NORTON SMB CYBER SECURITY SURVEY

New Zealand 2017

Norton by Symantec

CONTENTS

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 New Zealand. The survey findings have been released to help raise awareness about the security risks many New Zealand 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.

24%

of New Zealand small businesses experienced a cyber attack

(Up from 18% in 2016)

Over 1/3

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

In 2017, New Zealand 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.

24% New Zealand small businesses have been hit by cyber crime, increasing from 18% in 2016.

More than a third of business operators (35%) don't think they would last one week without access to critical information. 24% of New Zealand small businesses have been hit by cyber crime, increasing from 18% in 2016.

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, 7% of business operators had been affected by a ransomware attack, up from 5% in 2016.

Businesses with an IT spend of over $10,000 NZD were more likely to have experienced a ransomware attack (15%).

Over two thirds (69%) of business operators were likely to report a ransomware attack to the police, increasing from 2016 results at 68%.

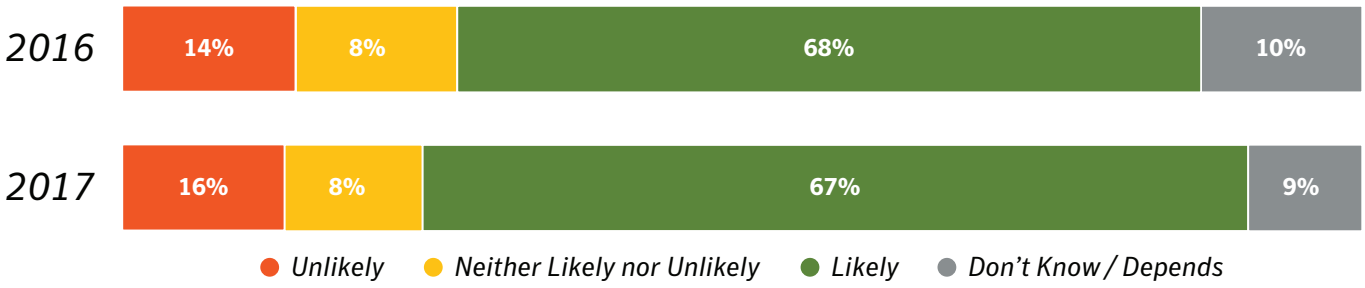
7%

of business operators had been affected by a ransomware attack

69%

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

Over one in five (23%) micro and small businesses back up their business data no more than once a month, compared to 11% in 2016.

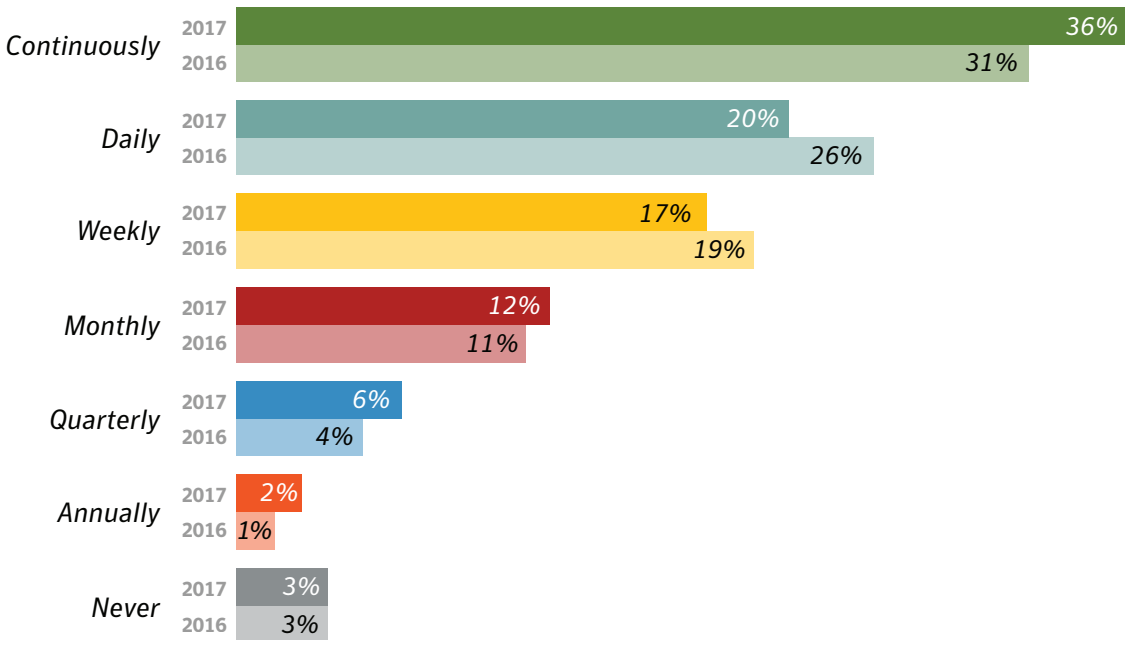
Businesses who did backups were most likely to back up to an external hard drive (nominated by 69% of business operators, up from 62% last year), while 43% are using a cloud provider for their backups, increasing from 31% in 2016.

In 2016, 16% of respondents backed up to their own computer, declining to 10% in 2017.

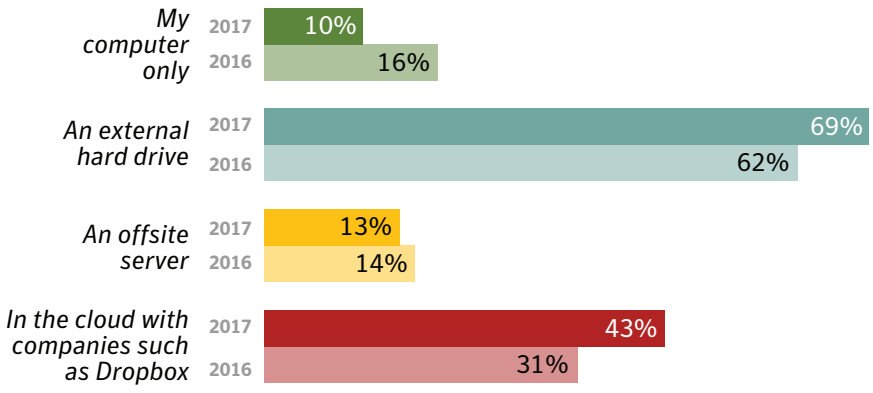
Over 1 in 5

small businesses back up their data no more than monthly

FREQUENCY OF DATA BACKED UP



WHERE IS DATA BACKED UP



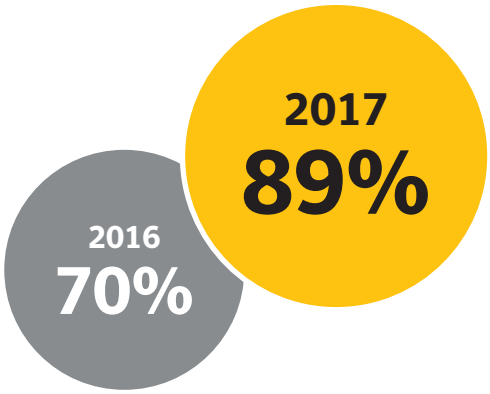
ADOPTION OF INTERNET SECURITY SOLUTIONS

Sign-ups for Internet security solutions have increased, from 70% in 2016, to 89% in 2017.
However, 11% are yet to be protected.

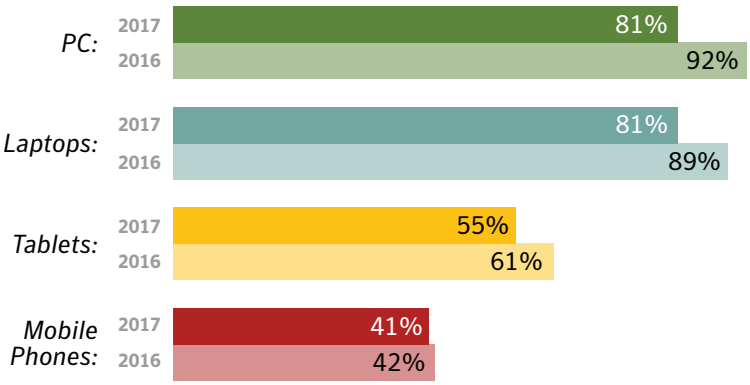
The survey found that the main reasons for Internet security sign-ups were to prevent against potential threats (60%), and believed it was simply good business practice (42%). Interestingly, older business operators (50-59 years) were more likely to implement internet security solutions as part of following good business practice (51%), than their younger counterparts (aged 40 and under and only 31%)

The proportion of workplace devices including laptops and PCs that were secured by an Internet security solution were 81% each. This has unfortunately declined since the 2016 survey.

SIGNUPS FOR INTERNET SECURITY



AVERAGE USE OF INTERNET SECURITY SOLUTION BY DEVICE



MOST PREVALENT CYBER ATTACKS

The survey reported email or phishing scams (66%) 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
Email or phishing scam	66%
Hacking attempt	27%
Ransomware scam	21%
Online identity fraud	10%
Privacy or data breach	7%
An employee posting confidential information on a social networking site	2%
An accidental loss of a laptop or mobile device or well-meaning employee distributing confidential data unintentionally	7%
An internal threat such as employee stealing data on USB key or leaking information to competitors	2%

66%

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 (34 %), followed by expense for re-doing work (19%), inconvenience (34%), financial loss (13%) and data loss (8%).

Of those that had lost data, over one third of that data (38%) had not been able to recover it, while the average financial loss caused per attack was over $15,500 NZD.

Impact of Cyber Threats	2017
Downtime	34%
Inconvenience only	34%
There was no damage done to the business	29%
Additional time and expense for re-work	19%
Financial loss	13%
Privacy breach	9%
Lost important business information or data	8%
Reputational damage	7%

OF THOSE THAT HAD LOST DATA, THE AVERAGE FINANCIAL LOSS PER ATTACK:

2017
$15,592 NZD

PUBLIC Wi-Fi USAGE

With around 35% 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:

31%

ENSURED THEIR DEVICES WERE SECURELY CONNECTED TO ENSURE PRIVACY

29%

ONLY TRUSTED Wi-Fi LOCATIONS THAT REQUIRED A PASSWORD

24%

ONLY TRUSTED HTTPS (PADLOCK) SITES

At Least

39%

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

69%

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 35% 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.

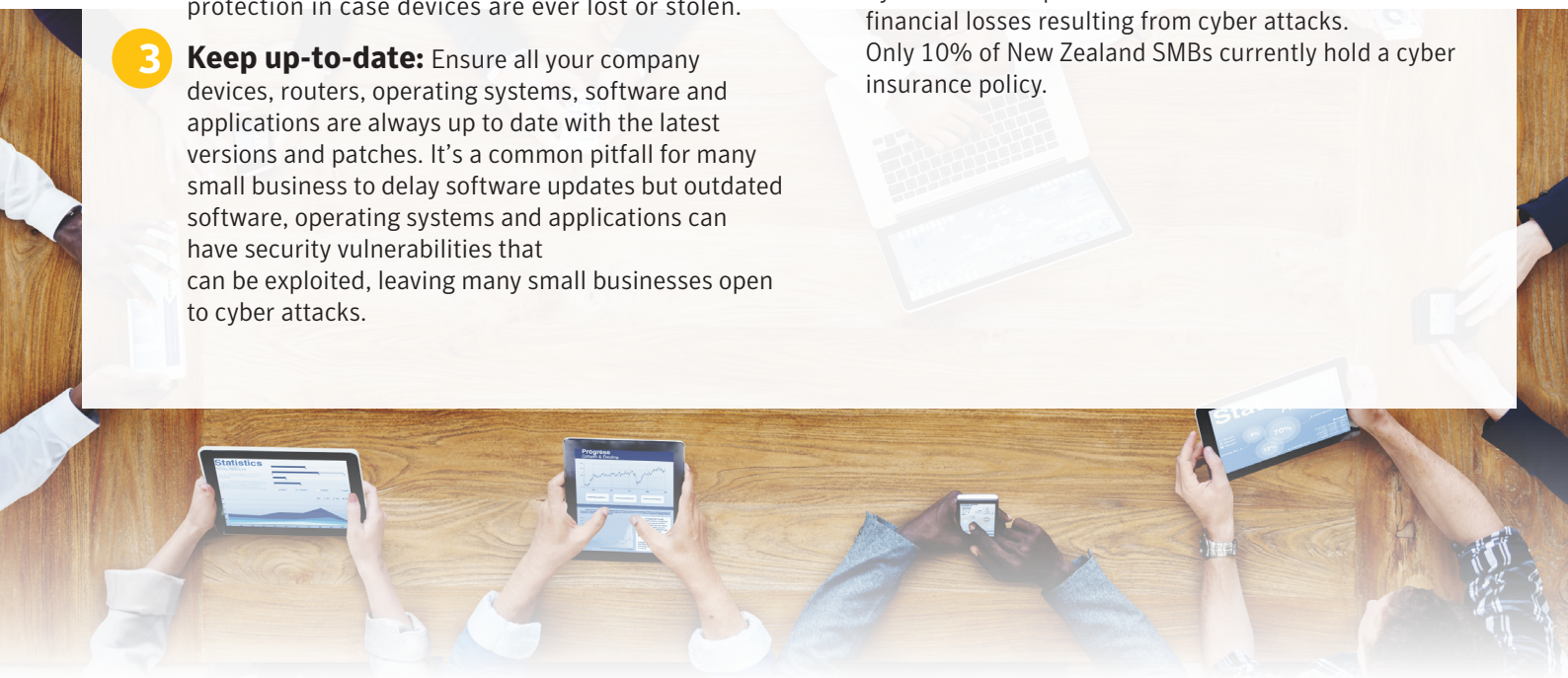
2. **Invest in security and backup**: To reduce the risk of being hit by a cyber attack, SMBs must implement comprehensive security software solutions such as Norton Security for Professionals or Norton Small Business for all their devices. Businesses should also use backup solutions to protect important 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 businesses for financial losses resulting from cyber attacks. Only 10% of New Zealand SMBs currently hold 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 502 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 New Zealand.

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.**