TribeTech

8 CYBER SECURITY BEST PRACTICES FOR NON PROFITS

EVERYTHING YOU NEED TO KNOW TO START SECURING YOUR NON PROFIT

Table of Contents

The Cyber Security Threat To The NFP Industry

Did you know, In a typical two year period, 10% to 15% of Australian not-for-profits have been the targets of fraud, with an average loss of $23,000, according to data from the Australian Charities and Not-for-profits Commission.

Companies of all sizes and government agencies fall victim to cyberattacks. Charities – even smaller ones – can be targeted too. And, often having weaker defenses, smaller charities can be especially vulnerable.

Common cybersecurity risks include:

Unauthorised access to a device, network or system
Viruses or other malicious software that can collect, change or delete information and spread throughout a network
Fake emails or websites set up to trick someone into revealing personal or sensitive information

The consequences of an incident can be significant. They may include:

Loss of crucial information
Disruption to services
Unauthorised changes to your charity's information and systems
Expensive costs to restore data and services
Costs of notification and investigation (including legal costs)
Costs arising from the attack itself (for example, extortion or ransomware)
Regulatory action and penalties
Loss of trust and reputation

Common Threats to NFPs

Payment Fraud Against NFPs and Charitable Groups

One type of card testing fraud that's often done on charity and NFP sites is **"BIN bashing."**
A BIN is the bank identification number on a payment card, usually the first 4 to 6 digits of the card number. All the cards from a specific issuer will start with the same BIN. Ordinarily, the random nature of the remaining digits prevents anyone from guessing a particular cardholder's full card number.

BIN bashing aims to get around that safeguard. Criminals start with a verified BIN number from a particular issuer and use bots to quickly try out different combinations in search of a random sequence that matches an existing payment card. To test their computer-generated numbers, they make a flurry of small donations to charity websites—all handled by their bots.

When a donation goes through, it confirms that the bot-generated card number used is valid. Each number that's validated this way can be used by fraudsters to buy merchandise from online retailers for resale or to defraud digital product merchants like game networks.
Because the test amounts are so small, they don't usually trigger alerts the way a large, unexpected purchase might. A cardholder reviewing a monthly statement or recent activity might not notice them. However, these small attacks can add up fast. Some not-for-profits we've spoken to report seeing bot-driven attacks with rates as high as 10,000 tests per minute.

Source: *https://australiancybersecuritymagazine.com.au*

DID YOU KNOW?

Under the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021, the **maximum penalty of $2.1 million** for serious or repeated breaches of privacy will increase to not more than the greater of **$10 million, or three times the value of any benefit** obtained through the misuse of information, or **10 per cent of the entity's annual Australian turnover.**

Could your NFP Survive this kind of implication?

A BENCHMARK FOR NFP GOVERNANCE AND RESPONSIBILITY

As the **Not-for-Profit** sector is evolving, so too have the expectations the community has of it, particularly regarding its governance and protecting people's data and personal information.

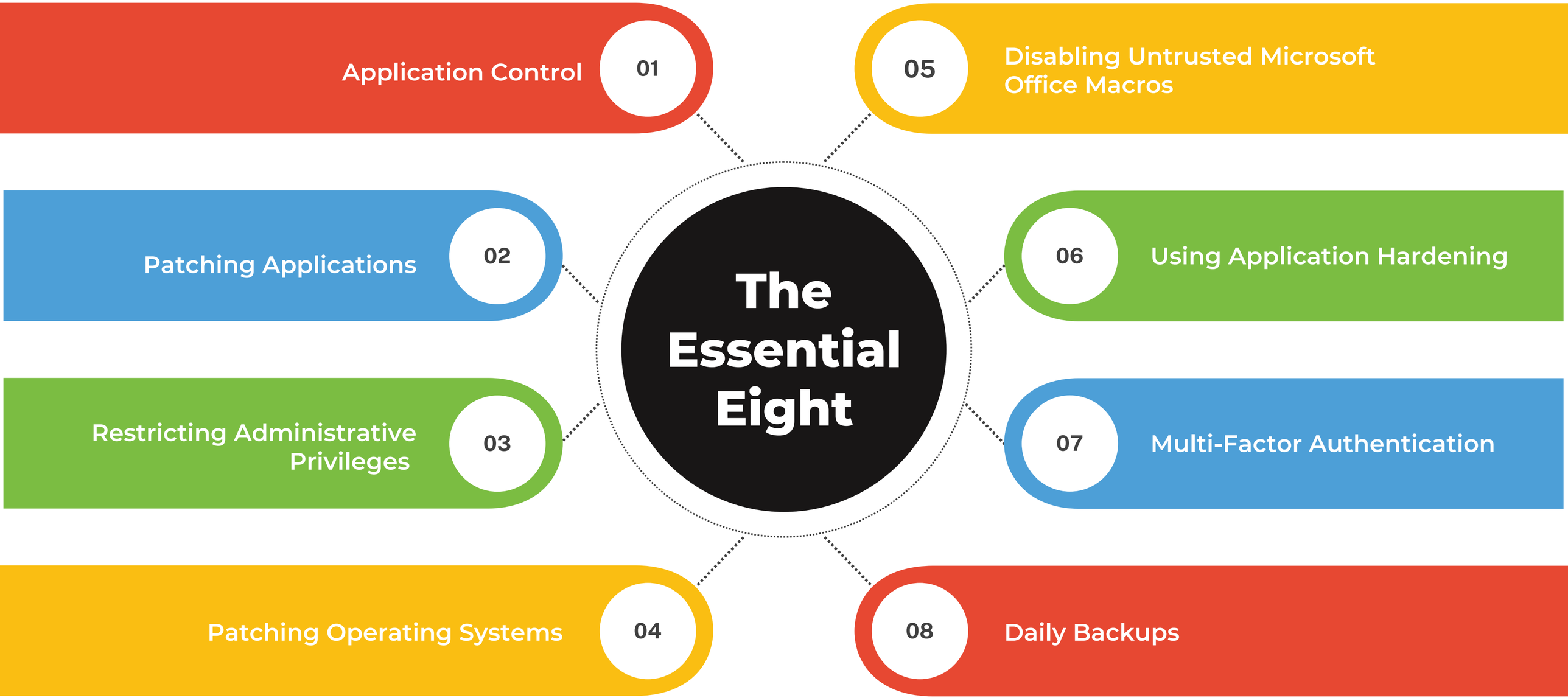
Although everyone in an **NFP** has an important part to play in protecting against cyberattacks, the ultimate responsibility is with the charity's CEO and board members.

They must consider the circumstances of their charity and make sure that they can identify and manage relevant cybersecurity risks.

Introducing The Essential 8...

We are living in a world of electronic systems! We use our digital information daily for business, and in our day-to-day activities, from paying bills, online banking, booking appointments or invoicing clients. There is an endless opportunity on the web with what we can do and with that, comes exposure to cybercriminal activity.

In 2017, The Australian Signals Directorate produced a list of 8 essential strategies for organisations to mitigate cybersecurity threats, called the Essential Eight.

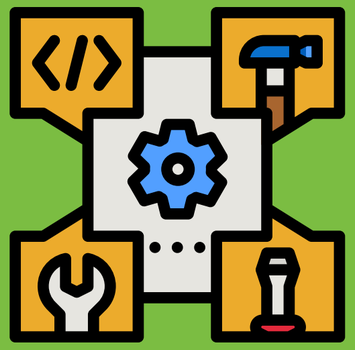

The Essential Eight
01
Application Control
02
Patching Applications
03
Restricting Administrative Privileges
04
Patching Operating Systems
05
Disabling Untrusted Microsoft Office Macros
06
Using Application Hardening
07
Multi-Factor Authentication
08
Daily Backups

Four reasons why all NFPs should embrace the Essential 8 Framework

The Essential 8 ranks organisational maturity across different pillars of security. When embraced, it provides a roadmap of what you need to address and maintain as your NFP evolves.

The Essential 8 offers best practice mitigation for cyber attacks

Increased expectation to have appropriate mitigation strategies for cyber-attacks in place



The Essential 8 Framework is constantly evolving and updated to keep your NFP safe

The Essential 8 is a highly cost-effective mitigation strategy for cyber security attacks

Let's Dive Into the Best Practices!

Best Practice #1

Application Control

Application control technologies are intended to stop the execution of malware and other unauthorised software.

It is important to understand there is a difference between antivirus software and application control. Antivirus software is known to block known bad activity and permit all other, application control technologies are designed to permit known good activity and block all other.

Threats:
Application control software prevents installation and/or execution of any application that is not specifically authorised for use on a particular host. This mitigates multiple categories of threats, including malware and other unauthorised software.

TOP TIPS

Identify the applications your business relies on. Unused applications pose a risk to your business, so let's remove them!

APPLICATION CONTROL

WHITE

A whitelist is a list, such as hosts, email addresses, network port numbers, runtime processes, or applications that are authorised to be present or active on a system.

BLACK

A blacklist is a list of discrete entities that have been previously determined to be associated with malicious activity.

GREY

A greylist is a list of discrete entities that have not yet been established as benign or malicious.

TribeTech

Know that this process is in-depth and takes time.

Doing this process yourself is gruelling and the chances are you will miss something. Your best bet is to ask for help and hire a professional. You can try patching by starting with your current application inventory. Prioritise your applications and make sure you have the latest stable version of each. If you are a few versions behind, acquire, test, and deploy the patches using your change management process. Sound too hard? Get someone who knows what they're doing. Your processors are too important to not be protected.

Best Practice #2

Patching Applications

Patch management is the process of delivering and applying updates to software. These patches are often necessary to correct errors (also referred to as "vulnerabilities" or "threats") in the software.

Common areas that will need patches include operating systems, applications, and embedded systems (like network equipment). When a vulnerability is found after the release of a piece of software, a patch can be used to fix it. Doing so helps ensure that assets in your business are not susceptible to exploitation.

Why is Patch Management so important for your business?

Security: Patch management fixes vulnerabilities on your software and applications that are susceptible to cyber-attacks, helping your organisation reduce its security risk.

System uptime: Patch management ensures your software is running smoothly and is kept up to date as well as supporting system uptime.

Compliance: With the continued rise in cyber-attacks, organisations are often required by regulatory bodies to maintain a certain level of compliance. Patch management is a necessary piece of adhering to compliance standards.

Feature improvements: Patch management can go beyond software bug fixes to also include feature/functionality updates. Patches can be critical to ensuring that your business is running efficiently and effectively.

Best Practice #3

Restricting Administrative Privileges

Restricting administrative privileges is one of the most effective mitigation strategies in ensuring the security of systems.

Users with administrative privileges for operating systems in your business can make significant changes to configuration and operation, bypass critical security settings and access sensitive information. Domain administrators have similar abilities for an entire network domain, which usually includes all the workstations and servers on the network.

Attackers often use malicious code (also known as malware) to exploit security vulnerabilities in workstations and servers. Restricting administrative privileges makes it more difficult for an attacker's malicious code to elevate its privileges, spread to other hosts, hide its existence, persist after reboot, obtain sensitive information, or resist removal efforts.

TOP TIPS

Understand everyone's role and determine the access they *actually* need.

Take inventory before reviewing the roles that have administrator privileges. Review your policies, plan, and run it through proper change management. If in doubt, TribeTech can help make this process easy and effortless for you.

BEST PRACTICE #4

PATCHING OPERATING SYSTEMS

Operating system (OS) patching is an important part of keeping IT systems and applications safe from malicious users that exploit vulnerabilities. An effective patch management process can close vulnerabilities before malicious users or threats have an opportunity to. The timely deployment of patches dramatically reduces corporate risk.

Patching operating systems shares similarities with patching applications and is equally, if not more important. While the applications you use impact specific areas of your job function, your operating system underpins your entire technology environment.

BUT, not every update fixes every problem! There may in fact be other issues, which is why patches should be tested prior to deployment. Scheduling of patches needs to be handled right for things to run smoothly.

There's also the chance of human-error with patches. People often overlook them and are guilty of putting them off until later if they're in the middle of something or, perhaps they can’t be bothered rebooting their computer. Implementing some checks and balances can help mitigate these potential challenges.

TOP TIPS

We recommend implementing operating system management tools to ensure patches are rolled out in a timely manner using a dedicated applications manager either in-house or through your managed services provider.

Best Practice #5

Disabling Untrusted Microsoft Office Macros

Think of macros as a batch of commands and processes all grouped together to make life a little easier when performing routine tasks. In many cases, they simply execute as the user and can save untold hours and reduce the errors made on tedious tasks.

However, macros can contain malicious code resulting in unauthorised access to sensitive information as part of a targeted cyber intrusion.

An increasing number of attempts to compromise organisations using malicious macros have been observed. Adversaries have been observed using social engineering techniques to entice users into executing malicious macros in Microsoft Office files. The purpose of these malicious macros can range from cybercrime to more sophisticated.

Best Practice #5 Cont.

Disabling Untrusted Microsoft Office Macros

One of the most effective application hardening techniques is privilege escalation detection: that is, a system that identifies when an intruder has granted themselves restricted access to data or networks. A common method of taking control of a system is “jailbreaking” or “rooting,” which involves taking control of a system from its “root” or most basic level. Privilege escalation detection notifies you when the root level of a system has been compromised.

Prevention

They say prevention is the best cure. That’s true when it comes to information security in general and application hardening.

TOP TIPS

Disable Macros from untrusted sources by working with your IT team or Managed IT Services Provider. They can implement a process to evaluate the following:

- **Is there a business requirement for a particular macro?**
- **Has the macro been developed or provided by a trusted party?**
- **Has the macro been validated by a trustworthy and technically skilled party?**

Unless you have the resources, put up your hand and ask us for help you.

Best Practice #6

Using Application Hardening

Application hardening is the general term for “hardening” or protecting an app against invasions by eliminating vulnerabilities and increasing the layers of security.

According to Statista, 178.1 billion mobile apps were downloaded in 2017, and that number is expected to increase to 258.2 billion in 2022.

With the growing use of mobile phones and devices, using them within the work environment too has increased. This means transferring and processing sensitive information through multiple applications which security breaches a particularly important concern.

So how does a company protect its software from hacking and cyber intrusions?

Security measures should be integrated into the app’s development from the outset, but one way to externally secure the app is a process called application hardening.

Best Practice #6 Cont.

Using Application Hardening

Think of application hardening like spring cleaning for your systems. You can get rid of anything you do not need and keep what you know you do. Securing a mobile app, whether with application hardening or internal security measures, involves three main components:

Prediction
To be prepared for intrusions, it is imperative to know what it is you're likely to be facing. Cybersecurity software can make some educated guesses by analysing data and threat intelligence to calculate trends within cyber-attacks.

Detection
To successfully stop a cyberattack you need to first know what is happening.

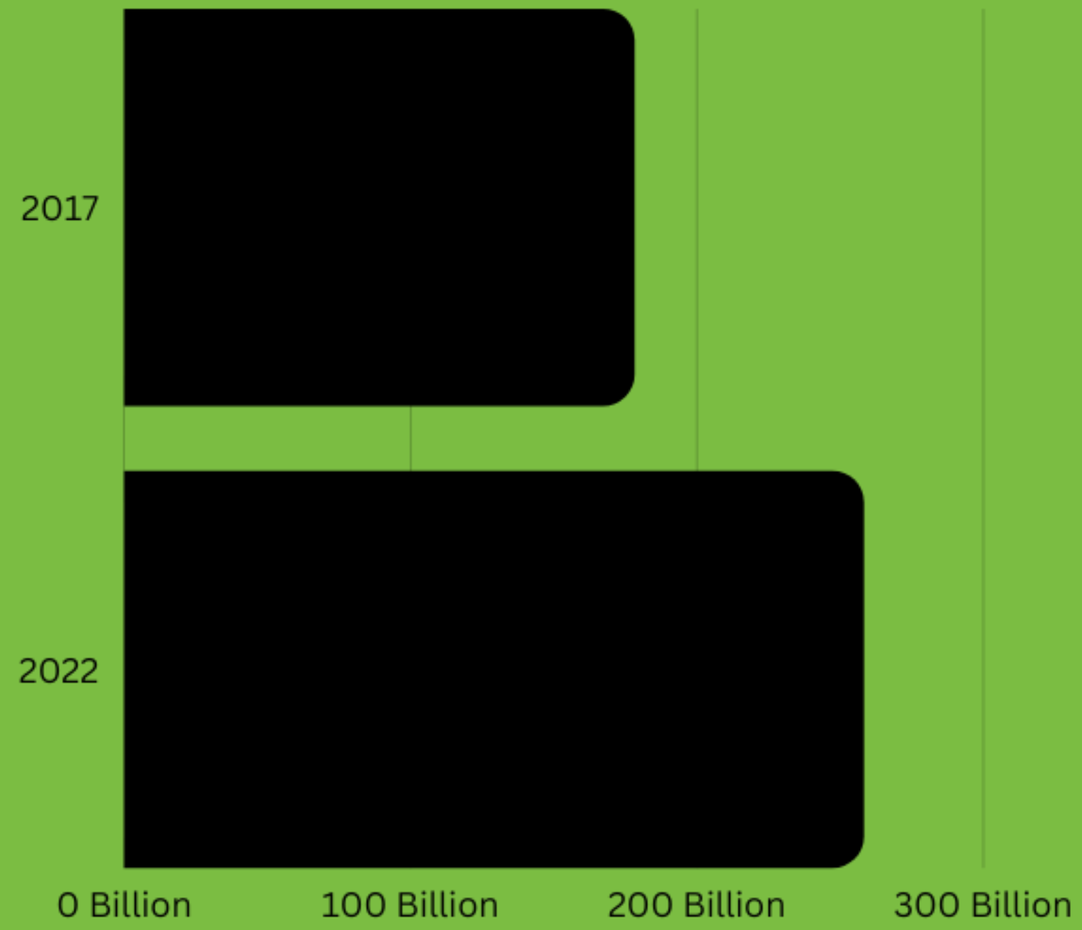
One of the most effective application hardening techniques is privilege escalation detection: that is, a system that identifies when an intruder has granted themselves restricted access to data or networks. A common method of taking control of a system is "jailbreaking" or "rooting," which involves taking control of a system from its "root" or most basic level. Privilege escalation detection notifies you when the root level of a system has been compromised.

Prevention
They say prevention is the best cure. That's true when it comes to information security in general and application hardening.

It is always best to start with an inventory to understand what you have. Understand how best to secure these applications and create a plan to address these issues. If this becomes too complex for you, reach out to the experts!

DID YOU KNOW?

178.1 billion mobile apps were downloaded in 2017, and that number is expected to increase to 258.2 billion in 2022



TribeTech

No matter the size of your business, having MFA is a must-needed step in keeping sensitive information safe. If your business doesn't have it, you should. If you do have it, ask if you can do it better or more securely. Always be willing to go back and re-assess knowing that threats and how they attack continue to evolve every day.

Best Practice #7

Multi-Factor Authentication

Having Multi-Factor Authentication adds extra layers of security by forcing you to provide another means of identifying yourself. Multifactor authentication combines two or more independent credentials: **what the user knows**, such as a password; **what the user has**, such as a security token; and **what the user is**, by using biometric verification methods.

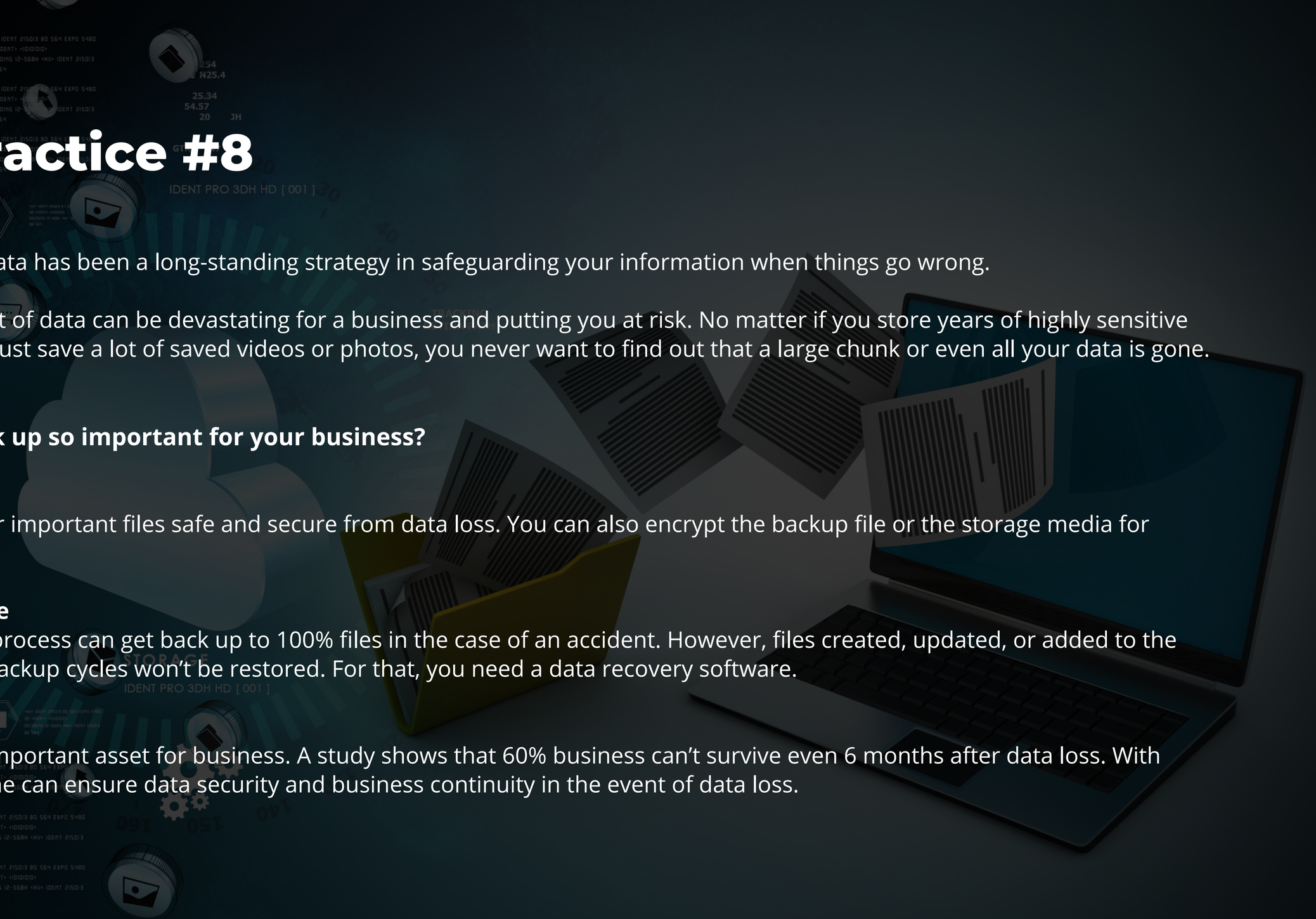
The reason having MFA is so important, is it creates a layered defence that makes it hard for an unauthorised person to access a target. This may include things such as a computing device or network, a database or even a physical location. If one factor is compromised or broken, the attacker still has at least one or more barriers to breach before successfully breaking into the target.

Best Practice #8

Daily Backups

Backing up your data has been a long-standing strategy in safeguarding your information when things go wrong.

Losing any amount of data can be devastating for a business and putting you at risk. No matter if you store years of highly sensitive customer data or just save a lot of saved videos or photos, you never want to find out that a large chunk or even all your data is gone.



Why is data back up so important for your business?

Data Security
Backups keep your important files safe and secure from data loss. You can also encrypt the backup file or the storage media for added security.

Recover with Ease
A regular backup process can get back up to 100% files in the case of an accident. However, files created, updated, or added to the system between backup cycles won't be restored. For that, you need a data recovery software.

Business Risk
Data is the most important asset for business. A study shows that 60% business can't survive even 6 months after data loss. With regular backup, one can ensure data security and business continuity in the event of data loss.

Best Practice #8 Cont.

PATCHING OPERATING SYSTEMS

Here are some scary Data Disaster & Backup Statistics

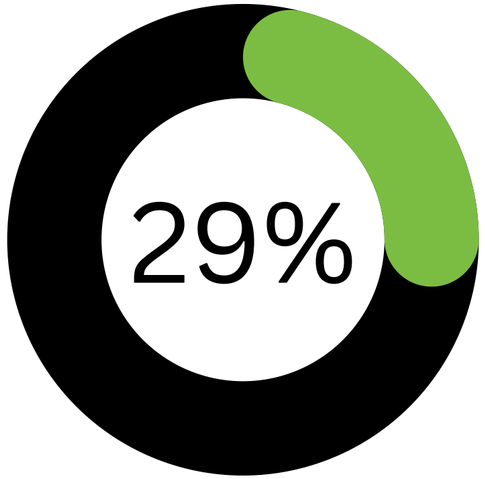
- Every five years, 20% of small and medium-sized businesses suffer from data loss due to a major disaster.
- 60% of businesses going through a data loss incident will shut down within six months after that.
- 93% of entities losing their data center for 10+ days file for bankruptcy within one year of the incident.
- 96% of businesses don’t back up their workstations.
- More than half of businesses don’t have enough budget to recover from data incidents.
- 75% of small businesses lack a disaster recovery plan.
- 93% of organisations that suffer a major data disaster and don’t have a recovery plan will go out of business within one year.

(Source: Webtribunal)

A small incident is enough to wipe out your company’s important data. You should always follow the best practices on data safety, which start with a backup solution. We recommend following the 3-2-1 rule and implementing a backup solution that stores 3 copies of your data. At least 2 in different locations (e.g. on your local server and a USB drive). And a 3rd copy stored offsite (which could be a cloud solution).

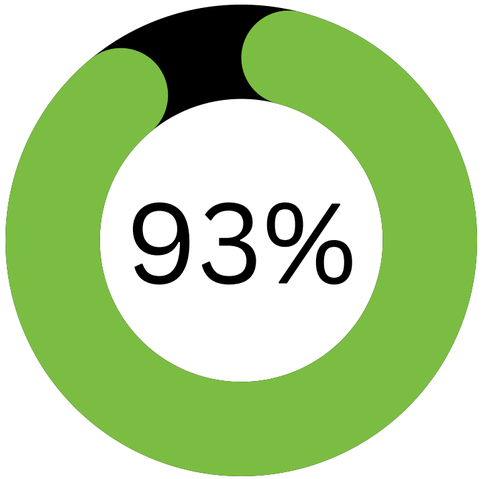
Data Disaster & Backup Statistics

60% of businesses going through a data loss incident will shut down within six months after that.



29% of hard drive failures are caused by accident.

TribeTech



93% of organisations that suffer a major data disaster and don’t have a recovery plan will go out of business within one year.

How protected is your NFP?

Take our mini cyber security audit by answering the following questions...

ARE YOU CURRENTLY ENSURING THAT YOU RESTRICT THE USE OF UNAUTHORISED SOFTWARE FROM BEING PRESENT OR RUNNING ON A COMPUTER OR SERVER?

ARE YOU AWARE IF MACROS ARE BEING USED WITHIN YOUR BUSINESS?

DO YOU HAVE SOMEONE DELEGATED TO VULNERABILITY ASSESSMENT AND PATCHING WITHIN YOUR BUSINESS?

DOES YOUR COMPANY USE MULTI-FACTOR AUTHENTICATION (MFA) ON BUSINESS APPLICATIONS?

WHO HAS ADMINISTRATIVE ACCESS WITHIN YOUR NETWORK?

DOES YOUR COMPANY CURRENTLY USE FLASH OR JAVA?

IF YOUR COMPUTER CURRENTLY AUTOMATICALLY DOWNLOADS AND INSTALL UPDATES, HOW OFTEN IS THIS CONDUCTED?

ARE YOUR BACKUPS MONITORED AND WORKING?

If you have more questions or would like help with cyber security, book a free 1:1 consultation with our team.

BOOK A CALL

TribeTech

PHONE

1300 874 238

EMAIL

info@tribetech.com.au

FACEBOOK

www.facebook.com/TribeTechAU

LINKEDIN

www.linkedin.com/company/tribetechnology

WEBSITE

www.tribetech.com.au