesses to increase their cyber posture to prevent attacks and be resilient to them. Our goal is simple — for cyber criminals to consider Australia 'closed for business'.

Cyber Wardens is a national initiative of the Council of Small Business Organisations of Australia (COSBOA), supported by the Australian Government and an industry alliance led by Telstra, CommBank and the Australian Cyber Security Centre, to help protect Australia's 2.5 million small businesses from online threats.

Cyber Wardens are the digital equivalent of first aid officers or fire safety wardens. They are equipped to prevent, prepare, fight and help recover from a cyber attack such as the theft of customer data or intellectual property.

Just as we physically protect ourselves by locking up our businesses and homes at night, the Cyber Wardens program will give small businesses the skills to shut their digital doors to lurking cyber threats.

Leveraging COSBOA's grassroots infrastructure and reputation to change the behaviours of Australia's 2.5 million small businesses, the free Cyber Wardens program uplifts small businesses by educating an in-house cyber safety officer to build cultural competencies alongside technical know-how.

By bolstering the cyber capabilities of people who work in small businesses, we make it easier for small businesses to prevent and recover from cyber-attacks.

Cyber Wardens will complement Australia's growing pool of cyber technical experts to drive cultural change and cyber-safe mindsets in Australia's small businesses.

The Cyber Wardens program works in conjunction with two new initiatives recently announced by the Albanese Government: \$7.2 million to establish a voluntary cyber health-check program that will allow businesses to undertake a free, tailored self-assessment of their cyber security maturity, and \$11 million in the Small Business Cyber Resilience Service which will provide one-on-one assistance to help small businesses navigate their cyber challenges, including walking them through the steps to recover from a cyber attack.