NORTON SMB CYBERSECURITY SURVEY

Australia

Norton by Symantec

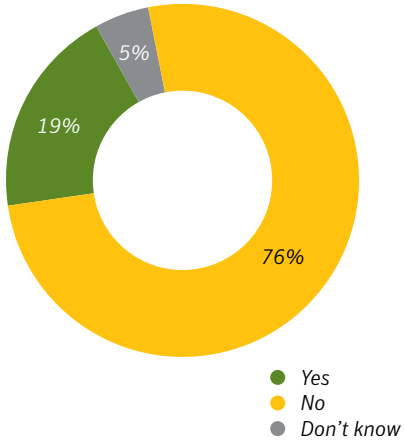
CONTENTS

SMB CYBERSECURITY SNAPSHOT

NORTON SMB CYBERSECURITY SURVEY

This report presents the summary findings of Norton's SMB Cybersecurity Survey, which aimed to get an understanding of cybersecurity perceptions and practices amongst small to medium businesses (SMBs) across Australia. The survey findings have been released to help raise awareness about the security risks many Australian small businesses are exposed to, and provide insights into the measures business owners can take to help mitigate those risks to improve the security of their business.

BUSINESSES AFFECTED BY CYBERATTACK



1 in 5

SMBs have been targeted by a cyberattack

The survey found that ***almost one in five (19 percent)*** have been targeted by a cyberattack. More than one in 10 SMBs (11 percent) have been affected by a ransomware attack and over one-third (34 percent) of businesses are paying up.

Companies that are more likely to have seen an increase in cyberattacks tended to be larger SMBs (22 percent), SMBs with a revenue of $1 million or more (24 percent), and those affected by a cyberattack in the past (41 percent).

SMBs that experienced a cyberattack were most likely to have been attacked within the last two years (84 percent), with almost half (46 percent) having experienced an attack within the last 12 months. The main sources for these attacks came from email or phishing scams (52 percent) and ransomware attacks (28 percent). Not surprisingly, hackers accessing company information was seen as the biggest threat to security for Australian SMBs.

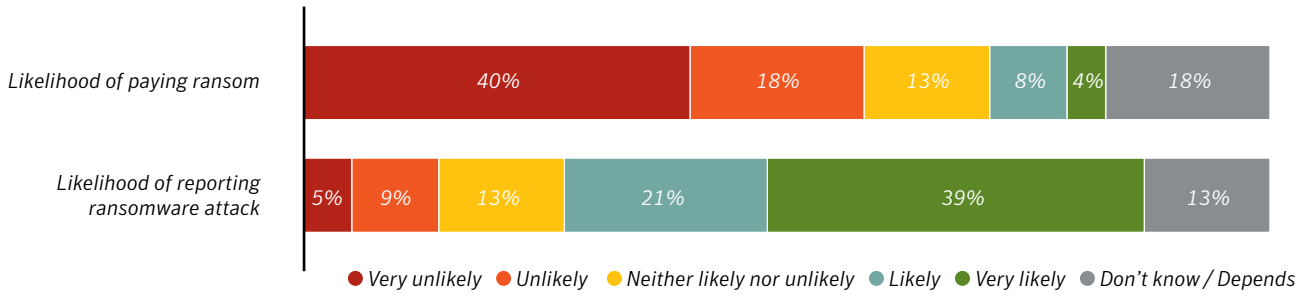
SMBs HELD TO RANSOM

Ransomware prevents or limits users from accessing their system unless a ransom is paid

Just over one in 10 SMBs (11 percent) had been impacted by a ransomware attack, and just over one third of businesses affected (34 percent) paid the ransom, which, on average, amounted to AUD$4,677 and 8 percent of those who paid did not get their files back.

11%

of business operators had been affected by a ransomware attack



Businesses more likely to have suffered a ransomware attack included: businesses with a revenue of $1 million or more (20 percent), construction and trades businesses (19 percent), businesses with a server (14 percent) and business operators aged under 40 years (17 percent).

Three out of five (61 percent) business operators are likely to report a ransomware attack to the police or relevant authorities, and 58 percent would not likely pay the ransom.

Interestingly, businesses which had previously been impacted by a cybersecurity threat are more likely to pay the ransom (22 percent).

61%

of business operators are likely to report a ransomware attack

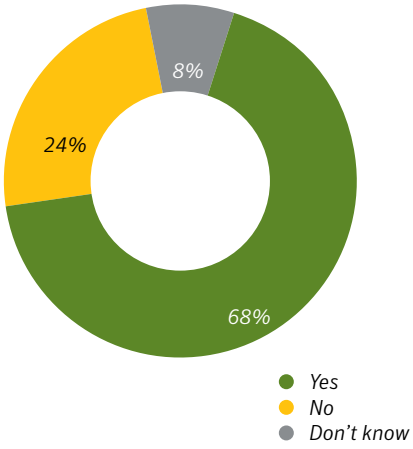
ADOPTION OF INTERNET SECURITY SOLUTIONS

Almost a quarter of small businesses have no Internet security solution, *many have no professional IT support and little interest in cyber insurance*

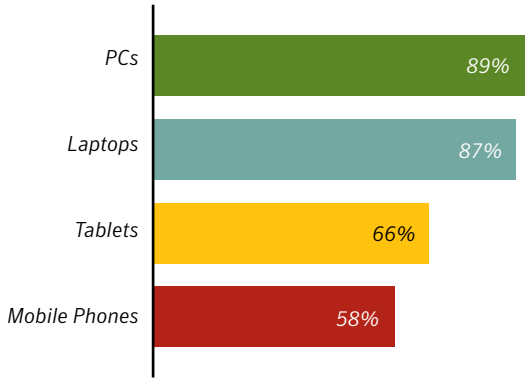
The survey found that **24 percent of Australian SMBs do not have an Internet security solution**. The main reason business operators gave for forgoing Internet security was that it was not a priority for their business (39 percent).

Even those businesses with Internet security are taking risks with their critical business information. While 89 percent of PCs and 87 percent of laptops are secured, that percentage drops to 66 percent for tablets and 58 percent for mobile phones.

SMB USE OF INTERNET SECURITY



AVERAGE USE OF INTERNET SECURITY SYSTEM BY DEVICE



MOST PREVALENT CYBERATTACKS

The survey reported email or phishing scams (52 percent) are the most prevalent cyberattacks that Australian SMBs had fallen victim to, with hacking attempts (35 percent) and ransomware scams (28 percent) also common.

Type of Cyber Threat	
Email or phishing scam	52%
Hacking attempt	35%
Ransomware scam	28%
Privacy or data breach	14%
Online identity fraud	10%
An employee posting confidential information on a social networking site	12%
An internal threat such as employee stealing data on USB key or leaking information to competitors	8%
An accidental loss of a laptop or mobile device or well-meaning employee distributing confidential data unintentionally	7%

52%

of the businesses who had experienced a cyberattack had fallen to an email or phishing scam

Downtime the main impact of a cyber security threat

Of the small business operators impacted by a cyberattack, downtime emerged as the main impact of a cybersecurity threat (40 percent), followed by expense for re-doing work (26 percent), inconvenience (24 percent), financial loss (16 percent) and data loss (15 percent).

Of those that had lost data, almost two-thirds (63 percent) had not been able to recover it, while the average financial loss caused per attack was just under AUD $6,600.

Impact of Cyber Threat	
Downtime	40%
Additional time and expense for re-work	26%
Inconvenience only	24%
Privacy breach	22%
Financial loss	16%
Lost important business information or data	15%
Reputational damage	13%
There was no damage done to the business	21%

BACKUP AND RECOVERY

Almost 1 in 4 small businesses back up their data no more than monthly

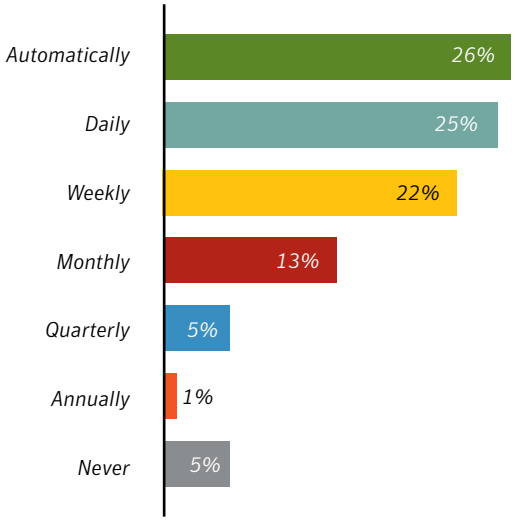
One in four (24 percent) small businesses back up their business data no more than once a month and amongst micro-SMBs the figure is even higher with 33 percent backing up no more than monthly.

A similar number (28 percent) are required to retrieve lost data such as emails or deleted files on at least a monthly basis, and almost one third of SMBs did not think they would last a week without critical business information, highlighting the importance of a robust and regular backup system.

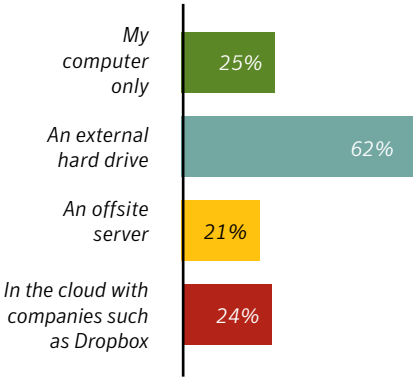
Businesses who did backups were most likely to back up to an external hard drive (nominated by 62% of business operators who performed backups), while only 24% are using a cloud provider for their backups.

A quarter of respondents backed up to their own computer, and of these 48% did not backup anywhere else leaving themselves vulnerable to complete loss of data.

FREQUENCY OF DATA BACKUP



WHERE IS DATA BACKED UP



Almost a third of businesses did not think they would last a week without critical business information

Time business could last without access to critical information	Total
One day	11%
One week	20%
One month	16%
2-3 months	8%
4-6 months	4%
7-12 months	2%
More than a year	20%
Don't know	20%

FROM THE EXPERTS: SECURITY TIPS AND TRICKS

As attackers evolve, ***there are many steps businesses can take to protect themselves.*** *As a starting point, Norton recommends the following best practices:*

1. **Don't wait until it's too late to know your business:** It's tough running a small business at the best of the times and sometimes businesses overlook things until it's too late. Businesses shouldn't wait until they've been hit by a cyberattack to think about what they should have done to secure their information. Not only is downtime costly from a financial perspective, but it could mean the complete demise of a business. SMBs need to begin understanding the risks and the security gaps within their business before it's too late.

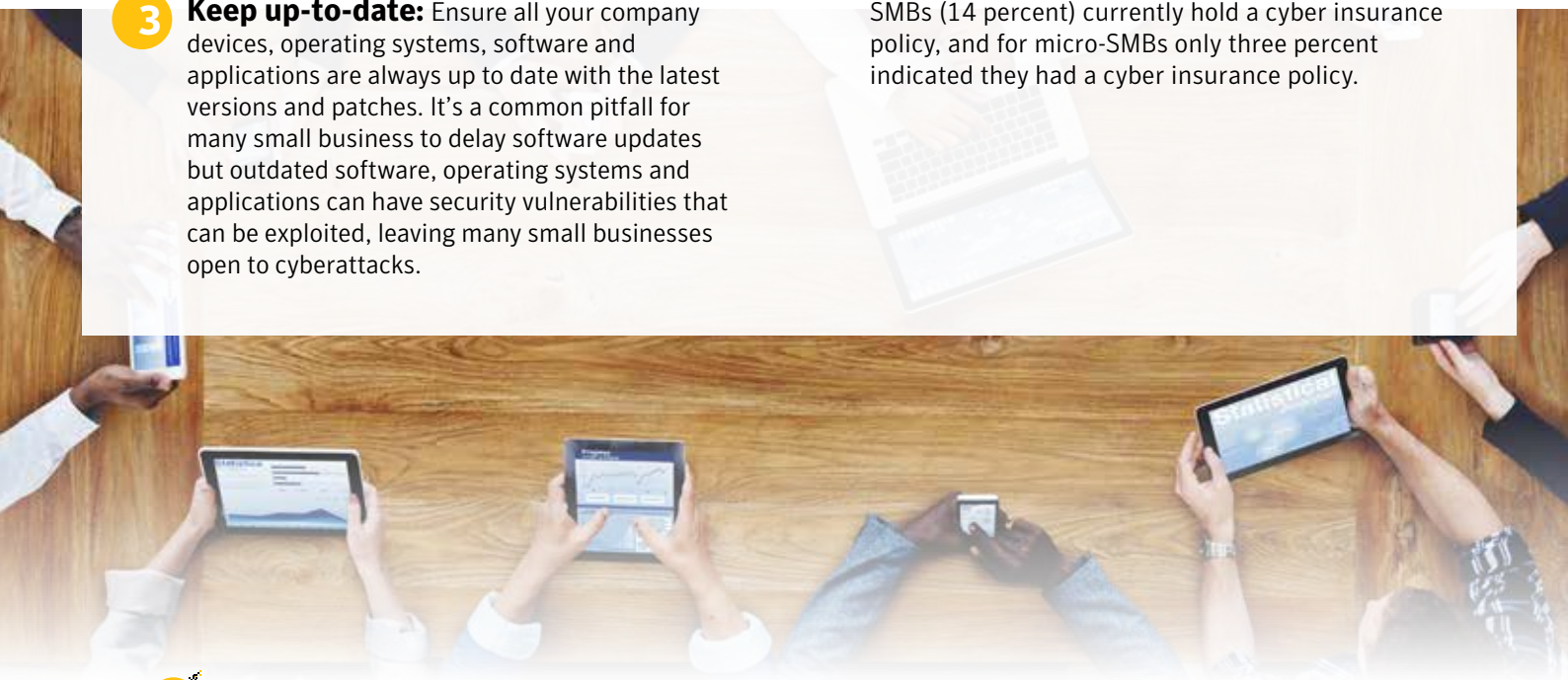
2. **Invest in security and backup**: To reduce the risk of being hit by a cyberattack, SMBs must implement comprehensive security software solutions such as Norton Security for Professionals or Norton Small Business for all their devices. Businesses should also use backup solutions to protect important files, such as customer records and financial information, and should consider encryption to add further protection in case devices are ever lost or stolen.

3. **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. It's a common pitfall for many small business to delay software updates but outdated software, operating systems and applications can have security vulnerabilities that can be exploited, leaving many small businesses open to cyberattacks.

4. **Get employees involved:** Employees play a critical role in helping to prevent cyberattacks, and should be educated on security best practices. Since small businesses have few resources, 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.

5. **Use strong passwords:** Use unique passwords for all your devices and business accounts. Change your passwords every three months and never reuse your passwords. Additionally, consider encouraging staff to use Norton Identity Safe to further protect your information and keep cybercriminals at bay. Wi-Fi networks should also be password protected to help ensure a safe working environment.

6. **Consider adding a cyber insurance policy:** Cyber insurance policies can cover business for financial losses resulting from cyberattacks. Only one in seven of Australian SMBs (14 percent) currently hold a cyber insurance policy, and for micro-SMBs only three percent indicated they had a cyber insurance policy.



ABOUT THE SURVEY

Norton's SMB Cybersecurity survey researched business perceptions of cybersecurity issues including computer backup, cybersecurity, ransomware and cyber insurance. This report presents the summary findings from the survey comprising a national sample of 1,023 business owners and operators, conducted from August 2 – 23, 2016. The businesses participating in the survey all employed between one to 20 people and were a registered business or sole trader in Australia.

This research report was prepared by Gundabluey Research and fieldwork was completed by QOR (Quality Online Research). It has a standard error margin of +/- 3 percent.

ABOUT SYMANTEC

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organisations, governments and people secure their most important data wherever it lives. Organisations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats.

For additional information, please visit **www.symantec.com** or connect with us on **Facebook, Twitter,** and **LinkedIn.**