Data#3

THE ASD ESSENTIAL EIGHT EXPLAINED

A Data#3 security eBook

Contents:

The Evolving Cybersecurity Threat

The last few decades have seen dramatic changes in the world of business. Today, organisations generate immense volumes of data, operate in an increasingly mobile environment and have become overwhelmingly dependent on connectivity and the cloud. This rapid pace of digital development has and will continue to change the way businesses operate – it's an exciting time for innovation and disruption.

However, with this evolution comes new risks. Businesses now face a completely new world of sophisticated cybersecurity issues - both external threats and internal vulnerabilities that continue to evolve.

For all organisations, implementing systems that minimise the impact of a cyberattack should be a high priority. Experience has shown that being proactive can save considerable time, money, effort and reputational harm compared to cleaning up after the damage has already been done.

Authored by Logan Daley, Information Assurance Specialist at Data#3, this collection of works deep dives into the practical actions organisations can take to make their networks more secure in an era of ever-changing threats.

In clear language, we discuss the **Australian Signals Directorate's (ASD) Essential Eight strategies to mitigate cybersecurity incidents** along with the who, what, where and why of successful implementation.

The ASD Essential Eight Explained

In February of 2017, The Australian Signals Directorate revised their long-standing go-to list of strategies for organisations to mitigate cybersecurity incidents.

The strategies have two main purposes; rendering critical information systems secure, while safeguarding organisational reputations and conserving valuable resources. However, unlike a great number of universally recognised and accepted establishments such as SOX, JSOX, PCI, SSAE, the Essential Eight:

- assists organisations to manage risks contextually relevant,
- provides prioritised steps in addressing relevant threats, and
- represents a baseline for organisations to achieve by following the Essential Eight Maturity Model.

Many companies struggle with their cybersecurity posture. The ASD's risk-based approach and prioritised controls are world-class, equating to a cost-effective and intelligent use of corporate security budgets, helping organisations that have arrived at a start of awareness progress to taking definitive action.

The evolution of the Top 4 to the Essential Eight firmly underlines the core message that information assurance is a process and not a project. Organisations that previously conducted a 'Top 4 project', but have not implemented ongoing security processes, may in fact, have missed the point. The Essential Eight is ASD's reminder of continual improvement.

Source: Australian Signals Directorate's Essential Eight Strategies to Mitigate Cyber Security Incidents

The ASD Essential Eight

1. APPLICATION WHITELISTING

A whitelist only allows selected software applications to run on computers.

WHY: Unsanctioned applications, including malware, are prevented from executing.

2. PATCHING APPLICATIONS

A patch fixes security vulnerabilities in software applications.

WHY: Adversaries can use known security vulnerabilities to target computers.

3. RESTRICTING ADMINISTRATIVE PRIVILEGES

Only use administrator privileges for managing systems, installing legitimate software and applying software patches. These should be restricted to only those that need them.

WHY: Admin accounts are the 'keys to the kingdom'; adversaries use these accounts for access to information and systems.

4. PATCHING OPERATING SYSTEMS

A patch fixes security vulnerabilities in operating systems.

WHY: Adversaries will use known security vulnerabilities to target computers.

5. DISABLING UNTRUSTED MICROSOFT OFFICE MACROS

Microsoft Office applications can use software known as 'macros' to automate routine tasks.

WHY: Macros are increasingly being used to enable the download of malware. Adversaries can then access sensitive information, so macros should be secured or disabled.

6. USING APPLICATION HARDENING

Application hardening involves disabling insecure and unused services from necessary applications, managing privileged access to the applications, and restricting the use of applications that are well-known attack vectors. Examples include blocking web browser access to Adobe Flash Player (uninstall if possible), web ads and untrusted Java code on the Internet, and disabling unused or insecure default services and applications.

WHY: Flash, Java and web ads have long been popular ways to deliver malware to infect computers.

7. MULTI-FACTOR AUTHENTICATION

This is when a user is only granted access after successfully presenting multiple, separate pieces of evidence. Typically, something you know, like a passphrase; something you have, like a physical token; and/or something you are, like biometric data.

WHY: Having multiple levels of authentication makes it a lot harder for adversaries to access your information.

8. DAILY BACKUPS

Regularly backup all data and store it securely offline or at an alternate site such as a secondary data centre or in the cloud.

WHY: That way your organisation can access data again if it suffers a cybersecurity incident.

Source: Australian Signals Directorate's Essential Eight Strategies to Mitigate Cyber Security Incidents

1. Application Whitelisting

What is it?

If you strip away all the 'next-generation' and Unified Threat Management (UTM) pieces from a firewall it becomes a simple yes/no device. Application whitelisting works in a similar same way. It specifies which applications can execute - the whitelist - leaving everything else implicitly or explicitly denied - the blacklist. Of course, there will always be some that fall in the middle - the greylist. However, these applications should be reserved for administrative decision rather than leaving for the user to decide. In addition, make sure the aforementioned firewall has a default 'deny all' rule in place. Installations where the final rule is 'allow all' have been known to attract millions of hits.

Where do I start?

Begin by identifying the different information systems and applications used to support organisational business processes. This will essentially become your 'whitelist'. It's worth noting that not every team in your organisation will use the same list. There may be a core list for everyone, such as Office applications, but different lists for other roles – think Payroll or HR. Getting a handle on the applications, both necessary and unnecessary, is crucial. Without your master list, you could wind up preventing good applications and allowing bad ones, which will be counterproductive to the strategy.

Any pitfalls?

There are many, which is why it's important to involve the right people. Beyond the IT team, include management to garner support and get the initiative signed-off. Having the whitelist as part of your information security/general IT policies is also recommended. You need to know exactly what applications are on your network and which ones are actually needed. It's not an easy voyage, but one worth taking. At the heart of it, executing code is the cause of a lot of breaches. Keep in mind, it's not always malware - sometimes your own tools and utilities can be used against you.

The ghost in the machine?

It's the users. Plain and simple. At the end of the day, everyone wants to do their jobs, get paid, and go home to their families. Be ready to uncover shadow IT and related shadow data that are known to arise as a result of shortcuts - intended or not - that are used to get the job done. Application whitelisting will help secure the environment but be prepared for some resistance from the masses.

How do I make it work?

You probably already have the required hardware and software to make this a reality. Most modern endpoint protection applications have the ability to perform application whitelisting. Modern UTM firewalls that offer application control are not really 'whitelisting', but can add an additional layer of defence. You should also consider dedicated whitelisting and application control solutions from several vendors who produce powerful applications specific for this purpose.

Am I missing anything?

Ensure an endpoint solution with application whitelisting functionality or a dedicated application whitelisting application is applied to every host. Also, think beyond workstations. Locking down the ability of applications to execute on your servers – particularly database servers and web servers – can be an invaluable tactic.

How do I start?

It's time to take stock and figure out what your business needs and what it doesn't want. This all comes down to what makes your business tick – the very applications you rely on.

2. Patching Applications

What is it?

In a nutshell, applications are designed to perform a specific task but often don't account for potential flaws and vulnerabilities. Unless it's actually a security-centric application, security is lower on the features list - that's if it makes the list at all. In some cases, applications are released with undocumented capabilities, use non-standard ports and services, and many enabled features are never used. It's well known in the industry that no application would make it to market if it underwent perfect quality assessment (QA).

Over time, the capabilities, features, and other bugbears come to the surface. When vulnerabilities are detected, many vendors will swoop in to fix the issue. In other cases, attackers can discover and exploit a vulnerability to their own advantage.

Where do I start?

As is the case with application whitelisting, a current inventory of applications is a must. You will need to know what is on your network and why. Odds are the vendors of those applications have released patches and updates to address these issues, add features, and improve performance. Once you know all applications, you can investigate whether or not you have the latest stable releases and patches. In some cases, vendors are very proactive and notify their clients, supplying the patches at no charge during the lifetime of the application. Some charge extra for this service. Others will just make them available without letting you know. In the end, patches and updates should be available.

TECHNOLOGY WAS CREATED BY HUMANS, SO HUMAN ERROR IS INNATE.

Any pitfalls?

Without a doubt, Shadow IT can bite hard. If you focus only on the 'known' and approved applications, you may overlook the one-off applications downloaded to perform some task not officially sanctioned by the company. Even these one-off systems should be updated - or preferably removed until their existence can be justified and approved. In larger enterprises, patching applications can become all-consuming as it seems there are updates every day. A solid change management process to test, schedule and deploy updates and patches on a prioritised basis is a must-have.

The ghost in the machine?

It's impossible to secure every application perfectly. Risk will always remain. The key is to reduce the risk inherent in using applications to an acceptable level. Where the possibility to interact with an application exists, so too comes the ability to exploit the application. Technology was created by humans, so human error is innate.

How do I make it work?

Once you have a current inventory of your applications and a reliable change management process in place, it's time to begin - or at least continue - with patching your systems to the current stable releases. Remove or replace any unsupported applications and make sure they're included in your application whitelisting solution. Create a list and subscribe to alerts, or alternatively, you can ask your vendors to notify you of updates and patches so you can include them in your regular scheduled maintenance. When it comes to emergency or urgent patches, treat them as a priority.

An incredibly valuable and powerful option here is to implement vulnerability management services through use of dedicated applications, many of whom are available as-a-Service from your cybersecurity service providers. By implementing such a system, you will receive regular reports with recommendations tailored to your business.

Am I missing anything?

While this approach considers the current state, make sure to include any new applications as soon as they hit production. Even the latest and greatest systems will be updated at some point. Also, don't overlook the software and firmware that run on your network appliances - physical and virtual. The programs that run your routers, switches, firewalls, and load balancers are still applications.

How do I start?

Take a deep breath and realise this isn't going to happen overnight. Get the right people involved and don't hesitate to put your hand up if you need help. Begin with your current application inventory. If you've recently undertaken an application whitelisting project, this will already be created. 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. Rinse and repeat.

3. Restricting Administrative Privileges

What is it?

In nearly every system, there are accounts that have elevated privileges beyond the everyday users that allow you to add, remove, and change elements. These accounts - including dedicated service accounts for automatic execution - yield considerable power along with the ability to cause untold issues if used inappropriately. Some may consider only the administrator accounts used directly on servers or in Active Directory. However, remember administrative privileges can be local, domain, or enterprise level, and each will have varying degrees of control – this includes power users, domain administrators, enterprise administrators and delegated privileges. Beyond that, they exist on workstations, network appliances, and just about every piece of Internet of Things (IoT) technology.

Where do I start?

As you would have with application whitelisting and patching, an inventory is critical. It will take a while to build a thorough a list of all of your administrator accounts, but the hard work will pay off. Include accounts with elevated privileges and not just local, domain, and enterprise administrator groups. Also, take into account power users and any users with delegated authority. While you're at it, inventory your service accounts as well. For the local administrator accounts on workstations, you will need to determine whether or not users have access. Finally, consider your network capable devices such as routers, switches, firewalls, IoT, and so on.

Any of these devices can have a number of local administrator accounts. It may also be a good opportunity to evaluate your password strategy. With administrator rights comes power and that power must be used wisely.

Any pitfalls?

When it comes to restricting administrative privileges, there are plenty of things that can go sideways. Service accounts can break so be sure to maintain the level of access required by the services and vendors. Maintain a secure local account on your network equipment in the event it cannot reach the domain for authentication. Failure to do this may mean you are unable to fix a router or switch quickly. Failing to deactivate administrator access for employees that change roles or leave the company can also cause headaches.

There may be accounts with administrative access to the most obscure things. You can restrict the ability of a hacker to run riot on your systems by including a degree of accountability for any changes made. This is a solid strategy that gives users a pause-for-thought before clicking OK. There are tools available to help and bringing in the professionals to untangle the mess can be worth its weight in gold.

A good password management application is a big plus too.

The ghost in the machine?

Politics will crop up pretty quickly. Administrative access is a powerful element to the psyche of a user. Taking it away can open Pandora's Box.

At the same time, it can also be the key to locking that very same box. Be ready for the battles that come with taking away admin rights, especially at the workstation level.

Application whitelisting can only help at an endpoint level by controlling installation and execution of programs - you can consider separate privileged accounts for those times when the user 'must' have access and the service desk is swamped. Managers and executives often demand administrator rights, so tread lightly. It's important to find out why they require access before arbitrarily granting power to the powers that be. Auditing and logging systems for privileged account activities should also be a consideration. This means that when things get a little hairy, you can follow the audit trail and quickly resolve the issue.

How do I make it work?

Technically, it's easy - no one is willing to arbitrarily revoke and grant administrator rights. Before beginning, ensure you have a rock-solid policy to underpin your strategy, and make sure it is supported and enforceable by management. The roles of staff should dictate what they can and cannot have access to. Where possible, use security groups rather than assigning admin rights to individual accounts. It's easier to move users in and out of groups rather than worry about individual accounts.

When in doubt, remember to question why the administrator privileges are required and ensure the final decision is backed up with a solid business case.

Am I missing anything?

Don't miss the presence of generic accounts that have administrator privileges. It is best to avoid generic accounts, but if you must have them, restrict them as tightly as possible and log everything they can do. Wherever possible, try to leverage your directory services as the 'source of truth' when logging onto network appliances. Changing the name of default administrator accounts doesn't hurt either. Finally, remember good password practices. There is nothing more regretful than a hacker on the core switch using 'admin' 'admin' to gain access.

How do I start?

Take inventory before reviewing the roles that have administrator privileges. Review your policies, make a plan and run it through proper change management. With a plan in place, you can start on the clean-up. Remember to take your time, restricting administrative privileges won't happen overnight.

4. Patching Operating Systems

What is it?

Patching operating systems shares similarities with patching applications. However, while you are applying updates and patches to your systems, the operating system is critical to making all the other parts in your environment operate. Remember that our favourite applications have to run on top of other software. After all, applications are installed into - or onto - operating systems. It is important to think beyond just the ubiquitous 'Windows' operating systems. Also, consider Mac, Linux, Unix, along with a range of lesser used platforms.

There are also operating systems that run on mobile devices powered by Apple, Android, Blackberry, Microsoft and so on. Also, add to this other network devices and IoT. Virtual or physical, the operating system is the heart of a computer. Think of it like a car - you may have the baddest hot rod on the block (app), but without the engine (operating system), it's useless, and without regular servicing it won't perform at its peak. Critical maintenance updates must be applied.

Like applications, operating systems don't have the luxury of sitting in QA for endless tests as every little bug and detail is corrected and perfected. This means that all operating systems have bugs; some are an annoyance, others are a major security flaw. Vendors know this. Whether the vendor catches it, or users bring the issue to their attention, they're constantly working on making their product better, safer, and more productive.

Take the notorious WannaCry ransomware attack, or the mayhem created by the Petya/NotPetya malware. These destructive program worms had global impact. You may also be aware there was a patch available prior to the outbreak. Nonetheless, the infection flourished. If you ever needed a case for regular patching, this is it.

Where do I start?

For Microsoft aficionados, Patch Tuesday is a thing and has been for a very long time. This doesn't mean that patches and updates aren't available at other times. Ask your team how patching is handled, how patches are acquired from the vendor, tested, and deployed. If it's a case of checking once in a while or whenever you have time, you should look at making this part of your regular security maintenance. Ask the questions and get the right people involved to understand your patching and updating strategy. Ideally, you want central control and distribution so you don't have 500 users downloading the same patch 500 times, let alone a patch that may cause issues. Understand what the patch is, what it impacts, and if you even need it.

Any pitfalls?

Plenty. However, in reality the biggest pitfall comes from not actually doing any patching at all. Keep in mind, not every update fixes every problem. Sometimes they can cause other issues, which is why patches should be tested prior to deployment - unless it's absolutely critical. Scheduling of patches needs to be handled right.

You don't want to reboot someone's computer when they're trying to make a deadline or have open documents with a lot of unsaved changes. Things can and do go wrong. It's important to remain cautious but doing patches is far better than doing nothing at all.

As we recommend with application patching, consider implementing vulnerability management services using dedicated applications managed either in-house or through your managed services provider.

The ghost in the machine?

Human error will always be a factor. People overlook patches, miss computers because they were offline and incorrectly assign patches to computers that don't need them. No doubt there will always be at least one user that simply cannot be interrupted or can't be bothered rebooting their computer. Implementing some checks and balances can help mitigate these potential landmines.

How do I make it work?

If you're not patching your operating systems, start now. There are plenty of applications available that can scan your network, identify the patch levels of computers, and provide a report to advise which systems need which patches. Get those patches, test them, and deploy them but try to automate the process as much as possible. There will always be systems that cannot be updated or must be done manually. You may also need to get management involved to help enforce the idea that computers have to be patched and users cannot simply ignore the updates because they will put more than just themselves at risk.

While it may be tempting to spend time evaluating every single patch that gets released, perhaps consider working with someone that understands your infrastructure - like a managed service provider - and have them either provide advice or oversee the patching entirely.

Am I missing anything?

Just remember the non-Windows systems such as Linux, Unix, Mac, and mobile platforms like Apple, Android, and Blackberry. If you haven't included network devices and IoT in your application patching strategy, include them here. They're all part of your extended IT family.

How do I start?

Remember to ask questions. Find out what your patch management strategy for operating systems is, and ask if you can do anything better. Talk with managed services providers and specialists in patch management. Implement a regular, scheduled patching regime and allow for the occasional emergency update. Include change management process in the strategy. Finally, decide which patches are needed, test, and deploy.

5. Disabling Untrusted Microsoft Office Macros

What is it?

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. Unfortunately, macros are also a popular exploit as it is possible to leverage this autonomy and to execute code, sometimes even reaching even beyond the application itself. Anyone that has been around for a long time will remember the Melissa macro virus and the havoc it caused with email services worldwide. Then there's the Wazzu macro virus that altered the content of files. Most of this is due to Visual Basic for Applications (VBA), which is still used to this day. Microsoft, to their credit, has done a tremendous amount of work to secure macros in the past several versions of Office, but you can't save people from themselves.

Where do I start?

It might be tempting to simply disable all macros full stop, but that isn't the answer. Remember that macros exist for a reason and that's to automate tasks, save time, and release users from tedious tasks. A better approach is to selectively trust macros but remove the choice from the end user. How do we trust macros? Digitally sign them and then lock down the application to disable all but the signed ones.

How do I digitally sign macros?

This is where it can get complex. While there are tutorials covering how to self-sign digitally signed macros, self-signed certificates really don't inspire any trust in the broader community. The availability of a Public Key Infrastructure (PKI), either internal using the Microsoft solution or external using a third party, trusted Certificate Authority (CA) is preferred. Start exploring digital signing of your macros and get the right people involved before moving ahead. Unless you have the in-house skills, seeking assistance may be required. On top of digitally signing and distributing your macros, you also need to consider policies that lock down these features in Microsoft Office applications. This will prevent savvy users from disabling their protection to run all macros anyway.

If your environment doesn't require macros, disabling them completely is fine. That said, not many of these environments actually exist.

Any pitfalls?

There can be a lot of moving parts, so planning is critical. Consider group policies, restricted privileges, macro control and distribution, digital signing and PKI and you will quickly see how easy it could be to come off the rails. It's important not to throw this in the 'too hard bucket'. There is a lot to gain when macros are managed correctly, especially in an environment where the productivity can be impacted tenfold by their proper use but a hundredfold by their exploitation.

The ghost in the machine?

The macros themselves have to be trusted. If a user makes a mistake and then trusts that mistake, digital signing won't make an ounce of difference. You must QA the macros and thoroughly test them before using them. Human error, as with all things, is omnipresent.

How do I make it work?

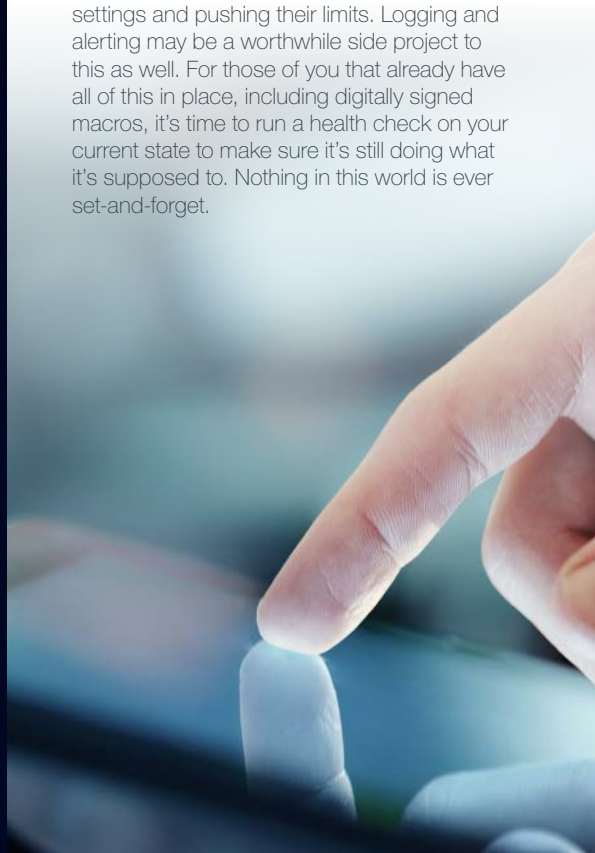
Determine if you need macros. If not, you can implement a blanket policy to disable them across the board and move on. For non-domain systems, just disable them in your applications. For the majority that require macros, you'll need to take inventory of all macro. Delete the unused ones and begin the process of vetting the ones that are used. Digitally sign your required macros after thorough QA and testing, and then distribute and control as needed. Ideally, you should never execute an untrusted macro unless you're the ones that developed it and are trying to make it legitimate.

Am I missing anything?

It's worth considering macros in applications other than Office. Microsoft isn't the only one that figured out macros are incredibly powerful and popular.

How do I start?

Find out what your current policy is on Microsoft Office macros, and if you don't have one, consider creating one. As previously discussed, this can be complex with a lot of moving parts. Unless you have the resources like in-house skills and PKI, put up your hand and ask us to help you. If you have the resources, look at locking down your macros and controlling their distribution and the end user control over the applications. People are very skilled at finding ways to bypass security settings and pushing their limits. Logging and alerting may be a worthwhile side project to this as well. For those of you that already have all of this in place, including digitally signed macros, it's time to run a health check on your current state to make sure it's still doing what it's supposed to. Nothing in this world is ever set-and-forget.



6. Using Application Hardening

What is it?

Think of application hardening like spring cleaning on top of a minimalist lifestyle. You keep only what you absolutely need after taking stock of what you have. Many applications are installed with defaults and as a result, many options, services, and capabilities enabled. Everyone is guilty of installing applications this way, being more interested in using the program than securing it. Default usernames and passwords, insecure services, default SNMP communities, anonymous access - the list goes on. Hardening these applications renders them more secure and less likely to be used against us. Every organisation has applications on their infrastructures that could have a negative impact if used incorrectly or maliciously. Reducing that possibility only makes sense. Controlling who can access an application, what the application can do, and revisiting this on a regular basis or after significant changes, is a smart approach.

Where do I start?

If you have undertaken an application whitelisting exercise or similar that required a full inventory of your applications, you have a big head start. Otherwise, it's time to make that list. It goes without saying that if you don't need it, get rid of it. You'll probably discover applications you never knew you had. List in hand, you can check with the vendors to see what their hardening recommendations are or even use the industry best practices to better secure your environment.

It should go without saying that you should change default usernames and passwords. It's surprising how often this is overlooked. If the application uses a service that is not essential, consider disabling it or, if possible, uninstalling that component completely. This can often be completed through the installation wizard - if the app uses one. Use non-default program folders to fool exploits that go looking for default installation locations. Close network ports unless required and for applications that use random ports, try to statically define these ports and adjust your firewall and security policies accordingly.

Another good tip is to leverage open source or commercial tools for vulnerability scanning. They will often locate vulnerable services that can be considered for hardening, disabling, or removal. Available 'as-a-Service, you can engage a provider to manage the solution.

Any pitfalls?

Many. Unless you harden your applications correctly, you may be effectively committing a denial-of-service attack against yourself. Some applications may just need 'insecure' services or settings, which will have to be accepted but can be guarded using a defence-in-depth strategy. Ensure that your approach allows for functionality as well as security. The most amazing applications are pointless if we can't use them due to security settings. Asking the right questions to the right people, testing, and change management is crucial.

The ghost in the machine?

Shadow IT seems to creep into our systems using grey applications, which are neither explicitly approved or denied for their use in the infrastructure. These 'unauthorised' programs can provide a quick and dirty workaround, but unless secured, can present a bigger risk to your environment. Shadow IT exists often when users feel the tools they are given are inadequate or unduly restricted, among many other reasons.

How do I make it work?

Once you have an inventory of applications, find out how to secure them using either vendor or industry best practices. Test these changes to understand what you can and cannot do, then run them through change management, while also considering the benefits and any potential negative impacts. Office politics will always be present when dealing with issues of control, so management support and enforcement is a good idea. Once the logistics have been looked after, set about implementing the changes. Unless you can control the changes through large-scale distribution, it can be a bit cumbersome. Putting all required hardening into a base image helps, followed by implementing the hardened applications through distributed software points, so the hardening is already embedded.

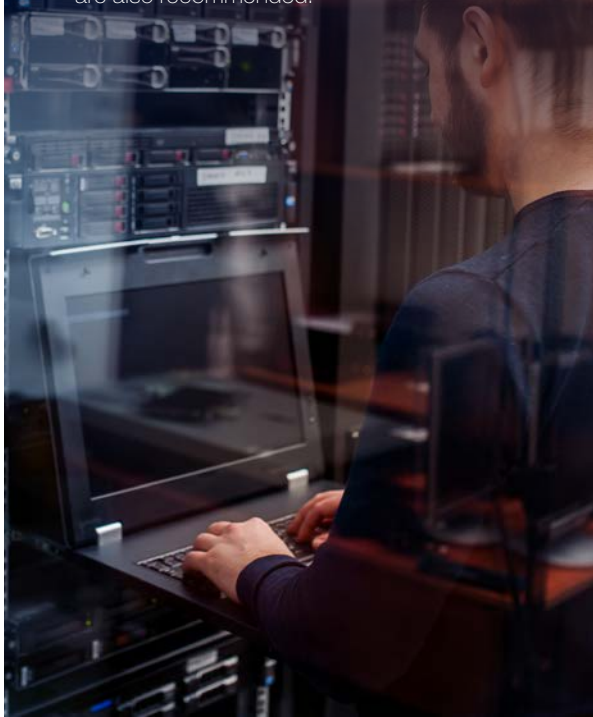
Am I missing anything?

It doesn't hurt to look at network appliances that may be running default services that are not used or may be insecure. Network printers and multi-function devices, UPS systems, routers, switches, and more, may be considered if one is undertaking a hardening exercise. FTP, SNMP, HTTP, TELNET and more, are often running on these devices and may present a risk.

Don't overlook patching your applications and enabling relevant logging and auditing.

How do I start?

As with most things, begin with a current state inventory to understand what you have. Understand how best to secure these applications and create a plan to address these issues. Perform proper testing and QA and ensure that proper change control is followed. Management support is important, so the initiative is viewed as not just an IT approach, but a business approach. Work your way methodically through the systems with a goal of allowing secure functionality of your applications. Regular reviews, such as after major upgrades or staffing changes are also recommended.



7. Multi-Factor Authentication

What is it?

Multi-factor authentication (MFA) adds another layer of security by forcing you to provide another means of identifying yourself. In some cases, it may include multiple means. So, what is the first factor? It's usually a username and password. MFA already exists in many other facets of our lives. For example, when you apply to lease a property and must provide several pieces of identification.

MFA is not new, but it is gaining considerable momentum. You may recall key fobs with a code that changed at set intervals. You entered your username and password, and then the code displayed on the fob. It is assumed that only you have that fob, thus providing a secondary way to identify whoever is logging in is whom they say they are. It isn't perfect, but it does improve security. While these fobs still exist, they appear to have been supplemented by - or replaced by - mobile apps, SMS codes, and other methods. Even smart cards are still very much in use.

On top of those methods, we're also seeing the proliferation of biometric authentication into the consumer market through fingerprint scanners and touch IDs on mobile devices. There are many options and given the current threat landscape, there is no reason it shouldn't be considered. If it's available, use it. If you have a cloud-centric strategy, it's quickly becoming a must rather than an option.

Where do I start?

Let's assume that you already have a solid username and password strategy and if you don't, stop reading and make that happen first. For the rest of us, we need to consider what we're safeguarding - implementing MFA can be expensive and time consuming. Take stock of your present situation. You will probably find that you have some systems that are more critical than others. Begin there. As with all strategies in the Essential Eight, make sure you ask the right questions and get the right people involved.

Perhaps use of an authentication app will suffice - such as those available from Microsoft or Google - and can be installed on your mobile. Maybe you're looking for a smart card solution, biometrics, or a combination of factors. Remember that while it needs to be secure, it needs to be usable. Fewer things can be more frustrating than taking what feels like forever just to log in. Combined with multiple systems that don't share credentials, you're just asking for trouble, so it may also be time to consider Single Sign-On options.

Spend time up front to figuring out what will be the most usable solution for you and what will deliver adequate security. Then set about implementing it in a phased approach. It may seem like a challenge, but adding that extra layer can mean the difference between a hacker infiltrating your intellectual property versus them moving on to a softer target.

Any pitfalls?

Unless your organisation is greenfield, you will need the implementation to be gradual and well received by those used to just typing in their username and password. Hopefully, by now you've already managed the nightmare known as password complexity requirements.
Users may often see this as just another obstacle in getting their work done, so explaining why is beneficial.

Be prepared for resistance from users that refuse to install company-mandated apps on their personal devices. Even if you allow them to expense part of their devices, it can be seen as intrusive. Policy can help, or you can consider other means such as SMS, biometric, smart cards, or old-school fobs. Whichever you choose, be ready for user pushback.

The ghost in the machine?

As with everything else, we humans seem to get in the way of perfect solutions. We lose our phones and are unable to log in. The same goes for smart cards and fobs that get left at home or lost. Even technology itself can let us down, so even if you have your phone but your battery is dead there are plenty of ghosts. Always have a Plan B to make sure users can get in when they need to. This is doubly critical for management and executives who may often refuse to accept there is an 'issue' that prevents them from getting their email and logging in to their computers.

7. Multi-Factor Authentication (continued)

How do I make it work?

Start with a plan. Implementing MFA is important, but it needs to be done for the right reasons and implemented correctly. Evaluate what you are protecting and why. Also involve the users early on – the last thing you want to do is suddenly drop it on the staff. As humans, we don't like change. Evaluate your options and thoroughly understand the pros and cons of each solution. If you need help, consult with MFA specialists who can help you find the best solution using the right combination of vendor products and services.

Trial your solution with a pilot group, learn from the experience, then begin a phased roll-out. Throughout the whole experience, always bear in mind the end users who will have to use the solution. In an environment with many systems, you may need to also consider Single Sign-On as well.

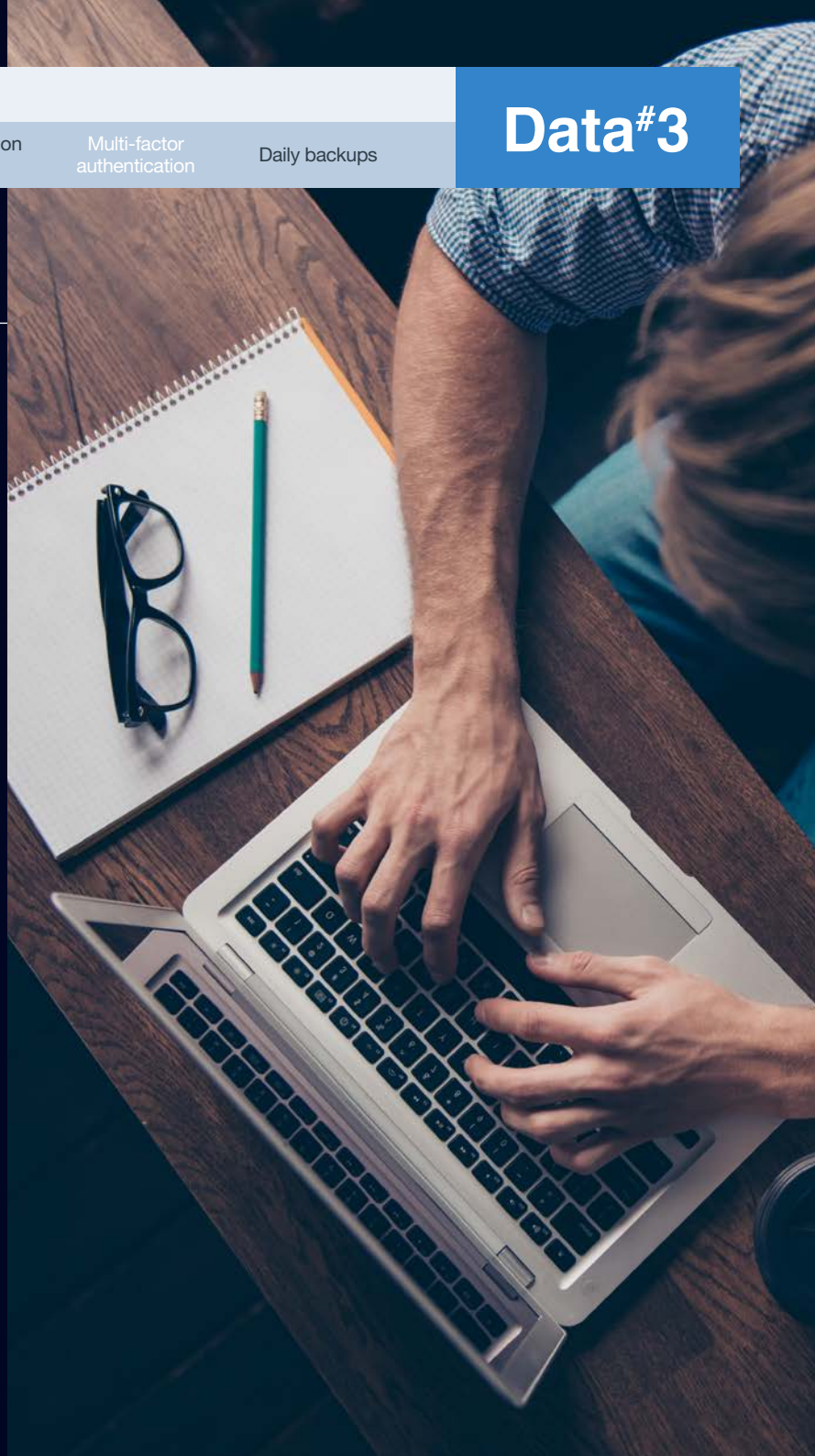
Am I missing anything?

In addition to considering mandatory work arounds for those times when something gets a little sideways, you really need to consider the personal angle. Use MFA on everything you can – email, remote access, social media, banking, and so on. Be ready to defend yourself as an individual as well as your enterprise.

Most popular platforms such as Outlook, Gmail, Facebook, and Twitter, all leverage MFA, so get hands-on and set it up. A personal breach may give an attacker enough information to launch an attack on your enterprise – especially if you're in the management tier of your organisation and a more attractive target.

How do I start?

Ask the questions to determine what your present stance is on MFA, and if you don't have it, ask if you should. If you already have it, ask if you can do it better or more securely. Always be willing to go back and re-assess, aligning your security posture with the present threat landscape. Once you have the answer to these questions, take action.



8. Daily Backups

What is it?

Backing up your data has been a long-standing strategy in safeguarding your information when things go wrong. Servers crash, laptops get lost, files get deleted accidentally, and mistakes are made. Mistakes - accidental or intentional - can have severe repercussions that require recovering your data such as in the event of a ransomware attack. Whatever the reason, the fact remains you should have a backup copy of your important data.

There are many options, at many different price points, that will suit everyone from individuals to large enterprises. These include magnetic and optical media, cloud-based storage such as iCloud, OneDrive, and Box, and even all the way up to Disaster Recovery (DR) sites. The latter can be fully functional exact replicas of production data centres with 100% live replication, to warm standby sites, to even cold sites ready to build from scratch and restore your data. In short, you have options, but you have no excuses.

Just as critical as backing up your data is the ability to restore it and use it without it being incomplete, corrupt, or completely inaccessible. Otherwise, it's like a one-way ticket to somewhere you can't get back from. You should consider replicating your data to a secondary data centre, backing it up to the cloud, or backing up to removable media such as tapes and storing it securely offsite.

Where do I start?

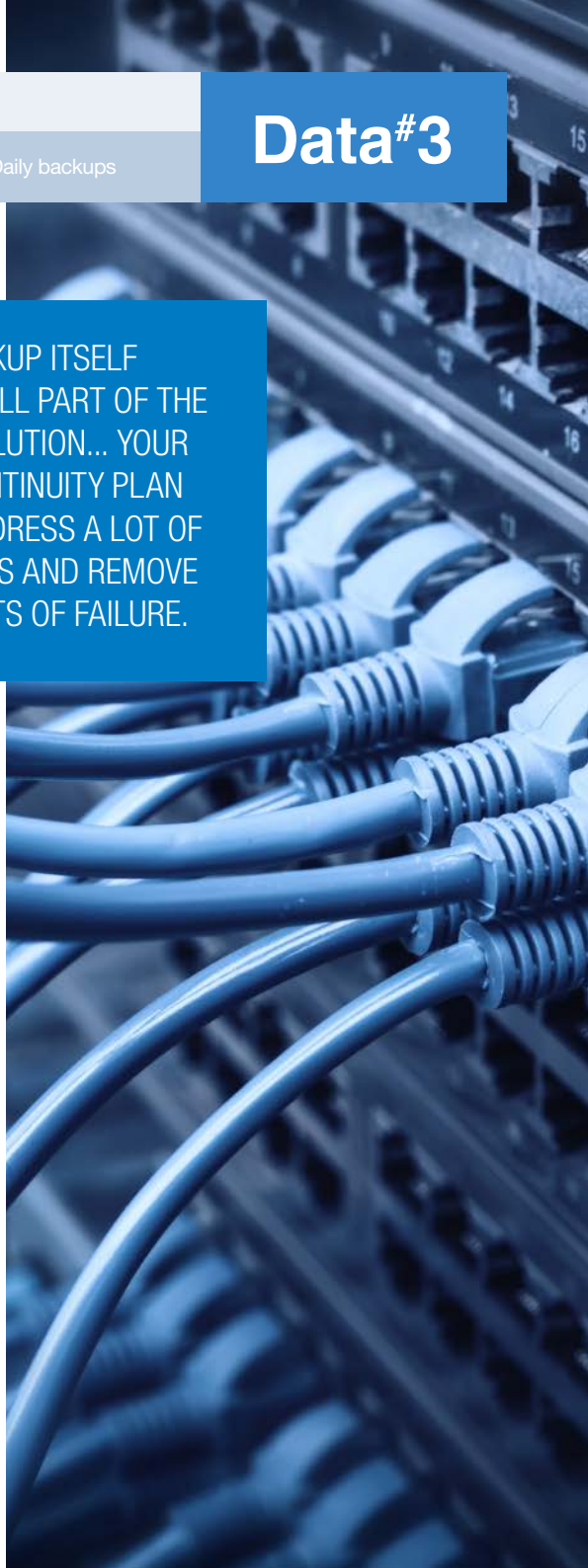
If you have data, you need to back it up, so the first part is already determined. Depending on service level agreements and who is responsible for your data, either on-premises, hosted, or cloud-based, a number of other factors need to be considered. How long can you be down before you have to have your services and data available? How much work can you stand to lose in the event you need to restore? Figuring out your Recovery Time Objective (RTO) and Recovery Point Objective (RPO) may determine your investment in the solution, and it needs to be a business-led conversation - not just technology. If you don't have a plan, you'll need to create one. If you already have a plan, it may be time to review it to make sure it meets your current objectives.

Determine what you need to backup in a prioritised order, and how to back it up. Will you do full backups every day, or a full backup once a week with incremental daily backups? Will you use tapes, cloud, or replication to a DR site? Will you rotate media off site on a regular basis and how quickly can you get that media back when you need it?

The backup itself is just a small part of the overall solution. Your DR/Business Continuity Plan (BCP) needs to address a lot of moving parts and remove single points of failure. For example, if John is expected to be the one that kicks off the restore, but he's in Bermuda on a fishing trip without his mobile, someone needs to do his job.

Regular testing, including full-scale DR exercises, are highly recommended. Whether you need to restore a file for someone in HR or recover a 10 TB database, your system has to work.

THE BACKUP ITSELF IS JUST A SMALL PART OF THE OVERALL SOLUTION... YOUR BACKUP CONTINUITY PLAN NEEDS TO ADDRESS A LOT OF MOVING PARTS AND REMOVE SINGLE POINTS OF FAILURE.



8. Daily Backups (continued)

Any pitfalls?

A common pitfall is not adjusting backups to allow for new servers, data stores, or applications. This means when new systems and data come online, they're not captured in the backup scheme. Also, commonly overlooked are device backups such as firewall and router configurations. If a device falls over, its replacement or the device itself can be quickly brought back up to speed. Another common pitfall is backing up everything for no reason. It's all well and good to capture every tiny bit of data, but not at the cost of bandwidth, storage capacity, or at the risk of over-writing critical information. Plan, execute, review, adjust the plan, repeat.

The ghost in the machine?

The list of things that can go wrong is extensive, but simply assuming the backups will work every time is hazardous. As with all technology, things can, and do, go wrong. We all have stories about how our backups let us down at the worst time possible. You simply have to stay on top of things, even if it's feeding the logs into another system so we can quickly check the status of our backups and right the ship. Like a good insurance policy, you need it to be there when it matters.

How do I make it work?

Rather than just jumping straight into backing up files, make sure you have a plan in place. Ideally, this should be a part of your overall DR/BCP. Identify what you are backing up and why, the priority of the data, the recovery time and recovery point objectives, and how it is being backed up. Equally important is how data gets restored and by whom, when, and where. Don't overlook the value of annual full-scale, live DR testing and regular revisions to the plans. Also, remember to include any new systems and their data as well as any storage location movements. Vendor support and even support by a managed services organisation can be worthwhile.

Am I missing anything?

While you're at it, it's time to evaluate backing up your personal data. Far too many of us fail to backup our home data and files, so with a wealth of cheap and cheerful options such as personal iCloud, OneDrive and GDrive, we've plenty of options. Just be wary of your bandwidth usage.

Also, watch out for data stored on local drives of workstations and laptops - anything business critical should be stored on the corporate servers.

How do I start?

Ask questions, get informed and if need be, get the right people involved. The ability to backup and restore critical information can mean the survival of your enterprise. Among the Essential Eight strategies, this one has probably been around the longest, but is most likely the one that gets overlooked the most. Make sure that any future changes to your data includes a section in change management to consider the backup and restore impacts.

Data#3

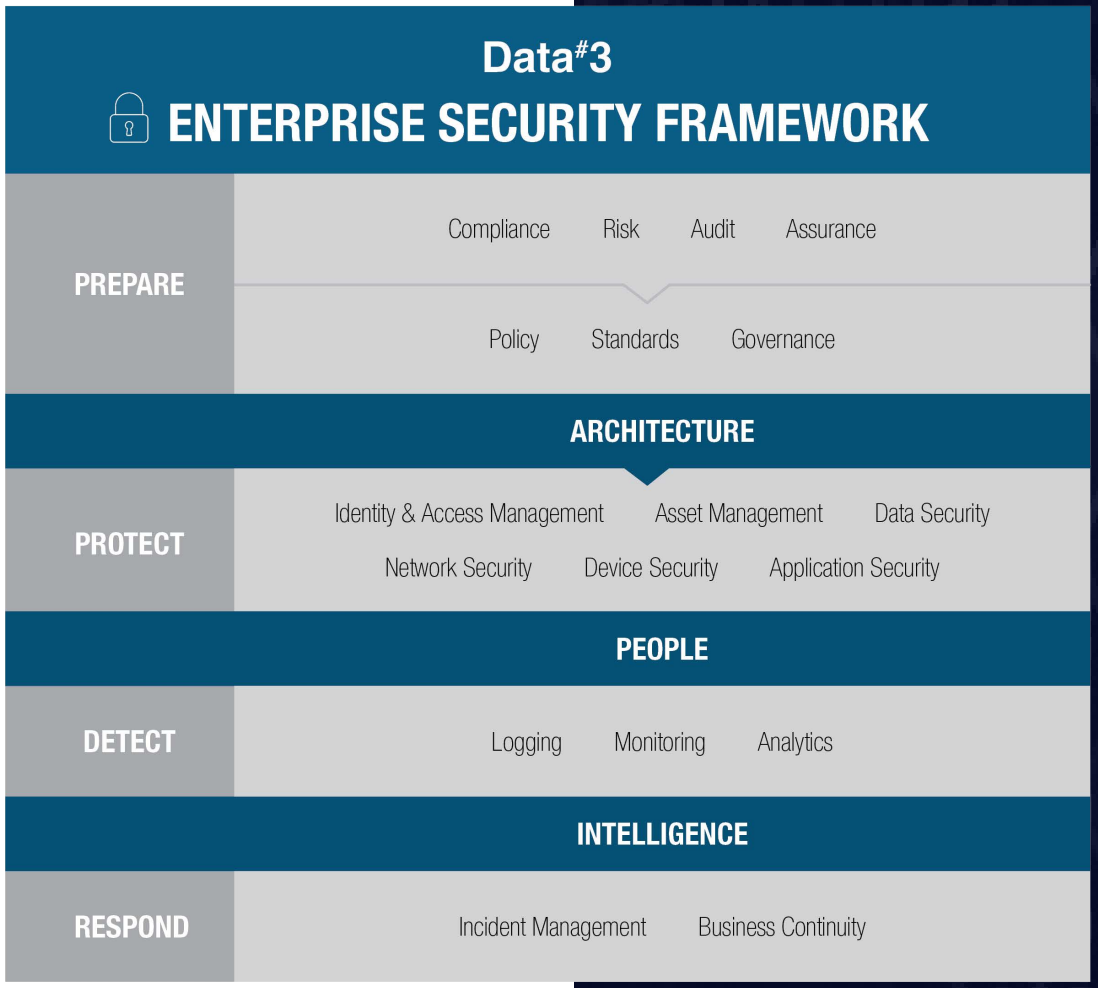
Are You Ready to Develop and Implement an Essential Eight Strategy?

While implementing the strategies discussed in this document can seem like a monumental task, rest assured that help is readily available to define, develop, and implement an Essential Eight Strategy that is right for your business.

Your organisation may have already completed a few of the elements, while others may be in the pipeline or yet to be considered, but please understand that you are not alone.

At Data#3, we help organisations stay one step ahead of cybersecurity threats by focusing the conversation on risk management. We will work closely with your stakeholders, cybersecurity teams, and service providers to achieve your information assurance goals and bolster your defences, incident response, and capability to recover.

Our comprehensive Security Framework forms the basis of our engagement:



For more information, visit
www.data3.com.au/security
or contact a Data#3 security specialist.

1300 23 28 23
www.data3.com.au

Brisbane (Head Office)
67 High Street
TOOWONG, QLD
4066, Australia

Melbourne
Level 4,
55 Southbank Boulevard
SOUTHBANK, VIC
3006, Australia

Sydney
107 Mount Street
NORTH SYDNEY, NSW
2060, Australia

Launceston
23A Earl Street
LAUNCESTON, TAS
7250, Australia

Adelaide
84 North Terrace
KENT TOWN, SA
5067, Australia

Canberra
Level 3,
65 Canberra Ave
GRIFFITH, ACT
2603, Australia

Hobart
16 Collins Street
HOBART, TAS
7000, Australia

Perth
Level 2, 76 Kings Park Road
WEST PERTH, WA
6005, Australia

Fiji
Suva Business Centre
217 Victoria Parade
Suva, Fiji

Follow Us:

twitter.com/Data3Limited
facebook.com/Data3Limited
linkedin.com/company/Data3
youtube.com/Data3Limited

Data#3