Microsoft

5 Strategies for Keeping Your Business Data Safe

New Zealand small businesses under attack

If you think that cybercrime is just something that happens to “other businesses” or “big businesses” or “overseas businesses”, think again.

Research shows that nearly one in five (18 percent) small and medium New Zealand businesses have been targeted by a cyber attack. These cyber attacks cost Kiwi businesses approximately NZD $19,000 on average and the main sources of these attacks were email phishing scams (70 percent) and hacking attempts (47 percent).°

Big or small, if your business keeps important or sensitive data such as customer details, financial information, trade secrets or other information you want to keep secure, data security is not something to take lightly.

In this eBook, we will discuss five strategies all businesses can adopt to better protect data, and the actionable steps they can take to reduce vulnerability.

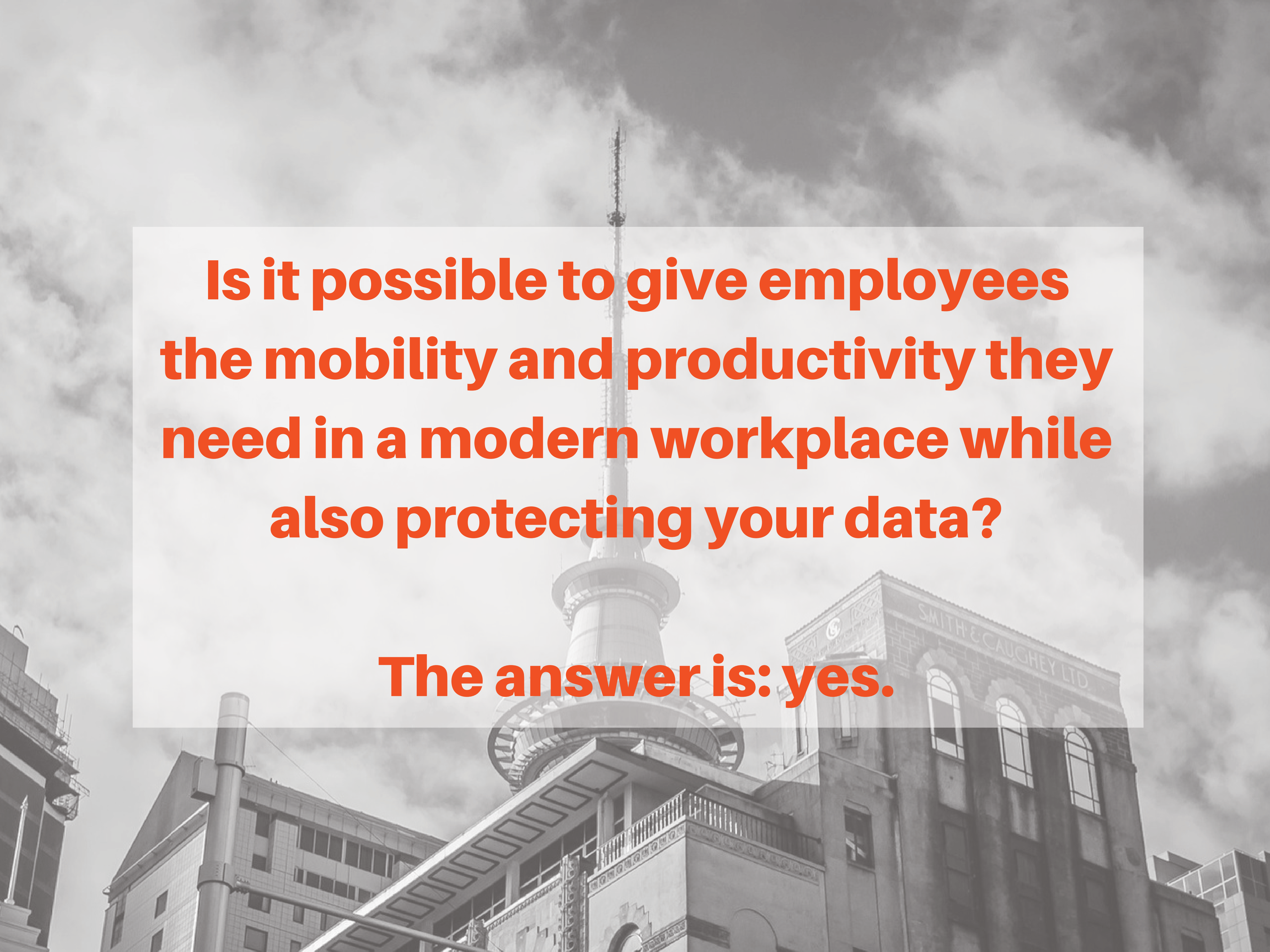
° *Source: Norton SMB Cyber Security Survey, NZ Entrepreneur Magazine*

Understanding the problem

The modern workplace has transformed the way businesses are operating. Advances in device mobility, cloud based software and mobile connectivity allows business owners and employees to adopt a less restrictive and highly productive work lifestyle.

The shift to a more mobile and cloud-based business means accommodating changes which previously may not have been considered. An increase in the number of personal mobile devices being used in work situations, dissolving office perimeters, and a greater use of non-business networks are some examples of business practices to consider while undergoing transformation.

While these changes result in increased productivity, they can also put sensitive data at greater risk of security threats, attacks, or breaches.



Is it possible to give employees the mobility and productivity they need in a modern workplace while also protecting your data?

The answer is: yes.

5 Strategies for Keeping Your Business Data Safe

- Reduce threats with identity and access management
- Manage mobile devices and apps
- Mitigate data loss with business continuity
- Enable secured collaboration
- Reduce malware exposure

Strategy # 1: Reduce threats with identity and access management

Often the weakest links in security incidents are due to human error, whether by accidentally leaking sensitive data (for example, passwords) or unknowingly activating malicious programs (for example, clicking malicious links, opening dangerous emails). With business applications and network access becoming readily available outside of the office there is an increasing need to address user identity and security.

Maintaining control over software applications across corporate networks and public clouds has become both a priority and a challenge. Workers want to access resources and technology from a variety of locations and devices, which can result in a number of complications from a security perspective – including password and location-based access management concerns.

External attackers look for corporate vulnerabilities – like leaked usernames and passwords – to access networks and steal customer information, intellectual property, or other sensitive data. This puts your business at risk of financial, legal, or public relations damage. Internal breaches can expose your data to risk as well.

How do you ensure control of the 'what', the 'when', the 'where' and the 'who' of software and information access?

Identity and access management can help reduce the risk:

- Eliminate the need for multiple credentials with a single identity to access cloud and on-premises resources.
- Limit individual access to what employees need to do their jobs.
- Revoke access privileges when an employee changes roles, leaves the company, or no longer requires access to certain shares.
- Enforce second factor authentication for all remote access to reduce authentication risk.

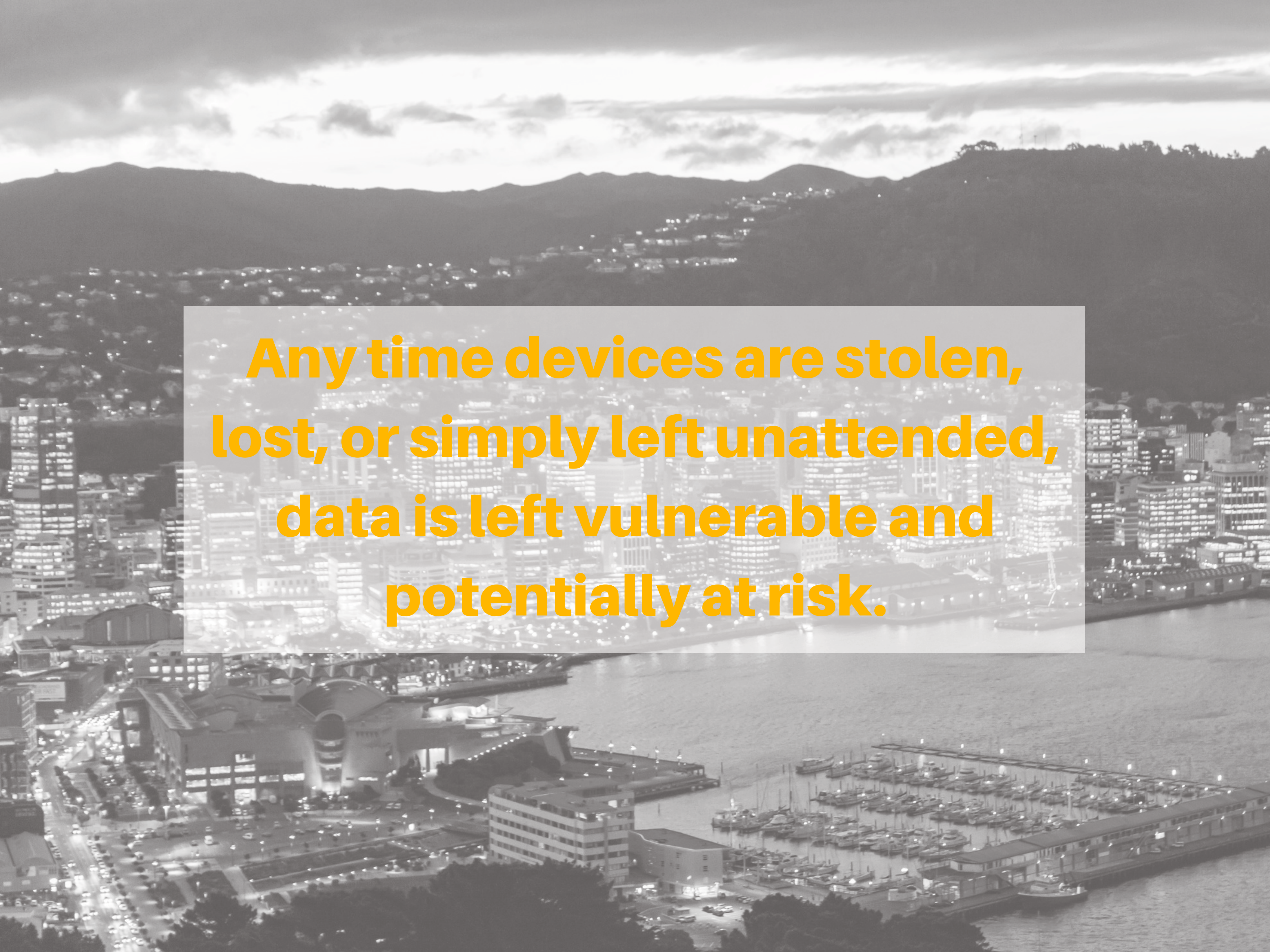
DID YOU KNOW...?

More than 80% of employees admit to using non-approved software-as-a-service (SaaS) applications in their jobs[1]

LEARN MORE

- Identity + Access Management
- Password Management for Small and Medium Business
- Mitigate threats by using Windows 10 security features

[1] Source: *"The hidden truth behind shadow IT – six trends impacting your security posture" (Frost & Sullivan)*



Any time devices are stolen, lost, or simply left unattended, data is left vulnerable and potentially at risk.

Strategy #2: Manage mobile devices and apps

As the Bring Your Own Device (BYOD) trend grows and the use of Software-as-a-Service (SaaS) applications proliferates, security concerns multiply. Access to business applications and storing business data is increasingly happening on personal devices which are not always governed by the same security standards as internal systems. This reality is forcing businesses to adapt new policies quickly to maintain a high level of security across the board.

An example: anytime devices are stolen, lost, or simply left unattended, data is left vulnerable and potentially at risk. There is also a potential of your corporate data leaking into personal applications. In this age of BYOD, how do you protect your critical data without reducing employee productivity? Begin with the basics:

- Don’t disrupt the user flow; make it easy and natural for them to comply. Consider managing important applications rather than the entire device.
- Be transparent about what IT is doing to employee devices. Protect only the corporate data.
- Look for solutions that enable employees to freely use the device for their personal purposes.

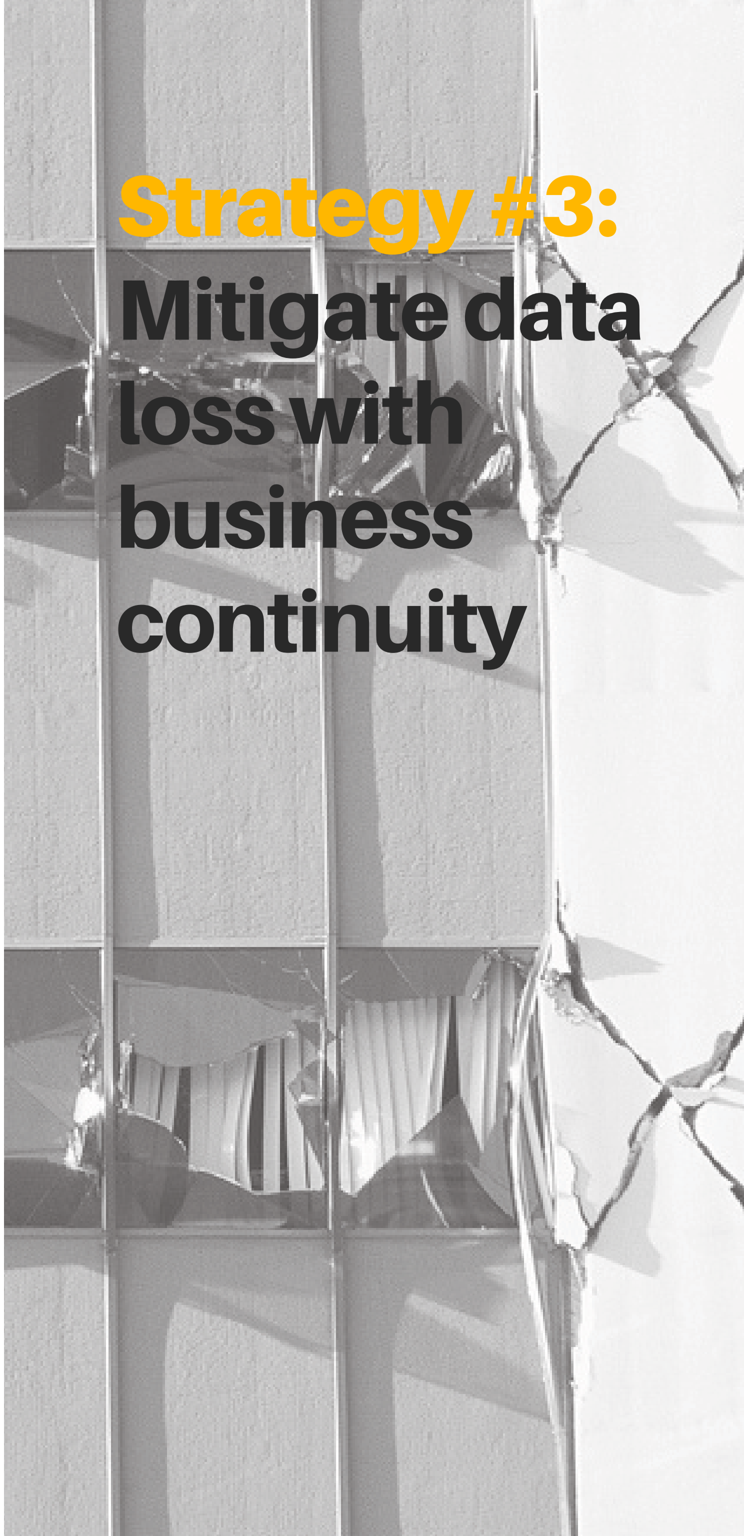
LEARN MORE

- How to integrate BYOD into your workplace
- Azure Multi-factor Authentication
- Microsoft Azure Active Directory
- Microsoft Intune

DID YOU KNOW...?

An estimated 52% of information workers across 17 countries report using more than three devices for work[2]

[2] *Source: “Employee devices bring added security concerns,” by Cindy Bates (Microsoft US Small and Midsize Business Blog)*



Strategy #3: Mitigate data loss with business continuity

Without a strong disaster recovery solution your business is exposed to risk from unexpected events such as natural disasters. Downtime can result in weakened customer loyalty, forgone opportunities, damaged reputation, low employee productivity, and critical expenses.

If your business was without power for an hour, how would your employees continue to do their work? It's probably quite manageable, right?

But what if it was a whole day, or a week, or even months that you were without access to your office and the equipment you and your staff used? It may sound like worst-case scenario, but it is a reality many have had to face in Christchurch, and more recently in Wellington, due to serious earthquakes affecting infrastructure.

Business owners and their employees were effectively locked out of their working environments with no warning, and no opportunity to recover anything.

The costs of maintaining secondary sites and infrastructure can be prohibitive, historically leaving a robust business continuity plan as a luxury afforded only to large enterprises.

DID YOU KNOW...?

Government estimates that the November 2016 Kaikoura earthquakes will reduce New Zealand's gross domestic product by $450m-$500m[3]

Start by evaluating the benefits of a business continuity plan enabled by a scalable cloud platform such as Microsoft Azure:

- Leverage cloud storage to retain offsite backups of mission critical applications and documents without a costly and labour intensive tape backup, hard disc or solid state storage solution.
- Identify the services your business needs to continue to operate in the event of a major outage, and plan for these to become available as part of a Business Continuity Plan.

LEARN MORE

- Business Continuity: what is it and why does your business need it?

[3] *Source: Cost of November earthquakes estimated at half a billion dollars* Stuff.co.nz

Workers can get creative with how they share information, putting your data in jeopardy and your company at risk of losing critical data.

Strategy #4: Enable secured collaboration

When it comes to sharing information, convenience often trumps security, which makes for a business owner's and IT security manager's living nightmare. Workers can get creative with how they share information, putting your data in jeopardy and your company at risk of losing critical data. How do you encourage workers to collaborate while minimising risks of compromised information? Offer a flexible, easy-to-use, secured solution that meets their needs:

- Establish secured tools for sharing information, and ensure the right workers have access. This includes a secured document sharing solution, such as the cloud-based SharePoint Online, or a restricted-access network share.
- Provide easy and secured information-sharing workflow to enable both internal and external collaboration.
- Learn more about the data loss prevention (DLP) capabilities within your ecosystem to protect your data where it is stored, when it is moved, and when it is shared. For example, an email can be limited to distribution within an organisation or carry a digital rights management setting that restricts who can open it.
- Extend DLP beyond email as well. Certain word processor, spreadsheets, and presentation programs also offer restricted access options that prevent unauthorised users from opening files.

LEARN MORE

- How to use 'OneDrive' to store business documents
- Azure Rights Management
- Office 365 Data Loss Prevention (DLP)
- SharePoint Online

Strategy #5: Reduce malware exposure

DID YOU KNOW...?

Malware is short for 'malicious software' and is a general term to describe computer viruses, worms, Trojans, spyware, adware and others[4]

Malware infections can often be traced back to user error. Phishing and spoofing schemes have become extremely sophisticated, tricking users with fake emails from trusted brands, luring them in with fake news stories, and convincing them to download seemingly innocuous apps that contain hidden attacks.

You can't stop users from surfing the web, using social media or accessing personal email on their own devices. How can you help them do these everyday tasks more safely? Education is your first line of defence:

- Ask employees to read basic guidance and/or complete training that details common methods of malware attack.
- Teach users to double check URLs in email to make sure they seem relevant, accurate, and legitimate. And consider implementing email protection solutions that can help prevent malware and phishing attempts from reaching employees' inboxes.
- Suggest that workers limit their app usage to those from a reputable source.
- Running machines 4+ years old costs you time and money, slowing you down, and putting you at risk of cyberattacks.

LEARN MORE

- Microsoft Office 365 Advanced Threat Protection
- Trojans, Viruses, Ransomware, Malware and Adware – what's the difference?
- Combat data threats with Windows 10 Pro
- Accelerate your business with modern devices

[4] Source: "Trojans, Viruses, Ransomware, Malware and Adware – what's the difference?" (Microsoft NZ Small and Medium Business Blog)

So there you have it.

Five practical strategies to help keep your valuable business data safe:

- Reduce threats with identity and access management
- Manage mobile devices and apps
- Mitigate data loss with business continuity
- Enable secured collaboration
- Reduce malware exposure

Next steps to learn more

For more information on security or making the most of cloud based technology in your business visit the Microsoft NZ Business Blog, browse Microsoft's solutions for businesses, or talk to a certified Microsoft partner in your area.