DIGITAL SENSE

An OvertheWire Company

Managing Data Risks

How using the Essential 8 secures your data and protects your business.

Protecting your data and your business.

Implementing a strong data security posture isn't always easy for SMEs. Resources are often restrained by budget which compounds the difficulty of remediation when a breach does occur.

Most SME operators will be familiar with the common cyber security threats such as malware, phishing attacks and ransomware. However, despite the commonality of these threats, many businesses still lack the basic security posture to insulate their data, customers and business.

An easy starting point for SME managers seeking an achievable blend of efficiency and security in managing data risk is by adopting the Australian Cyber Security Centre (ACSC) Essential 8.

The Essential 8 is a baseline of cyber security tactics designed to give Australian businesses a starting point to shape their data and cyber security posture. A key strength of the framework is its utility for businesses of all sizes to implement and build upon it as they grow.

The Essential 8 tactics deliver three layers of protection:

Prevention

- Application Whitelisting
- Application Patching
- Configuration of Microsoft Macros
- Application Hardening

Limitation

- Restriction of Admin Privileges
- Patch Operating System
- Multi-Factor Authentication

Recovery

- Daily Back-Ups

Learn more about managing data risks.
Book a discovery session with Digital Sense.

Following the Essential 8 delivers a number of data security benefits to businesses.

Depth of defence

Essential 8 tactics complement each other individually and collectively. They are powerful tools for protecting individual network components and constitute a multi-level defence that enables remediation, even if threats succeed in breaching a defensive mechanism.

Cost efficiency

Applying the framework comes at a modest financial investment for resourcing, hardware and software changes. The funds required to implement the Essential 8 provide a significant ROI compared to the cost of remediation and reputational damage to a business.

Productivity

Simplifying your security posture into a single cohesive framework enables your business to handle several components from a centralised location. Additionally, you'll gain the ability to apply policy easily across users, applications and devices.

Automation

The Essential 8 framework lends itself to automation processes that deliver security and compliance benefits. Configuring your security systems to monitor network traffic and automate alerts gives you a proactive security posture and the ability to maintain compliance requirements for your data.

Where does your organisation stand?

Take a look at the breakdown of each component to gauge where your organisation stands on data security.

PREVENTION LAYER

1. Application Whitelisting

What is it?

Whitelisting restricts a user's actions on their computer to those based on a set of rules that an administrator has implemented. This tactic protects an organisation's network from malicious applications by limiting user access to a set of functions that meet a safety criteria.

Why is it important?

Whitelisting enables an organisation to secure its data by proactively limiting entry to only trusted sources. Insulating against the malicious programs and apps is a significant challenge for SMEs and whitelisting plays a significant role in this.

Whitelisting is an effective tactic for protection against threats such as ransomware, zero-day threats, fileless malware and advanced persistent threats (APTs). The whitelisting process helps identify the threat before it can be identified by security software and breach your company's data.

How is it implemented?

Whitelisting is a crucial security element if your organisation is in a high-risk environment, such as where laptops and kiosks do not have admin privileges. Compiling an application whitelisting policy that's tailored to your organisation should be the first step in your implementation.

This policy should be constructed to cover key data breach points including email, applications and IPs with a streamlined approvals process. Using whitelisting software to automatically distinguish between approved and unapproved applications gives your business an automated defence against a malicious actor.

Utilising blacklisting software can also be a helpful tool to work alongside your whitelisting safeguards but it requires more time and resourcing in maintenance. Whitelisting gives your organisation a stronger line of defence by only allowing the approved applications to run.

PREVENTION LAYER

2. Patching Applications

What is it?

Application patch management refers to the practice of installing patches in your organisation's IT systems. The purpose being to correct errors or bugs in your existing software and improve performance.

Why is it important?

Patch management enables your organisation to minimise security threats through an automated plan that fixes vulnerabilities as they appear. The key component to the patch management process is implementing the process. Relying on a manual process for patch management is an onerous and high-risk tactic that can leave your systems vulnerable in the event of a delay. In addition to the cyber security benefits, automated patch management keeps your uptime at a maximum and your compliance requirements in check.

How is it implemented?

The simplest solution is to partner with a reputable vendor that can assist in delivering automated patch management. It's likely your business will have numerous servers, devices, apps and probably multiple operating systems. Without some outside help for automation, the resource requirement for your organisation can be particularly heavy.

A service provider can help you formulate a patch management plan that reduces complexity through a hierarchical structure is a great option. Move your patching into severity levels such as critical, important, moderate and low helps you prioritise urgency and keep your downtime to a minimum.

PREVENTION LAYER

3. Configuration of Microsoft Office Macros

What is it?

Microsoft Office applications contain macros that can bring unapproved access to sensitive data. The macros are helpful for productivity but can be used to carry out malicious activities such as exfiltrating or limiting access to sensitive information. Configuring your settings to counteract this vulnerability should be a key element of your cyber security posture.

Why is it important?

Users in your organisation may wish to generate and publish macros for a range of activities. This can be great for productivity in performing their daily duties but it opens up cyber security risks. Developing an internal procedure to manage the macros is the key to insulating a business from these vulnerabilities. Controlling your macros within the organisation gives your security administrators visibility of any breaches or symptoms of a breach.

How is it implemented?

Having a robust internal procedure or group policy for macros is an ideal starting point for managing them. System administrators can utilise group policy to enforce macro security settings and override the configuration options accessible to end users in Microsoft Office.

Learn more about managing data risks.
Book a discovery session with Digital Sense.

PREVENTION LAYER

4. Application Hardening

What is it?

Application hardening refers to the process of using multiple layers of security measures to protect apps from cyber security threats. This includes defence at host level, operating level, user level and administrator level. The physical security of device can also be included in an application hardening deployment.

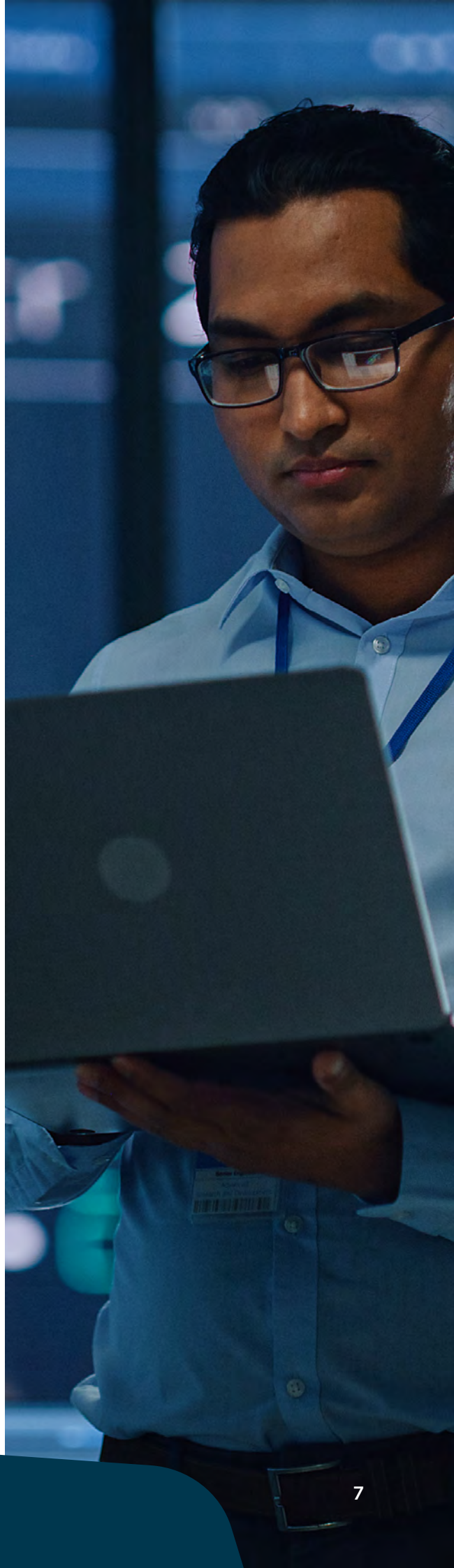
Why is it important?

Application hardening is key to protecting your organisation's intellectual property and any sensitive data stored in an app. The process safeguards your systems by using the multi-layered protections to identify and respond to breaches early. The early detection element that comes with application hardening delivers a significant advantage in the remediation process and protecting brand reputation.

How is it implemented?

Application hardening should start with diagnosis of the existing security layers of your current apps. Once you've got a high-level view of the security posture of your apps, seeking the advice of your vendors should be the next step. They can consult on implementation of security tactics for your apps and how best to integrate them into your hardening process.

One of the most effective techniques is privileged escalation detection. This refers to a system that identifies restricted access to data and networks by an authorised user.



LIMITATION LAYER

5. Restricting Admin Privileges

What is it?

Restriction of admin privileges refers to the process of assigning staff members into specific security groups within an organisation. These security groups dictate the level to which a user can change facets of a system within the organisation.

Why is it important?

Accounts with elevated privileges are often targeted by hackers due to the access they can provide to high level company information. Structuring administrative privileges into security tiers limits a hacker's ability to access sensitive data. This is a key element to creating security layers that counteract accidental or malicious damage.

Additionally, the majority of the employees in your organisation are unlikely to be able to spot the more subtle risks that lead to malware or ransomware attacks. Restricting admin privileges through security tiers creates a good balance between permissions and control for security and compliance. Using security tiers also enables high level administrators to efficiently move users in and out of tiers, rather than having to assign administrative rights to individual accounts.

How is it implemented?

First, you'll need to undertake an audit of your environment to identify access keys and which accounts need special authorisations. This process will assist in reducing the complexity of the security tiers and scale to a point where users only have access that is essential to performing their job.

The roles of staff should dictate what they can and cannot have access to. A simple methodology to define this element is using the Principle of Least Privilege (PoLP), which will ensure users will only gain privileges that are essential to perform their roles. Use a monitoring plan for all activities related to administrator accounts to ensure you have rapid detection of any anomalous activities.

LIMITATION LAYER

6. Patching Operating Systems

What is it?

Operating system patching refers to applying updates to your organisation's operating systems. Like application patching, the process enables an organisation to maintain currency and ensure its systems are not negatively impacted by outdated versions of its software.

Why is it important?

Patching operating systems reduces cyber security vulnerabilities by adding new features, fixing bugs and repairing security holes that can be overlooked in manual maintenance. Lacklustre patching is a significant contributor to security incidents as it leaves an organisation open to disruptions, downtime and resource drains in remediation.

How is it implemented?

Creating an effective patch management plan requires the implementation of consistent, repeatable processes that enable reviewing, testing and validation. Partnering with a managed service provider is a great way to manage patch management. If your organisation has a lean IT structure, is an SME, or just has limited scope for cyber security, finding a managed service partner can often be the best option for implementing a strong patch management system.

Learn more about managing data risks.
Book a discovery session with Digital Sense.

LIMITATION LAYER

7. Multi-Factor Authentication

What is it?

Multi-Factor authentication (MFA) is the security tactic of user identity verification through two or more separate credentials. MFA limits the ability of a hacker to gain entry to a system through protocols such as security tokens that ensure if one element is hacked or broken, the attacker still has another barrier to break through before they can breach.

Why is it important?

Hackers employ automated password cracking tools that can grant brute-force access to a system without an MFA security protocol. Employing a normal User ID and password login is particularly vulnerable to this type of breach. Cracking tools can simply guess multiple combinations of usernames and passwords until they uncover the correct sequence and gain entry. MFA implementation delivers an extra barrier to breaches like this and helps ensure that the entity seeking access to a system is what it claims to be.

How is it implemented?

There's a wide range of MFA deployments available. The difficulty comes in balancing the efficiency requirements of your staff and the security requirements of your organisation. If your users are constantly having to go through a laborious authentication for minor processes, the security may be coming at a productivity cost. The best option is to work with your IT security partner to help engineer an MFA solution that balances both. Some good options for consideration include:

1. **Security keys**
2. **One-time PINs**
3. **SMS or email verification**
4. **Software certificates**
5. **Biometrics**

RECOVERY LAYER

8. Daily Back-Ups

What is it?

Data back-ups are often the final failsafe for businesses in the event of a disaster. Back-ups are the process of copying your data and storing it securely in a separate location for use in the event of data loss or hack. Back-ups can replicate data from servers, databases, desktops, laptops and a range of other devices. The three key types of back-up solutions are:

1. **Full** – Complete copy of all files and folders.
2. **Incremental** – Only the data that has changed is backed up on top of an initial full back-up.
3. **Differential** – A middle ground between the two that uses less space than a full back-up but more network bandwidth than an incremental back-up.

Why is it important?

Problems such as hardware failure, accidental deletion of data or malicious breaches occur in even the most sophisticated IT set up. Whether a breach is accidental or malicious, the consequences of data loss can be crippling for a business. The reputational damage that can result from a data loss can be devastating for customer confidence and crippling for sales. If a customer doesn't trust your systems to protect their personal or payment data, the impact on sales can be devastating.

Additionally, the time and effort required for remediation from data loss can be a huge burden on resourcing. Without a strong back-up solution to fall back on, the drain on your staff to formulate a solution and fix the problem could stretch into days, all while your business is frozen or hampered by the missing data.

How is it implemented?

There's a range of back-up tactics available and like most IT solutions, the skill is in picking one that suits the operations of your business. The size of your business, number of users and volume of data needs to be considered in your implementation. There's a range of key stakeholders that need to be involved in this discussion including your technology leaders, operational leaders and frontline staff. Staff that frequently use key applications will be able to advise you on the implications that an app or system outage will have on customers and key service functions in your business.

Be sure to have a clearly set and understood RPO and RTO:

- **RPO** is the threshold of how much data you can afford to lose since your last back-up. Essentially, RPO refers to the frequency of your organisation's back-ups whether it's in minutes, hours, days or weeks.
- **RTO** is the measure for how quickly you need to have data restored. This measure determines how long it will take for your system to recover after there is a disruption.

You can back up your data in a variety of methods. Six of the most prevalent approaches are listed below:

- **Removable media**
  Back-up tapes and flash drives are often used for small data volumes, but this method is inefficient in large data environments.
- **Redundancy**
  A second hard drive or redundant system like a back-up email server that functions as a replica of your data.
- **External hard drive**
  Usually large capacity external hard drives with archival software that preserve changes to local files within that drive.
- **Hardware appliances**
  Usually storage devices or equipment that house back-up software.
- **Back-up software**
  Software that enables you to assign back-ups to the storage device of your choosing and control the back-up process automatically.
- **Back-up as a Service (BaaS)**
  Using a specialised managed service provider to manage back-up to a public or private cloud.

Learn more about managing data risks.
Book a discovery session with Digital Sense.

Need help with data risk management?

The team at Digital Sense can help you safeguard the growth of your business by harnessing the power of the cloud.

Our capability in data security, data management and cloud migration is designed to deliver the security, efficiency and availability that protects your staff, your reputation and your customers.

Our DSProtect solution is the ultimate Disaster Recovery as-a-Service technology. DSProtect provides complete protection for virtual machine workloads that are located within the Digital Sense Cloud, located on-premises, in private clouds or off-site. DSProtect services can provide a fully replicated environment at one or many Digital Sense Availability Zones.

Book a discovery session with one of our experts now.

1300 799 908

digitalsense.com.au

DIGITAL SENSE

An OvertheWire Company