Small doesn't mean you are safe from a big problem

By Luke Achterstraat

The Daily Telegraph
Wednesday 27th March 2024
625 words
Page 13 | Section: OPINION
260cm on the page


James Morrow
Labor loses on credibility when it comes to detainees

Small doesn't mean you are safe from a big problem

Luke Achterstraat

A week ago, the Australian Securities and Investment Commission released its monthly business insolvency statistics which showed almost 1000 Australian businesses went bust in February.

It didn't generate headlines on our nightly news. But it should.

With the highest monthly rise in business insolvencies since October 2015, our economy is on a trajectory to equal or exceed Australian businesses' "annus horriblis" of 2022-23 in which almost 8000 businesses entered administration or had a controller appointed to them.

For most small business owners, the thing that keeps them awake at night is identifying the tipping point between solvency and insolvency.

According to almost 2100 small to medium business owners surveyed by the Council of Small Business Organisations Australia (COSBOA) and Cyber Wardens, their top three concerns for 2024 are energy prices, the cost of staff and cyber security threats.

For the average small business owner captive to the regulated markets of energy and labour, there is not much they can do to mitigate rising energy and labour costs apart from factor it into their forward projections and hope for the best.

Cyber threats are another matter. The average cost of a single cyber attack is $46,000, according to the Australian Signals Directorate Cyber Threat Report 2022-2023. For some small businesses that surprise $46,000 cyber attack could be the tipping point between staying alive and going broke.

On Monday, 100 industry leaders and small business owners met in Canberra to learn about these research findings and collaborate on building the cyber capabilities of Australian small businesses. For example, most small businesses (61 per cent) are not talking about cyber security regularly, which further increases the risk they face.

We need to take control of one of the biggest threats to the sector, which is Australia's largest employer, representing five million people and contributing $418 billion to Australia's GDP.

Large-scale cyber attacks such as those directed at Optus and Medibank elevated awareness of cyber crime among consumers but it has had a counter effect on small businesses. There is a fallacy that small is safe.

While seven in 10 (67 per cent) small business owners/CEOs and employees report major cyber attacks on big companies have made them think more about cyber security, only a third (35 per cent) feel vulnerable to attack due to being a small business.

About four in 10 (38 per cent) still think it's much more important for medium and larger businesses to practise cyber security than it is for small businesses.

All of us are at risk of a "little fish" mentality, whether we are a small business owner, an employee, a supplier or a contractor.

In the words of one of our business owners: "I wouldn't think my business would be a target. I suppose I see myself as such a little fish. I'm sure there'd be a shark that would be meatier and would be able to provide cyber criminals with a lot more."

The good news is almost nine in 10 small business owners and employees (86 per cent) are keen for a program that simplifies cyber security and renders it attainable for businesses of all sizes.

That's why the Australian Government, with Telstra, CommBank and COSBOA, have developed Cyber Wardens which is a free online training course. It takes 45 minutes to complete on any device, is free to all Australian small businesses and you don't have to be tech-savvy or an IT wizard to understand it.

As a nation, we need a cyber reality check. Cyber security education gives all of us the skills to shut our digital doors to lurking cyber threats.

Luke Acterstraat is CEO of the Council Of Small Business Organisations Australia