**MEDIA RELEASE**

**FOR IMMEDIATE RELEASE**

**Five signs your small business may be targeted cyber criminals**

* A cyber crime is reported [every 10 minutes](https://www.cyber.gov.au/sites/default/files/2020-07/ACSC%20Small%20Business%20Survey%20Report.pdf) in Australia.
* [15% of Australians](https://www.bizcover.com.au/cyber-liability-insurance/) would stop dealing with an organisation if their data were breached.
* [Cyber Liability insurance](https://www.bizcover.com.au/cyber-liability-insurance/) helps protect small businesses from claims in the event of a cyber breach.

With cyber security and cyber crime dominating the news cycle in recent weeks, small business owners are being reminded that cyber criminals don’t discriminate, and no business is too small to fall victim to cyber crime.

While small business owners may assume that they aren’t attractive targets for cyber criminals, the fact is that all businesses can be targeted by cyber criminals. As such, a healthy respect for the risks and potential dangers cyber crime can pose to small business owners may be warranted. And alarmingly, [more than 60 per cent](https://insidesmallbusiness.com.au/technology/cyber-security/small-businesses-at-risk-of-exposure-in-the-wake-of-optus-cyber-breach) of Australian SMEs never fully recover from a cyber attack or a data breach.  
  
**How to spot the warning signs of a pending cyber attack**

Cyber crimes can be difficult to prevent before they occur, and difficult to identify once they’ve happened. However, there are certain specific traits and qualities that can make some small businesses more susceptible than others to being targeted by cyber criminals. Let’s look at each warning sign and why each can be attractive for cyber criminals.

**#1: Your small business collects personally identifiable information**

Small business owners may assume that they don’t have customer data that’s worth stealing. However, smaller organisations can be attractive targets for cyber criminals because they collect customer data just like large corporations do, but they typically don’t have the regimented [cyber security](https://www.bizcover.com.au/cyber-security-for-small-business/) provisions of large corporations in place.

Small businesses that collect and store sensitive customer data – such as first and last names, home addresses, and email addresses – may be attractive targets for cyber criminals.

**#2: Your small business processes financial transactions online**

Any business or organisation that processes financial transactions online can be targeted by cyber criminals. Whether your small business is an online retailer, a charity organisation, or another entity that accepts online payments or donations, you may be targeted by cyber criminals who want the financial data that your small business stores online.   
  
Financial information is considered so valuable that cyber threats specifically targeting online stores – called ‘e-skimming’ – have emerged in recent years. E-skimming occurs when a cyber criminal hacks into a store’s web server and intercepts financial transactions in progress.

**#3: You have employees**  
  
When it comes to small businesses and cyber security, often it can be your own people who are your weakest link. If your small business has employees or volunteers who use technology in your workplace to perform their job, they need to understand and adhere to the cyber security processes and protocols you have put in place for your business.

Your employees or volunteers can pose cyber risks to your small business because without even being aware of it they may bring poor cyber safety practices into your place of business. Your business may have regimented and well-planned cyber security protocols in place – but that can all be undone by human error.

Small business owners may reduce this risk by including cyber security protocols in their employee onboarding process, while also considering [business insurance](https://www.bizcover.com.au/business-insurance/) such as [Cyber Liability insurance](https://www.bizcover.com.au/wp-content/uploads/2019/12/BC1243_FactSheet_CyberLiability_Nov19_FINAL-5.pdf)\*.

**#4: Your business engages third-party vendors**

Supply chain attacks can present major risks for small businesses – so much so that small business owners that work with third-party vendors may consider reducing their risk from third-party vendors. While your business may have cyber security systems and processes in place, your third-party vendors may not, which could expose your business to cyber threats

**#5: You have a remote workforce**

The Covid pandemic forced changes to the ways most workforces collaborate. Now on any given day many of your staff may work remotely – whether that be in their own home, in a café, in their holiday home, or on the road. While this can be great for your staff, from a cyber security perspective it also needs to work for your business.  
  
Enabling your employees to work remotely and use their personal devices for work purposes can be great on paper for both employers and employees. But from a cyber security it needs to work for you as the business owner.

**How are you managing your cyber risk?**

With cybercrime in the headlines, now may be the perfect time for small business owners to review their risk management strategy for cyber attacks, which may include business insurance such as [Cyber Liability insurance](https://www.bizcover.com.au/cyber-liability-insurance/).  
  
Remember – no business is too small to be targeted by cyber criminals.

*\*This information is general only and does not take into account your objectives, financial situation or needs. It should not be relied upon as advice. As with any insurance, cover will be subject to the terms, conditions and exclusions contained in the policy wording.*   
© 2022 BizCover Pty Limited, all rights reserved. ABN 68 127 707 975; AFSL 501769.

ENDS   
  
**ABOUT BIZCOVER**

BizCover is Australia’s largest online business insurance service for SMEs. Operating globally in Australia, New Zealand and the US, more than 180,000 SMEs currently protect their business through BizCover’s proprietary platform.

BizCover allows SMEs to compare multiple free quotes from multiple insurers offering small business owners the option to choose from competitive market rates, purchasing online and getting policy documents delivered instantly.

To date, over one million business insurance policies have been sold through the BizCover platform globally partnered with a panel of leading global insurers. BizCover also provides market-leading solutions to the General Insurance Broking Industry including [BizCover for Brokers](https://bizcoverforbrokers.com.au/) and ExpressCover.

**To learn more about BizCover visit** [**bizcover.com.au**](https://www.bizcover.com.au)**.**

**Media enquiries to:**

Sharon Kenny

Head of Marketing  
M: 0403 048 084