Future IT Services

8 Cyber Essentials to Safeguard Your Business

THE IMPORTANCE OF CYBER SECURITY IN PROTECTING YOUR BUSINESS

www.futureitservices.au

Contents

The Importance of Cyber Security

Does Your Business Really Need Cyber Security?

Cyber Security is a growing concern for all Australian businesses, with 60% of all targeted cyber-attacks striking small and medium businesses, it has never been more important for SMEs to protect their sensitive information from getting into the wrong hands.

Despite this, only 14% of SMEs are prepared to defend themselves.

"Cyber criminals won't go after my small business!"

Don't let these be your famous last words. It's easy to assume that cyber criminals only target large corporations. They won't look at the small non-profit or accounting firm in Cairns. Local businesses are too small to be targets, right?

Sadly, cyber threats are closer to home than you think.

Cyber criminals are always finding new ways to break in and they don't discriminate. In fact, as small and medium businesses generally have lower or no effective security measures in place, they are often an easy target for cyber criminals. No matter how big or small your business is, it's vital that you have security measures in place to protect what matters most to you.

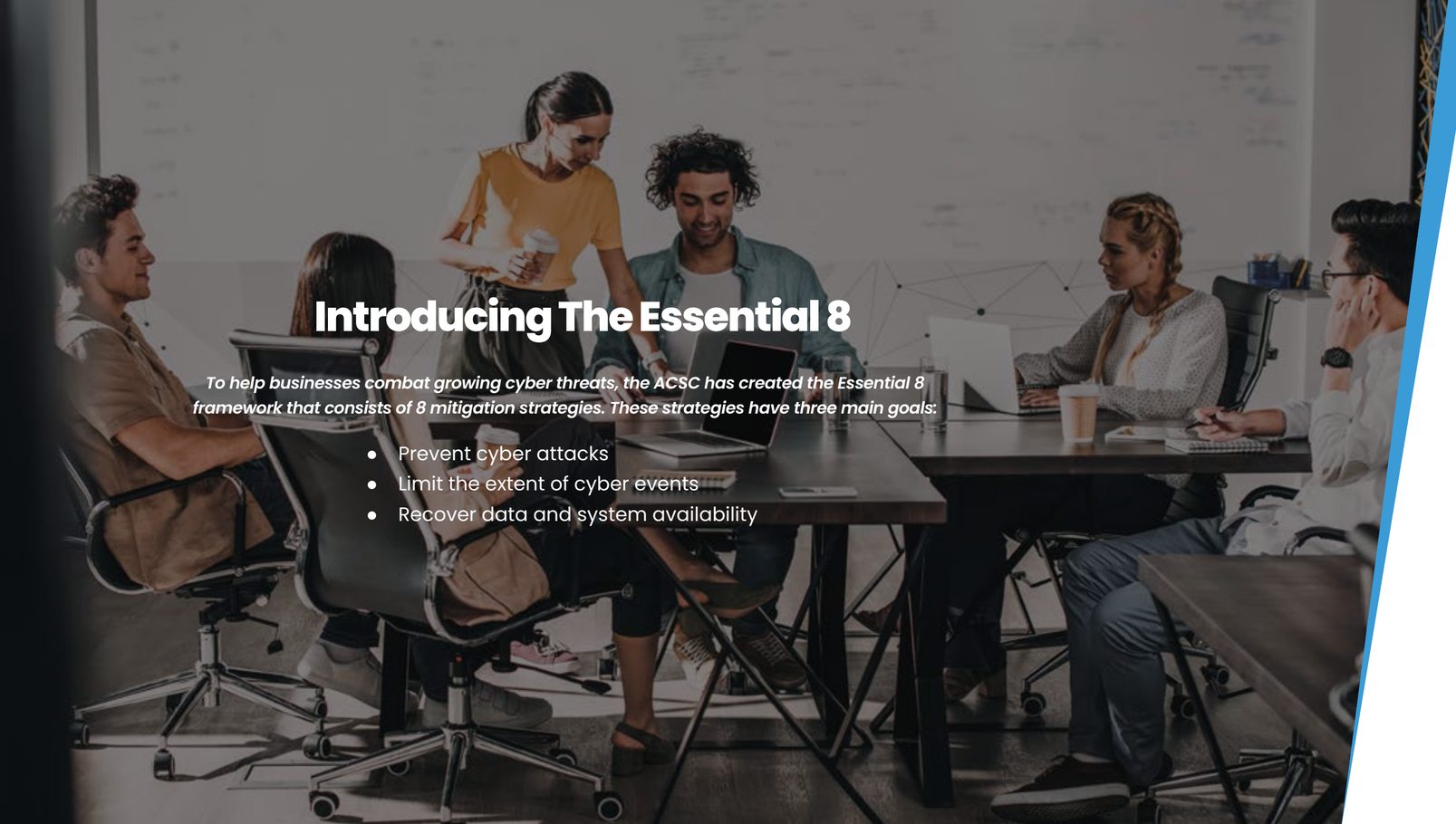
But Where Do You Start?

1 in 5
small businesses will suffer a cyber breach this year

$276k
is the average cost of a cyber crime attack in Australia

81%
of ALL breaches happen to SMEs

60%
of all targeted attacks struck SMEs



Introducing The Essential 8

To help businesses combat growing cyber threats, the ACSC has created the Essential 8 framework that consists of 8 mitigation strategies. These strategies have three main goals:

- Prevent cyber attacks
- Limit the extent of cyber events
- Recover data and system availability

What Are the Essential 8 Mitigation Strategies?

- Application Control
- Patch Applications
- Configure Microsoft Office Macros
- User Application Hardening
- Restrict Administrative Privileges
- Patch Operating Systems
- Multi-Factor Authentication (MFA)
- Daily Backups

What are the Four Maturity Levels?

Each of the Essential 8 areas have their own set of requirements and guidelines that is determined by 4 Maturity Levels.

0

Maturity Level 0

Not aligned with mitigation strategy.

1

Maturity Level 1

Partly aligned with mitigation strategy.

2

Maturity Level 2

Mostly aligned with mitigation strategy.

3

Maturity Level 3

Fully aligned with mitigation strategy.

We Break It Down

What Maturity Level Do You Need For Your Business?

Your Maturity Level is determined by what degree you have implemented the 8 mitigation strategies.

The level your business requires is dependent on several factors, such as the size and industry requirements, the sensitivity of data you store, the compliance requirements in tender proposals and even the insurability of your business. As you can't physically see cyber security, it can be tricky to know what maturity level you have or should have. So, to make it easier, let's think about cyber security in terms of home security.

Maturity Level 0:

Basic Security With No Strategy

Maturity Level 0 is like having a house and accidentally leaving the doors and windows unlocked. An opportunistic attack is a lot more common in these cases and the consequences can be devastating to any business.

When it comes to your business

Managed Service Providers will offer a good level of preventative security but without a strategy, your business is more likely to be a target of a cyber-attack and will have greater difficulty in recovering.

Maturity Level 1:

Improved Security With Basic Strategy

Maturity Level 1 equates to locking your doors and windows all the time, which makes it harder for criminals to gain entry.

When it comes to your business

Implementing the Essential 8 controls at Maturity Level 1 gives you the beginnings of a cyber security strategy and makes it harder for cyber criminals to access your internal networks.

Maturity Level 2:

Tighter Security With a Well-Formed Strategy

Maturity Level 2 significantly improves your cyber security posture. This is like having your house fully locked up and an alarm system with cameras in place.

When it comes to your business

By implementing Essential 8 controls at Maturity Level 2, this gives you the preventative protections to keep the criminals out and, in the case that they still get through, the visibility and forensics to see how they got in, what they have done and how to stop them in their tracks. For most businesses, this is the Maturity Level we recommend.

Maturity Level 3:

Enterprise Security With a Fully Formed Strategy

Maturity Level 3 reduces your attack surface dramatically. This would be like having a house with 24/7 security in place at all times.

When it comes to your business

Essential 8 controls at Maturity Level 3 fully aligns you with all controls at all levels. It is designed for large companies or companies that have a high degree of regulatory obligation or highly valuable data and is rarely seen in SME markets.

The Importance of Cyber Security

When is Your Business Considered Secure?

You wouldn't leave the house without locking the front door. The same should be said for your business. At a minimum, all businesses should have Maturity Level 1 security measures in place.

Some industries, such as government bodies, financial institutes or medical firms with large amounts of sensitive information, need to meet a higher maturity level to comply with the greater cyber security requirements.

Maturity Level 1 is Considered the Minimum Requirement for All Businesses

Future IT Services

Breaking Down the 8 Cyber Essentials

So by now you're aware of the importance of cyber security, but how do you get started? In the following sections, we will review each of the 8 Cyber Essentials and determine why and how you should use them to enhance your cyber security posture.

- Application Control
- Restrict Administrative Privileges
- Patch Applications
- Patch Operating Systems
- Configure Windows Macros
- Multi-Factor Authentication (MFA)
- User Application Hardening
- Daily Backups

Application Control

Prevent unauthorised apps from being installed on your work devices.

Why?

This is the first line of defence. If Malware is unable to run, it significantly reduces your risk and means the other strategies are backup plans. By implementing Application Control, you will have layered protection that makes it progressively harder for even a determined cyber criminal to breach.

What You Can Do

- Whitelist applications by first identifying all the different applications used by each department and for each process
- Determine whether the application is necessary or unnecessary – remove any unnecessary applications
- Regularly update stakeholders and maintain the list of applications
- Block applications and auto-uninstall unsecure software

Patch Applications

Regularly keep all of your applications up to date.

Why?

Cyber criminals are always looking for ways to get in to your systems and security vulnerabilities in applications are gateways for malware and exploits. Outdated and unpatched applications may contain weaknesses that would enable cyber criminals access to your network and your business's data.

What You Can Do

- Assign responsibility to individual/s for vulnerability assessment and patching
- Regularly update Allow-listed applications to the latest versions
- Update drivers and BIOS versions
- Remove or replace end-of-life applications that no longer have updates

97%

of breaches could have been prevented with today's technology

Configure Microsoft Office Macros

Block malicious scripts from compromising your systems.

Why?

Office Macros are special scripts and code and can run at elevated rights. Malicious Macros can download other code, run applications, encrypt your data and attack the remainder of your network.

What You Can Do

- Determine which (if any) macros your business uses and what purpose they serve
- Only allow known macros to run in your environment
- Configure applications to disable all but digitally signed macros
- Control browser plug-ins, extensions and allowed sites

User Application Hardening

Your browser can be an open window for cyber criminals so make sure to close it!

Why?

Internet applications like Java and Flash can be sources of malware. By hardening the internet browsers through our tools, you can restrict the opportunities for malware to infect your working environment.

What You Can Do

- Change default usernames and passwords
- Unless they are essential for an application, disable Java, Flash and web advertisements in your browser settings
- Provide or restrict access to web applications

Restrict Administrative Privileges

Ensure only the right people have full access to your systems.

Why?

Everyone likes being in control but, with too many cooks in the kitchen, the risk of making mistakes increases dramatically. With administrative privileges, users are able to download programs, install applications, lower security protections, delete or encrypt files – the list goes on. Even if it's not intentional, the more users set as administrators, the higher the security risk.

What You Can Do

- Remove unused administrative accounts
- Restrict the number of users with administrative access

Patch Operating Systems

Operate fully and securely with up-to-date operating systems.

Why?

Security vulnerabilities in operating systems are gateways for malware and exploits. Unpatched systems could allow an attacker access to your network and to steal, encrypt or otherwise damage your data.

What You Can Do

- Set your devices to automatically download and install updates
- As soon as the update has processed, restart computer immediately
- Work with Future IT Services to ensure all of your devices are running on the latest operating system

Multi-Factor Authentication (MFA)

The easiest and most effective method of security in just 1 click.

Why?

MFA adds an additional layer of protection by restricting access to applications like Microsoft 365, Google Workspace or many other SaaS platforms to only those users who can respond to the MFA prompt. This means that even if an account is compromised, the target needs to positively respond to the MFA prompt for the attacker to be successful.

What You Can Do

- Determine what applications and processes require you to sign in
- Enable MFA for all platforms and accounts
- Use a password manager
- Create unique passwords for all accounts and applications
- Be mindful when accepting MFA prompts

Daily Backups

You can never have too many backups.

Why?

Businesses should always backup their data. It is very risky to only store your data on local file storage either through Microsoft 365 or a server. Regular, automated backups of all data is essential to ensure that there is a recovery path should a device or account be compromised.

What You Can Do

- Implement the 3-2-1 Rule: have 3 copies of your data in 2 different types of media and at least 1 copy stored offsite in Cloud storage
- Determine the priority of information and what data needs to be backed up daily, weekly or monthly
- Implement regular restoration testing and have a disaster recovery plan

Implement the 3-2-1 Rule

3 Have at least 3 copies of your data

2 Store your copies in 2 different locations

1 Have at least 1 copy stored offsite in the Cloud

Time to Safeguard Your Business!

We hope you now have a better understanding of the Essential 8.

While we've tried to bring clarity to this crucial component in today's businesses, we understand it isn't quite so easy to implement.

To ensure your business has the right level of security...

TALK TO US TODAY →

Future IT Services

WWW.FUTUREITSERVICES.AU

Trust Our IT Team to
Empower, Connect & Protect
What Matters Most to Your Business.

Call our expert team today to find out how.

07 4058 5700

www.futureitservices.au

enquiries@futureitservices.au

147 Anderson St, Manunda, QLD, Australia, 4870