NORTON SMB CYBER SECURITY SURVEY

Australia 2017

Norton
by Symantec

CONTENTS

SMB cyber security snapshot 3

SMBs held to ransom 4

Backup and recovery 5

Adoption of internet security solutions 6

Most prevalent cyber attacks 7

Public Wi-Fi usage 8

From the experts: security tips and tricks 9

About the survey / About Symantec 10

SMB CYBER SECURITY SNAPSHOT

NORTON SMB CYBER SECURITY SURVEY 2017

This report presents the summary findings of Norton's annual SMB Cyber Security Survey 2017, which aimed to gain an understanding of cyber security 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.

1 in 4

Australian small businesses have fallen victim to cyber crime

(Up from 1 in 5 in 2016)

Over 1/3

of businesses don't think they'd last a week without critical information.

In 2017, Australian small businesses turned to cyber security measures to future-proof their business, as they begin to acknowledge the serious impact a cyber threat can have.

1 in 4 Australian businesses have been hit by cyber crime, increasing from 1 in 5 from 2016.

More than a third of business operators (37%) don't think they would last one week without access to critical information. Thus, Australian small businesses backing up their data was at 26% in 2016, and while its increased to 32% in 2017, this is still too low, and can lead to unnecessary financial loss and downtime required to recover.

SMBs HELD TO RANSOM

Ransomware is a type of malware (malicious software) that prevents or limits users from accessing their system, either by locking the system's screen or user's files unless a ransom is paid.

In 2017, one in ten business operators had been affected by a ransomware attack, and 16% of those affected by the ransomware attack had paid the ransom (compared to 34% in 2016).

Businesses more likely to have suffered a ransomware attack included: businesses with a revenue of $1 million or more (20%), and businesses with an IT spend of $5,000+ (13%), businesses with a server (14%) and business operators aged under 40 years (17%).

Almost two thirds (66%) of business operators were likely to report a ransomware attack to the police. This was an increase from 2016 results at 60%.

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

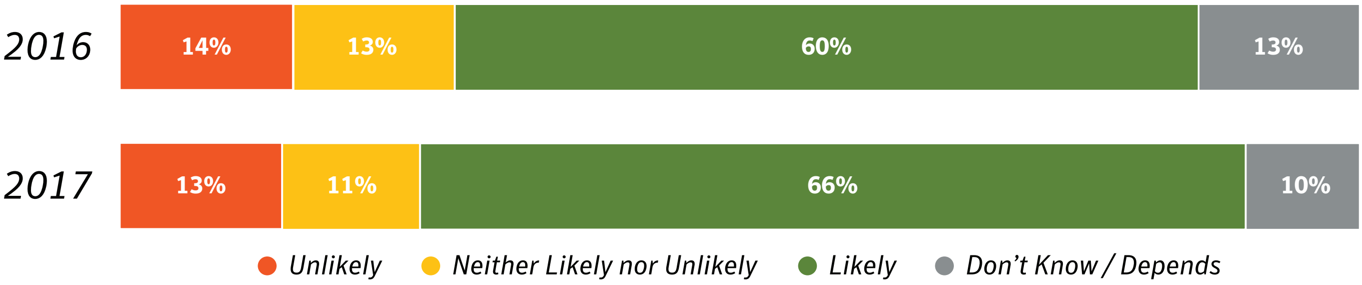
1 in 10

of business operators had been affected by a ransomware attack

66%

of business operators are likely to report a ransomware attack

Likelihood of reporting a ransomware attack



As a preventative measure and overall good business practice all businesses should consider backing up their data. Backup can be done locally or to an offsite location, but you need a method of retrieval should something go wrong. See the next page for more detail.

BACKUP AND RECOVERY

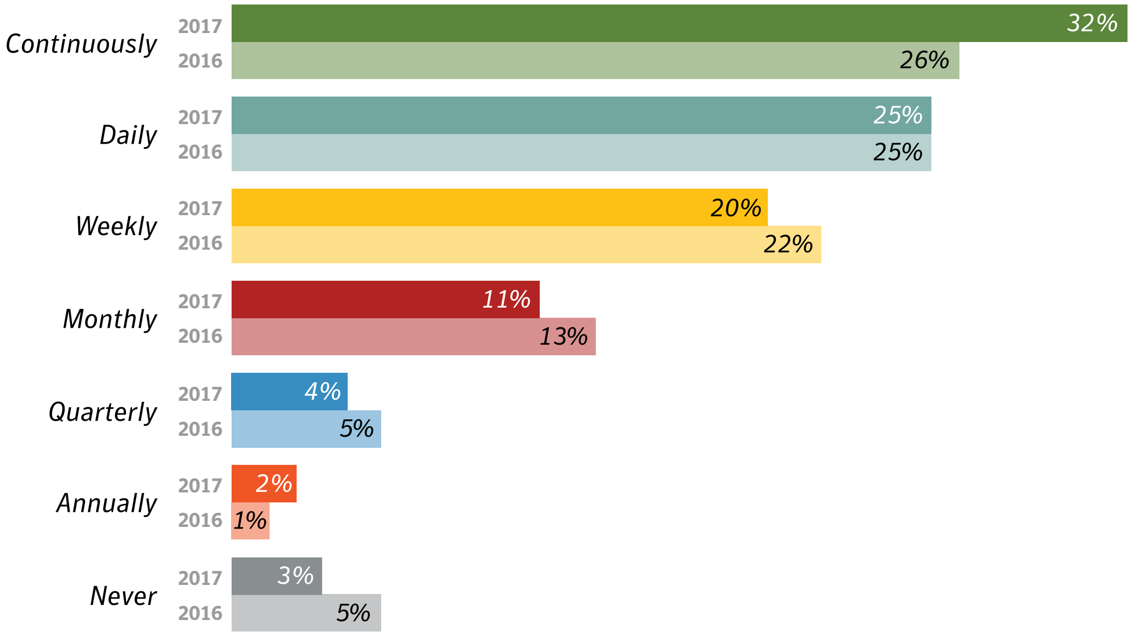
One in five (20%) micro and small businesses back up their business data no more than once a month, compared to 24% in 2016. Businesses with 1-3 employees.

Businesses who did backups were most likely to back up to an external hard drive (nominated by 67% of business operators, up from 62% last year), while 32% are using a cloud provider for their backups, increasing from 24% in 2016.

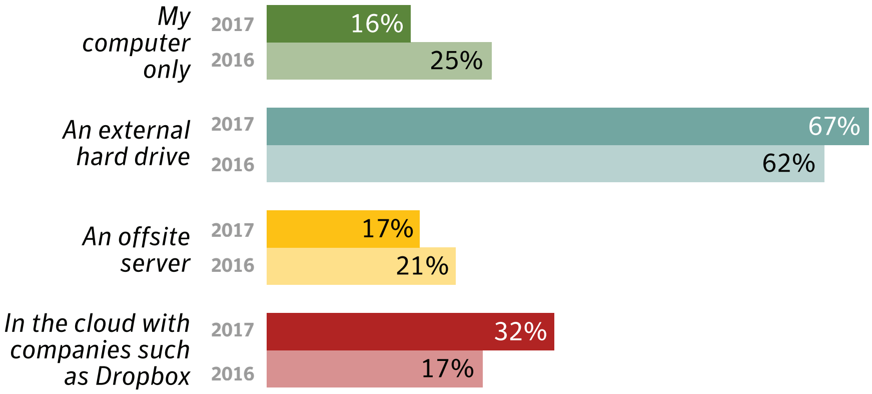
In 2016, a quarter of respondents backed up to their own computer, significantly declining to 16% in 2017. A similar decline occurred for those who backed up to an offsite server (21% in 2016, and 17% in 2017).

Almost 1 in 5 small businesses back up their data no more than monthly

FREQUENCY OF DATA BACKED UP



WHERE IS DATA BACKED UP



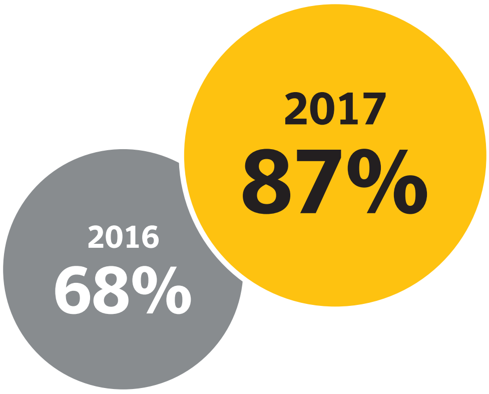
ADOPTION OF INTERNET SECURITY SOLUTIONS

Sign-ups for Internet security solutions have increased, from 68% in 2016, to 87% in 2017. ***However, 13% are yet to be protected.***

The survey found that the main reasons for Internet security sign-ups were to prevent against potential threats (60%), and believed it was simply good business practice (34%). Interestingly, older business operators (50-59 years) were more likely to implement internet security solutions as part of following good business practice, than their younger counterparts (aged 40 and under and only 23%)

More company devices, including laptops, PCs, tablets and smartphone, became password protected in 2017 (80-88%), compared to 72-82% of password protected devices in 2016. There are also less opportunities for sensitive information to be compromised and accessed by unauthorised persons with fewer micro and small business operators having access to financial data from a mobile (36%) or personal device (46 per cent) compared to those surveyed in 2016.

SIGNUPS FOR INTERNET SECURITY



MOST PREVALENT CYBER ATTACKS

The survey reported email or phishing scams (54%) are the most prevalent cyber attacks that Australian SMBs had fallen victim to, with hacking attempts (36%) and ransomware scams up from 52% in 2016 also common.

Type of Cyber Threat	2017	2016
Email or phishing scam	54%	52%
Hacking attempt	36%	35%
Ransomware scam	28%	28%
Online identity fraud	12%	10%
Privacy or data breach	11%	14%
An employee posting confidential information on a social networking site	5%	12%
An accidental loss of a laptop or mobile device or well-meaning employee distributing confidential data unintentionally	5%	7%
An internal threat such as employee stealing data on USB key or leaking information to competitors	4%	8%

54%

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

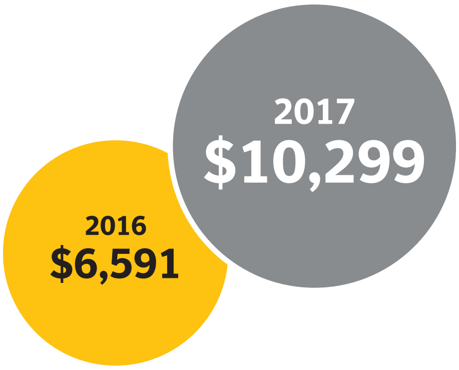
Downtime the main impact of a cyber security threat

Of the small business operators impacted by a cyber attack, downtime emerged as the main impact of a cyber security threat (39 %), followed by expense for re-doing work (25%), inconvenience (27%), financial loss (11%) and data loss (13%).

Of those that had lost data, over half of that (52%) had not been able to recover it, while the average financial loss caused per attack was over $10,000 AUD.

Impact of Cyber Threat	2017
Downtime	39%
Inconvenience only	27%
There was no damage done to the business	26%
Additional time and expense for re-work	25%
Privacy breach	14%
Lost important business information or data	13%
Financial loss	11%
Reputational damage	7%

OF THOSE THAT HAD LOST DATA, THE AVERAGE FINANCIAL LOSS PER ATTACK INCREASED BY $3,708 FROM 2016:



PUBLIC Wi-Fi USAGE

With around 40% of businesses having employees on the road or working remotely some of the time, use of public Wi-Fi networks and the potential security threats they can create is increasing.

Around two thirds to three quarters of businesses took security measures when accessing public Wi-Fi:

40%

ENSURED THEIR DEVICES WERE SECURELY CONNECTED TO ENSURE PRIVACY

35%

ONLY TRUSTED Wi-Fi LOCATIONS THAT REQUIRED A PASSWORD

32%

ONLY TRUSTED HTTPS (PADLOCK) SITES

At Least

25%

of businesses did not take security measures when accessing public Wi-Fi

60%

of businesses do not use VPNs across their business devices

While this shows that most many businesses understand the importance of undertaking such security measures, it still allows opportunity for security breaches, as only 40% use VPN (Virtual Private Networks) across their business devices.

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 times and sometimes businesses overlook things until it’s too late. Businesses shouldn’t wait until they’ve been hit by a cyber attack 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.

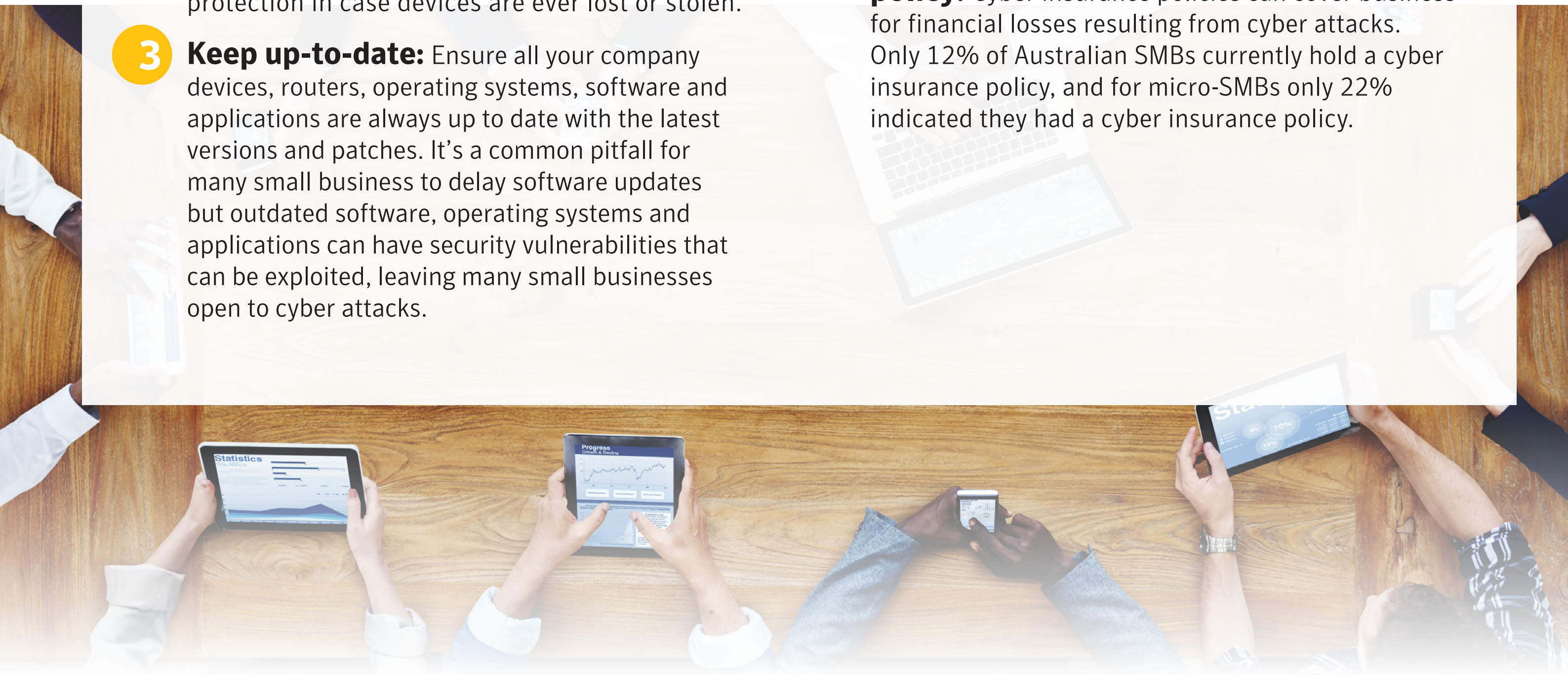
2. **Invest in security and backup**: To reduce the risk of being hit by a cyber attack, SMBs must implement comprehensive security software solutions such as Norton Security for Professionals or Norton Small Business for all their devices. Businesses should also use backup solutions to protect important 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, routers, 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 cyber attacks.

4. **Get employees involved:** Employees play a critical role in helping to prevent cyber attacks, 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 cyber attacks, 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 share or reuse your passwords. Additionally, consider encouraging staff to use password managers such as Norton Identity Safe to further protect your information and keep cyber criminals 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 cyber attacks. Only 12% of Australian SMBs currently hold a cyber insurance policy, and for micro-SMBs only 22% indicated they had a cyber insurance policy.



ABOUT THE SURVEY

Norton's SMB Cyber Security survey researched business perceptions of cyber security issues including computer backup, cyber security, ransomware and cyber insurance. This report presents the summary findings from the survey comprising a national sample of 1,048 business owners and operators, conducted from October 5-23, 2017. The businesses participating in the survey all employed between 1 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%.

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 60 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.**