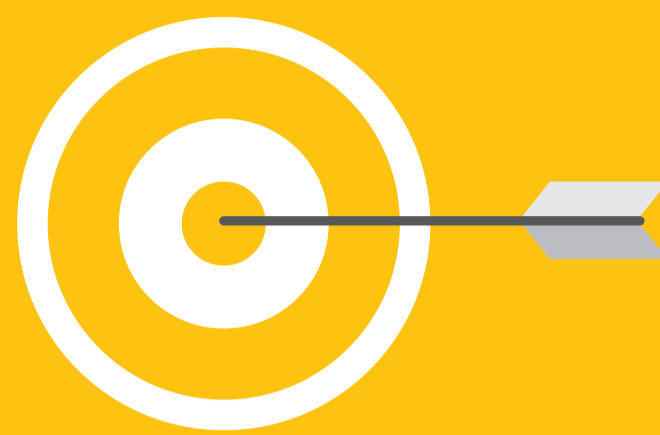


THE NUMBERS: CYBERATTACKS ON AUSTRALIAN SMALL BUSINESS

ALMOST **1 IN 5**
AUSTRALIAN SMBs
HAVE BEEN
TARGETED BY A
CYBERATTACK



24% OF SMBs IN AUSTRALIA DO NOT HAVE AN INTERNET SECURITY SOLUTION



1 IN 3
SMBs

BELIEVE THEY WOULDN'T
LAST A WEEK WITHOUT CRITICAL
BUSINESS INFORMATION

! FILE NOT FOUND

63%
DID NOT RECOVER
DATA LOST
IN AN ATTACK

OF THE BUSINESSES
WHO HAD EXPERIENCED
A CYBERATTACK:

52% 

HAD FALLEN TO AN EMAIL
OR PHISHING SCAM

28% 

WERE THE VICTIM OF A
RANSOMWARE ATTACK

100 DOLLARS 
AVERAGE FINANCIAL LOSS
PER ATTACK
AUD\$6,600



MAIN IMPACT
OF CYBERCRIME:

40%
DOWNTIME

26%
EXPENSE FOR
RE-DOING WORK

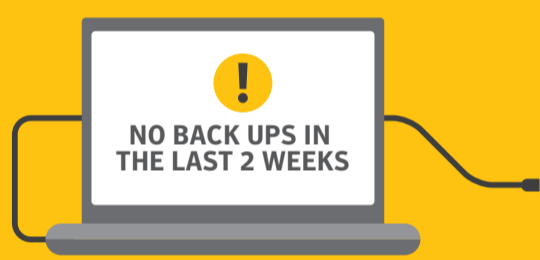
24%
INCONVENIENCE

22%
PRIVACY BREACH

16%
FINANCIAL LOSS

15%
DATA LOSS

BACK UP & RECOVERY



1 IN 4
SMALL BUSINESSES BACK UP
THEIR BUSINESS DATA NO MORE
THAN ONCE A MONTH

28%
OF SMBs NEED TO RETRIEVE
LOST DATA ON AT LEAST A
MONTHLY BASIS



SMBs HELD TO RANSOM

JUST OVER **1 IN 10 SMBs**
HAVE BEEN AFFECTED BY A
RANSOMWARE ATTACK



JUST OVER ONE THIRD
OF BUSINESSES AFFECTED
BY A RANSOMWARE ATTACK
PAID THE RANSOM

AVERAGE RANSOM PAID:

AUD \$ **4677**

8% OF THOSE WHO PAID, DID NOT GET THEIR FILES BACK



FROM THE EXPERTS: SECURITY TIPS AND TRICKS

**Don't wait until
it's too late to know
your business**

Don't wait until you've been hit by a cyberattack to think about what you should do to help secure your information. Learn the risks, review your business practices and identify security gaps that you can start to address before it's too late.

**Invest in security
and backup**

To reduce the risk of being hit by a cyberattack, implement comprehensive security software such as Norton Security for Professionals or Norton Small Business, and use backup solutions to help safeguard business critical data.

**Keep
up-to-date**

Ensure all your company devices, operating systems, software and applications are always up to date with the latest versions and patches to reduce the risk of being exposed to security vulnerabilities.

**Get employees
involved**

All employees should be vigilant and know how to spot phishing scams, ransomware attacks and be aware of which sites they can visit on their work devices. Small businesses should invest in educating employees so they become your best line of defence against cyberattacks, not your weakest link.

**Use strong
passwords**

Use unique passwords for all your devices, accounts and WiFi networks, change them every three months and don't reuse them. Consider using an online password manager like Norton Identity Safe as an added layer of protection.

To start protecting your business
visit au.norton.com/small-business

