Kaine Mathrick
TECH

Best Cyber Security Practices For Business For 2023

Your comprehensive guide to safeguard your business data and systems against cyber attacks.

Based on the ACSC Essential Eight Maturity Level 2.

TECH

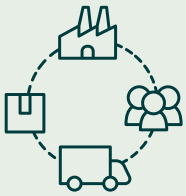
Key factors behind an expanding attack surface

Increased remote working arrangement

Increased hybrid working & remote working.
The remote work trend continues, creating a lack of visibility and control over employees. Remote environments are harder to secure, as they lie outside organizations' perimeters. Hybrid work environments are also a source of risk, as they expand the area of potential attacks. When cybersecurity officers must protect both in-house and remote environments, ito increases the possibility of human error and, eventually, a breach.

Business shifting to the cloud

Migrate data to the cloud.
Majority of Australian businesses operate mainly or partly online and many more of enterprise IT spending will shift to the cloud. Securing cloud infrastructure may be challenging due to the increased number of attack vectors, the complexity of cloud environments, and the sharing of security responsibilities between the client and the cloud services provider.



Supply chain interactions

Supply chain risk monitor.
The supply chain continues to be a common point of cybersecurity failure. As the number of third parties you connect and interact with grows, so does the potential for hackers to access your infrastructure.

Convergence of IT with OT and IoT

IT/OT-IoT convergence.
Security measures and protocols for Internet of Things (IoT) and operational technology (OT) devices are still developing, exposing IT systems to cybersecurity risks. Cyber attackers may use IoT and OT devices as entry points into your organization's systems.

Cyber-First Approach For Businesses

Developing cloud security

The rapid rate of cloud migration in recent years hasn't left time for cybersecurity to catch up. Poorly secured remote work environments that cloud services are often accessed from and other cloud vulnerabilities are pushing the cloud security industry to develop fast. Gartner predicts the cloud security sector to have strong growth in 2023–2024.

Implement zero trust policy

The zero trust approach is both secure and scalable which always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.
It also limits user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data and productivity. Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defences.

Cyber-First Approach For Businesses

Augmenting supply chain infrastructure

In 2023, cyber security specialists are expected to pursue new ways for protect supply chains and develop existing methods of cyber supply chain risk management. This is mostly a response to cases of espionage, state-driven cyber-attacks, and geopolitical disturbances that affect the global supply chain. For instance, Russia targeted technology involved in running critical Ukrainian infrastructure in February 2022.

How to protect supply chain

- Access your chain risks
- Establish a cyber supply chain risk management program
- Collaborate with suppliers on improving your mutual security
- Limit subcontractor's access to your resources
- Monitor vendors' activity within your IT infrastructure

Stricter requirements for cyber security compliance

Governments worldwide are advancing their efforts to secure their citizens' personal data. It's been predicted that in 2023, 65% of the world's population will have their personal data covered under modern privacy regulations, up from 10% in 2020.

How to balance privileges with user needs

Zero trust model	Only granted to authenticated & verified users
Principle of least privilege	Only given to access the information & resources necessary for a legitimate purpose
Just-in-time approach	Only given to the right users, to certain systems and resources, for a valid reason and for a specific time

Cyber-First Approach For Businesses

Rise of threat detection and response tools

The only way your organization can efficiently handle an attack is by detecting suspicious user activity in your infrastructure and reacting to it promptly. Threat detection and response solutions are designed for just that.

Key practices to reduce the risks of privileged user and third-party access

- Monitor user activity
- Restrict access to sensitive data
- Provide one-time passwords
- Approve access request manually

Top 8 Cyber Security Best Practice For Australian Business

While no set of mitigation strategies are guaranteed to protect against all cyber threats, organisations are recommended to implement eight essential mitigation strategies from the ACSC's Strategies to Mitigate Cyber Security Incidents as a baseline. This baseline, known as the Essential Eight, makes it much harder for adversaries to compromise systems.

This best practice guide is based on ACSC Essential Eight Maturity Level 2 guidelines which will focus on the adversaries who are willing to invest more time in a target and, perhaps more importantly, in the effectiveness of their tools.

- Generally, adversaries are likely to be more selective in their targeting but still somewhat conservative in the time, money and effort they may invest in a target.
- Adversaries will likely invest time to ensure their phishing is effective and employ common social engineering techniques to trick users into weakening the security of a system and executing malicious code, for example, via a Microsoft Office macro.
- Adversaries will also often seek to compromise user accounts. If successful, they may seek to exploit privileges associated with these accounts or escalate privileges to higher levels.
- Depending on their intent, adversaries may also seek to steal or destroy data (including backups) or make data otherwise unavailable through various denial-of-service techniques.

The practice guide below outlines the requirements to be assessed in addition to the requirements of the Essential Eight maturity level 1.

Application control

For Maturity Level Two, application control requires the use of a dedicated application control solution. This may be one of the in-built solutions from Microsoft (e.g. AppLocker or Windows Defender Application Control) or it may be a third-party solution (e.g. AirLock Digital's AirLock, Ivanti's Device and Application Control, Trend Micro Endpoint Application Control or VMWare Carbon Black App Control).

- Application control is implemented on workstations and internet-facing servers.
- Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.
- Allowed and blocked execution events on workstations and internet-facing servers are logged.

Patch applications

At this maturity level, the timeframe for patching security vulnerabilities in internet-facing systems is decreased from one month to two weeks. In addition, this maturity level introduces patching timeframes for additional applications, and an increase in associated vulnerability scanning frequencies and scope.

- A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.
- A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in other applications.
- Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release.
- Patches, updates or vendor mitigations for security vulnerabilities in other applications are applied within one month of release.

Configure Microsoft Office macro settings

At this maturity level, an additional requirement is introduced relating to the use of the Attack Surface Reduction (ASR) rule ‘Block Win32 API calls from Office macros’. This ASR rule prevents Microsoft Office macros from calling Win32 APIs, which adversaries can exploit to run malicious code that is more powerful than the actions they can perform using the Microsoft Office VBA macro language itself.

Event logs for Microsoft Office macro execution events should be collected and stored in case there is a cyber security incident and they are required for forensic or incident response purposes. Often, the lack of sufficient logging can impact the ability to determine the extent of a cyber security incident, how it occurred and what security vulnerabilities need to be mitigated.

- Microsoft Office macros are blocked from making Win32 API calls.
- Allowed and blocked Microsoft Office macro execution events are logged.

User application hardening

This stage requires the implementation of several (Attack Surface Reduction) ASR rules to prevent adversaries from using Microsoft Office applications to create child processes that can be used to download and run malicious code, write malicious code to disk or inject malicious code into other processes. In addition, the ASR rule ‘Block Adobe Reader from creating child processes’ should be implemented to prevent adversaries from using Adobe Reader to create child processes which can be used to download and run malicious code.

Adversaries often attempt to exploit security vulnerabilities in Microsoft Office through its support for Object Linking and Embedding (OLE) packages. This maturity level requires Microsoft Office to be configured to prevent activation of these OLE packages.

- [ ] Microsoft Office is blocked from creating child processes.
- [ ] Microsoft Office is blocked from creating executable content.
- [ ] Microsoft Office is blocked from injecting code into other processes.
- [ ] Microsoft Office is configured to prevent activation of OLE packages.
- [ ] Microsoft Office security settings cannot be changed by users.
- [ ] PDF software is blocked from creating child processes.
- [ ] PDF software security settings cannot be changed by users.
- [ ] ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented.
- [ ] Blocked PowerShell script execution events are logged.

Restrict administrative privileges

To avoid users collecting privileges and access as they change roles throughout an organisation, and to enforce the principle of least-privileged role-based access control, privileged users should be required to regularly revalidate their requirement for privileged access. As such, privileged accounts that have not been used within 45 days strongly indicate that they are no longer required.

Rather than accounts remaining active, and a possible target for adversaries to exploit, inactive accounts should be disabled on a regular basis.

Event logs relating to the use of, and changes to, privileged accounts should be collected and stored in case there is a cyber security incident and they are required for forensic or incident response purposes. Often, the lack of sufficient logging can impact the ability to determine the extent of a cyber security incident, how it occurred and what security vulnerabilities need to be mitigated.

- [ ] Privileged access to systems and applications is automatically disabled after 12 months unless revalidated.
- [ ] Privileged access to systems and applications is automatically disabled after 45 days of inactivity.
- [ ] Privileged operating environments are not virtualised within unprivileged operating environments.
- [ ] Administrative activities are conducted through jump servers.
- [ ] Credentials for local administrator accounts and service accounts are long, unique, unpredictable and managed.
- [ ] Privileged access events are logged.
- [ ] Privileged account and group management events are logged.

Patch operating systems

At this stage of implement, the timeframe for patching security vulnerabilities in operating systems is decreased from one month to two weeks. In addition, this maturity level requires weekly vulnerability scanning.

- A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in operating systems of workstations, servers and network devices.

- Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release.

Multi-factor authentication

At maturity level 2, an additional requirement for all privileged users logging onto systems, both locally and remotely, to use multi-factor authentication is introduced.

In addition, the authentication methods that can be used, and in what combination, are restricted to avoid weaker implementations. Specifically, acceptable multi-factor authentication implementations include:

Something users have (i.e. look-up secret, out-of-band device, single-factor one-time PIN (OTP) devices, single-factor cryptographic software or single-factor cryptographic device) in addition to something users know (i.e. a memorised secret)
Something users have that is unlocked by something users know or are (i.e. multi-factor OTP device, multi-factor cryptographic software, or multi-factor cryptographic device).

Event logs for multi-factor authentication events should be collected and stored in case they are required to support forensic or incident response activities following a cyber security incident.

- Multi-factor authentication is used to authenticate privileged users of systems.
- Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are.
- Successful and unsuccessful multi-factor authentication events are logged.

Regular backups

In this stage of guideline, privileged accounts (with the exception of backup administrator accounts) are limited to only accessing their own backups and should not be able to modify and delete backups.
It is important that backup administrator accounts (as well as user accounts in general) are provisioned following the principles of least privilege and separation of duties. As such, backup administrator accounts should only be given to a small group of trusted administrators and a separate group should be setup for the purpose of restoring backups.

Excessive permissions for accounts increases the chance that they will be compromised. Should this occur for these accounts, adversaries performing ransomware attacks can easily encrypt or delete all backups. Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts.

- Privileged accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.

5 Principles Of Directors' Obligations In Relation To Cyber Security

- Your enterprise management include regular and ongoing consideration of cyber security: Conduct cyber-first policies Including risk assessment and investment in the development and implementation of a resilient digital strategy.
- Keeping informed about the company's cyber security risks and the measures in place to address them
- Ensuring the company has policies and procedures in place to manage cyber security risks
- Ensuring that the company has adequate resources to address cyber security risks
- Ensuring the company has appropriate security controls in place for its information and technology systems
- Ensuring that the company has processes in place to respond to and recover from cyber security incidents

Need Help? We'd love to hear from you!

Take a cyber-first approach with your cyber security policy, and we're here to bridge the gap between technology and humans as your technology partner. Kaine Mathrick Tech has over 12 years experience providing Cyber-First Managed Services that scale with your business across Australia.

To understand where your cyber posture sits against Essential Eight, take our Assessment.

You can access to more resources at www.kmtech.com.au or you can contact us at info@kmtech.com.au we'd love to hear from you and see how we can help!

info@kmtech.com.au

1300 400 266

KM TECH