accountantsdaily BULLETIN

Average cyber crime costs a small business $40k

TECHNOLOGY

With an online threat every seven minutes, attacks are up 13 per cent and Australia has become a favourite target.

By Philip King•07 November 2022•5 minute read

Each cyber crime costs a small business $40,000 on average and the number of attacks leapt 13 per cent last year to the equivalent of one every seven minutes, the Australian Cyber Security Centre reveals in its 2021-22 report.

Australia was a gold mine for cyber criminals it said, with the highest median adult wealth in the world, and while “destructive” ransomware had stolen the headlines recently more prosaic threats such as fraud and online banking scams were much more common.

“Australia’s prosperity is attractive to cybercriminals,” the report said, highlighting the increase in documented attacks to 76,000 during 2021-22.

“Ransomware groups have further evolved their business model, seeking to maximise their impact by targeting the reputation of Australian organisations.

“In 2021–22, ransomware groups stole and released the personal information of hundreds of thousands of Australians as part of their extortion tactics. The cost of ransomware extends beyond the ransom demands, and may include system reconstruction, lost productivity, and lost customers.”

But it said cyber crimes directed at individuals, such as online banking and shopping compromise, remained the most common.

Small businesses lost an average of $39,555 while the Professional, Scientific and Technical Services sector, which includes accounting, was the sixth most targeted with 7 per cent of all incidents.

However, medium-sized businesses with 20-199 employees lost the most on average, at $88,407, against $62,233 for large organisations.

The ACSC said this could be because “they were less likely than large organisations to apply cyber security mitigations”.

But it said at least 150,000 to 200,000 devices in homes and small businesses were vulnerable and those users should follow its step-by-step guides on securing data.

It also highlighted an AFP initiative, Operation Dolos, that works with small and medium businesses that have been targeted by a business email compromise attack to counter the international criminals typically involved. These attacks were increasingly aimed at high-value transactions like property settlements, it said.

Deputy Prime Minister and Minister for Defence Richard Marles said the increased attacks reflected global strategic competition and “regrettably, too many Australians have also felt its impacts”.

“The government considers cyber security and reinforcing our online resilience to be a national priority,” he said.

The ACSC said an strike on Australia’s critical infrastructure could put access to essential services at risk although potential disruptions in 2021–22 were largely averted by effective cyber defences, including network segregation and effective, collaborative incident response.

However, government bodies – state and federal – experience the most security incidents and accounted for one in three of the total.

ATO Second Commissioner Jeremy Hirschhorn recently revealed that the body was hit by up to 3 million attempted cyber hacks per month and said criminals were getting smarter about the way they gathered information for identity theft.