Maturity Uplift for the Essential 8 and the "Further Five"

Steve Woods

April 2025

CISO Perth 2025

GOVERNMENT OF WESTERN AUSTRALIA

Western Australian Government Cyber Security Policy

2024

2024 WA Government Cyber Security Policy

1 Govern
Establish essential governance and foundations of cyber security management.

2 Identify
Identify elements of your entity's cyber security environment and manage its cyber security risks.

3 Protect
Protect your entity's critical services and information holdings.

4 Detect
Detect and diagnose a cyber security incident.

5 Respond
Respond to an identified cyber security incident.

6 Recover
Recover from the impact of a cyber security incident and restore capability, services and information.

3. Protect

Protect critical services and information holdings.

3.1 Australian Cyber Security Centre (ACSC) Controls

3.1.1 The "Essential Eight"

Each entity must:

a. Implement the set of technical controls comprising the ACSC's Essentia Eight controls to Maturity Level One as defined by ACSC in November 2022 as the minimum baseline maturity level and continue to Maturity Level Two where appropriate.

b. Based on its cyber security risk assessment, the entity should decide whether the entity requires a level of maturity higher than Level One fo any of the Essential Eight controls to manage its cyber security risks.

For more information, please refer to:

- ACSC – The Essential Eight
- ACSC – Essential Eight Maturity Model

3.1.2 The "Further Five"

In addition to the "Essential Eight", each entity must implement the "Further Five" mitigation strategies,[5] unless your entity's cyber security risk assessmen determined that they were not required.

The Further five include:

1. server application hardening
2. block spoofed emails
3. network segmentation
4. continuous incident detection and response
5. personnel management.

ABC NEWS

Just In | For You | Politics | World | Business | More

Cyber Security 9h ago

NSW court website involved in major data breach, 9,000 documents leaked

Approximately 9,000 court documents, including apprehended violence orders and affidavits, have been downloaded following a major data breach to the NSW Online Registry website.

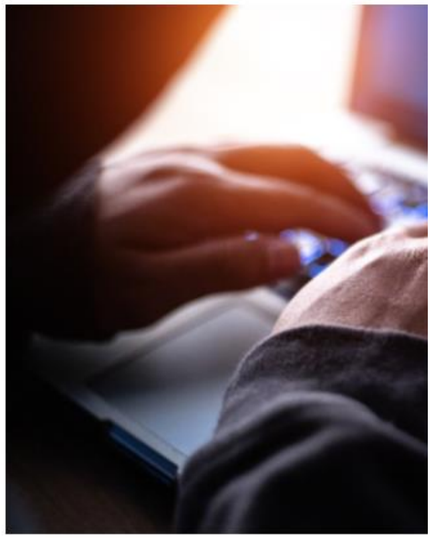
News

Published: 13 days ago Updated: 13 days ago 3 min read

NSW law firm Brydens Lawyers at the centre of major cyberattack and data breach

The breach 'resulted in unauthorised access to some data on its servers'.

By Dominique Tassell



Home › News › Court Services Victoria – Cyber Incident Information

COURT SERVICES VICTORIA – CYBER INCIDENT INFORMATION

COURT SERVICES VICTORIA

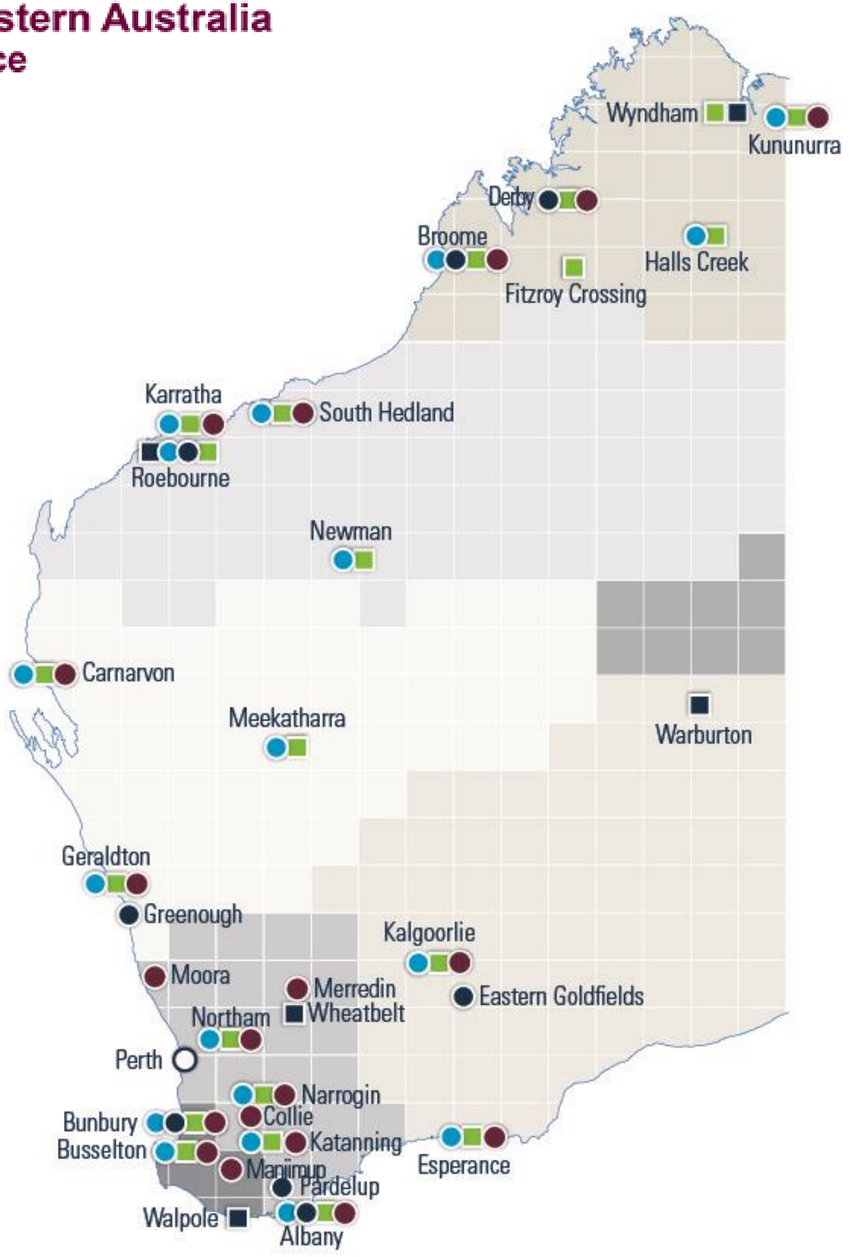
Thursday, 18 January 2024

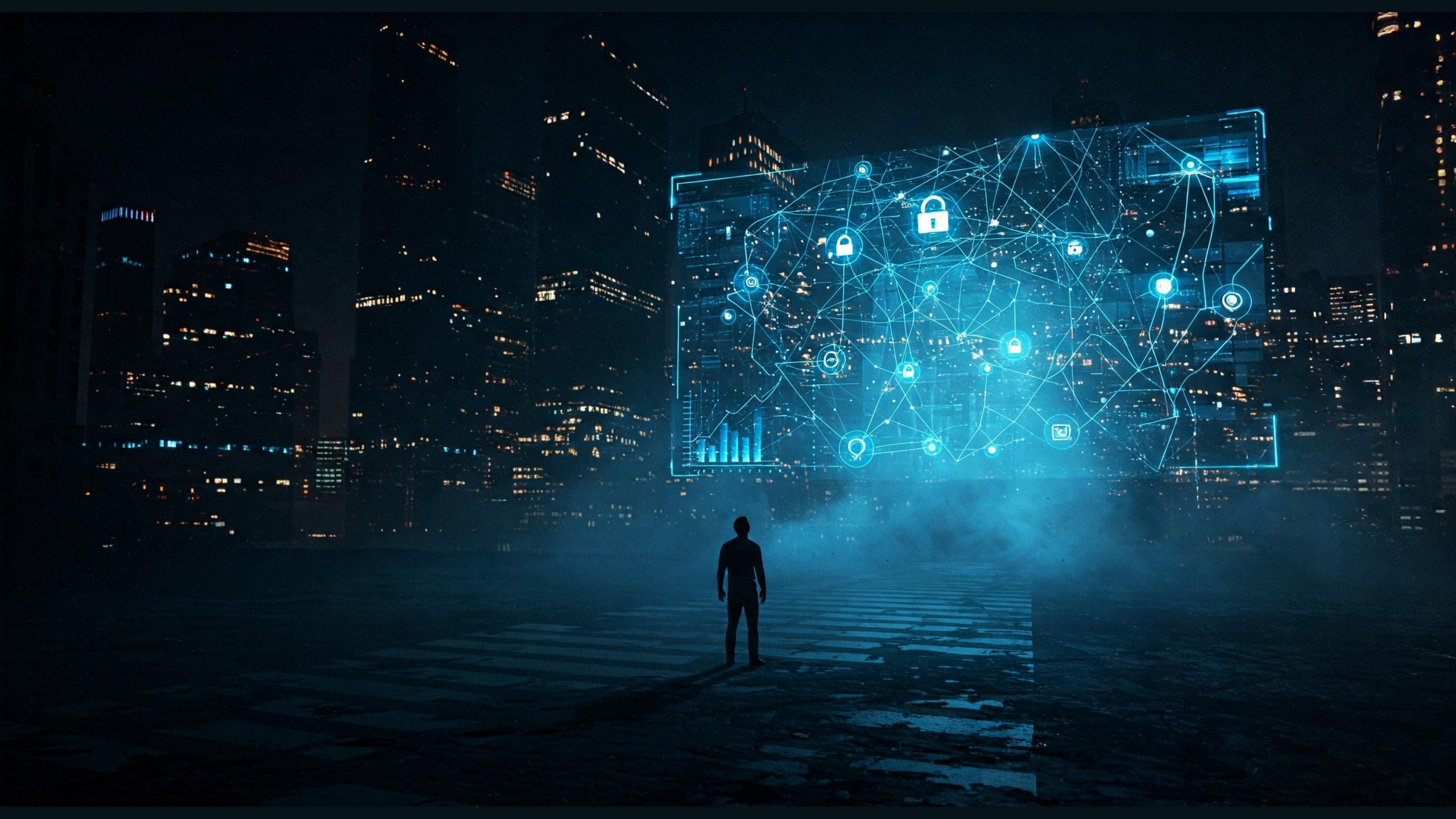
Government of **Western Australia**
Department of **Justice**

- Court and Tribunal Services
- Corrective Services
- Registry of Births, Deaths and Marriages
- Equal Opportunity Commission
- Office of the Public Advocate
- Public Trustee
- Parliamentary Counsel’s Office
- State Solicitor's Office
- Office of the Commissioner for Victims of Crime
- WA Office of Crime Statistics and Research

- Adult Community Corrections
- Prisons
- Work Camps
- Youth Detention Centres
- Youth Justice Services
- Head Office Buildings
- Courthouses

Government of **Western Australia**
Department of **Justice**





Strategies to mitigate cybersecurity incidents

Last Updated: February 2017. First published February 2010.

Suggested Mitigation Strategy Implementation Order
(start with threats of most concern to the organisation)

Targeted cyber intrusions (advanced persistent threats) and other external adversaries who steal data:

1. Implement 'essential' mitigation strategies to:
   a. prevent malware delivery and execution
   b. limit the extent of cybersecurity incidents
   c. detect cybersecurity incidents and respond.
2. Repeat step 1 with 'excellent' mitigation strategies.
3. Repeat step 1 with less effective mitigation strategies until an acceptable level of residual risk is reached.

Ransomware and external adversaries who destroy data and prevent computers/networks from functioning:

1. Implement 'essential' mitigation strategies to:
   a. recover data and system availability
   b. prevent malware delivery and execution
   c. limit the extent of cybersecurity incidents
   d. detect cybersecurity incidents and respond.
2. Repeat step 1 with 'excellent' mitigation strategies.
3. Repeat step 1 with less effective mitigation strategies until an acceptable level of residual risk is reached.

Note that 'Hunt to discover incidents' is less relevant for ransomware that immediately makes itself visible.

Malicious insiders who steal data:

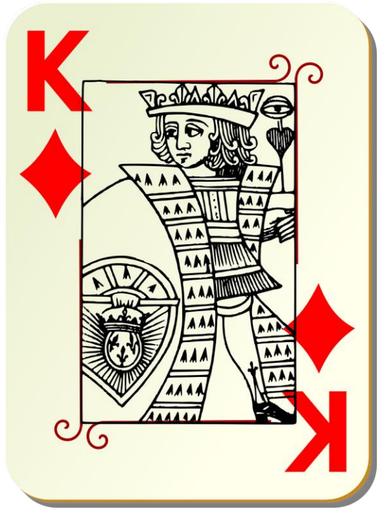
1. Implement 'Control removable storage media and connected devices' to mitigate data exfiltration.
2. Implement 'Outbound web and email data loss prevention'.
3. Implement 'essential' mitigation strategies to:
   a. limit the extent of cybersecurity incidents
   b. detect cybersecurity incidents and respond.
4. Repeat step 3 with 'excellent' mitigation strategies.
5. Implement 'Personnel management'.
6. If employees are likely to have hacking skills and tools, implement 'essential' mitigation strategies to prevent malware delivery and execution, and repeat step 3 with less effective mitigation strategies until an acceptable level of residual risk is reached.

Note that technical mitigation strategies provide incomplete security since data could be photographed or otherwise copied from computer screens or printouts, or memorised and written down outside of the workplace.

Malicious insiders who destroy data and prevent computers/networks from functioning:

1. Implement 'essential' mitigation strategies to:
   a. recover data and system availability
   b. limit the extent of cybersecurity incidents
   c. detect cybersecurity incidents and respond.
2. Repeat step 1 with 'excellent' mitigation strategies.
3. Implement 'Personnel management'.
4. If employees are likely to have hacking skills and tools, implement 'essential' mitigation strategies to prevent malware delivery and execution, and repeat step 1 with less effective mitigation strategies until an acceptable level of residual risk is reached.

Relative Security Effectiveness	Mitigation Strategy	Potential User Resistance	Upfront Cost (staff, software and hardware)	Ongoing Maintenance Cost
Mitigation strategies to prevent malware delivery and execution:				
Essential	**Application control** to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.	Medium	High	Medium
Essential	**Patch applications** (e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers). Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.	Low	High	High
Essential	**Configure Microsoft Office macro settings** to block macros from the internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.	Medium	Medium	Medium
Essential	**User application hardening**. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.	Medium	Medium	Medium
Excellent	**Automated dynamic analysis of email and web content run in a sandbox**, blocked if suspicious behaviour is identified (e.g. network traffic, new or modified files, or other system configuration changes).	Low	High	Medium
Excellent	**Email content filtering**. Allow only approved attachment types (including in archives and nested archives). Analyse/sanitise hyperlinks, PDF and Microsoft Office attachments. Quarantine Microsoft Office macros.	Medium	Medium	Medium
Excellent	**Web content filtering**. Allow only approved types of web content and websites with good reputation ratings. Block access to malicious domains and IP addresses, ads, anonymity networks and free domains.	Medium	Medium	Medium
Excellent	**Deny corporate computers direct internet connectivity**. Use a gateway firewall to require use of a split DNS server, an email server and an authenticated web proxy server for outbound web connections.	Medium	Medium	Low
Excellent	**Operating system generic exploit mitigation** e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET).	Low	Low	Low
Very Good	**Server application hardening** especially internet-accessible web applications (sanitise input and use TLS not SSL) and databases, as well as applications that access important (sensitive/high-availability) data.	Low	Medium	Medium
Very Good	**Operating system hardening** (including for network devices) based on a Standard Operating Environment, disabling unneeded functionality (e.g. RDP, AutoRun, LanMan, SMB/NetBIOS, LLMNR and WPAD).	Medium	Medium	Low
Very Good	**Antivirus software using heuristics and reputation ratings** to check a file's prevalence and digital signature prior to execution. Use antivirus software from different vendors for gateways versus computers.	Low	Low	Low
Very Good	**Control removable storage media and connected devices**. Block unapproved CD/DVD/USB storage media. Block connectivity with unapproved smartphones, tablets and Bluetooth/Wi-Fi/3G/4G/5G devices.	High	High	Medium
Very Good	**Block spoofed emails**. Use Sender Policy Framework (SPF) or Sender ID to check incoming emails. Use 'hard fail' SPF TXT and DMARC DNS records to mitigate emails that spoof the organisation's domain.	Low	Low	Low
Good	**User education**. Avoid phishing emails (e.g. with links to login to fake websites), weak passphrases, passphrase reuse, as well as unapproved: removable storage media, connected devices and cloud services.	Medium	High	Medium
Limited	**Antivirus software with up-to-date signatures** to identify malware, from a vendor that rapidly adds signatures for new malware. Use antivirus software from different vendors for gateways versus computers.	Low	Low	Low
Limited	**TLS encryption between email servers** to help prevent legitimate emails being intercepted and subsequently leveraged for social engineering. Perform content scanning after email traffic is decrypted.	Low	Low	Low
Mitigation strategies to limit the extent of cybersecurity incidents:				
Essential	**Restrict administrative privileges** to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.	Medium	High	Medium
Essential	**Patch operating systems**. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.	Low	Medium	Medium
Essential	**Multi-factor authentication** including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.	Medium	High	Medium
Excellent	**Disable local administrator accounts** or assign passphrases that are random and unique for each computer's local administrator account to prevent propagation using shared local administrator credentials.	Low	Medium	Low
Excellent	**Network segmentation**. Deny traffic between computers unless required. Constrain devices with low assurance (e.g. BYOD and IoT). Restrict access to network drives and data repositories based on user duties.	Low	High	Medium
Excellent	**Protect authentication credentials**. Remove CPassword values (MS14-025). Configure WDigest (KB2871997). Use Windows Defender Credential Guard. Change default passphrases. Require long complex passphrases.	Medium	Medium	Low
Very Good	**Non-persistent virtualised sandboxed environment**, denying access to important (sensitive/high-availability) data, for risky activities (e.g. web browsing, and viewing untrusted Microsoft Office and PDF files).	Medium	Medium	Medium
Very Good	**Software-based application firewall, blocking incoming network traffic** that is malicious/unauthorised, and denying network traffic by default (e.g. unneeded/unauthorised RDP and SMB/NetBIOS traffic).	Low	Medium	Medium
Very Good	**Software-based application firewall, blocking outgoing network traffic** that is not generated by approved/trusted programs, and denying network traffic by default.	Medium	Medium	Medium
Very Good	**Outbound web and email data loss prevention**. Block unapproved cloud computing services. Log recipient, size and frequency of outbound emails. Block and log emails with sensitive words or data patterns.	Medium	Medium	Medium
Mitigation strategies to detect cybersecurity incidents and respond:				
Excellent	**Continuous incident detection and response** with automated immediate analysis of centralised time-synchronised logs of allowed and denied computer events, authentication, file access and network activity.	Low	Very High	Very High
Very Good	**Host-based intrusion detection/prevention system** to identify anomalous behaviour during program execution (e.g. process injection, keystroke logging, driver loading and persistence).	Low	Medium	Medium
Very Good	**Endpoint detection and response software** on all computers to centrally log system behaviour and facilitate cybersecurity incident response activities. Microsoft's free SysMon tool is an entry level option.	Low	Medium	Medium
Very Good	**Hunt to discover incidents** based on knowledge of adversary tradecraft. Leverage threat intelligence consisting of analysed threat data with context enabling mitigating action, not just indicators of compromise.	Low	Very High	Very High
Limited	**Network-based intrusion detection/prevention system** using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.	Low	High	Medium
Limited	**Capture network traffic** to and from corporate computers storing important data or considered as critical assets, and network traffic traversing the network perimeter, to perform incident detection and analysis.	Low	High	Medium
Mitigation strategies to recover data and system availability:				
Essential	**Regular backups** of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.	Low	High	High
Very Good	**Business continuity and disaster recovery plans** which are tested, documented and printed in hardcopy with a softcopy stored offline. Focus on the highest priority systems and data to recover.	Low	High	Medium
Very Good	**System recovery capabilities** e.g. virtualisation with snapshot backups, remotely installing operating systems and applications on computers, approved enterprise mobility, and onsite vendor support contracts.	Low	High	Medium
Mitigation strategy specific to preventing malicious insiders:				
Very Good	**Personnel management** e.g. ongoing vetting especially for users with privileged access, immediately disable all accounts of departing users, and remind users of their security obligations and penalties.	High	High	High

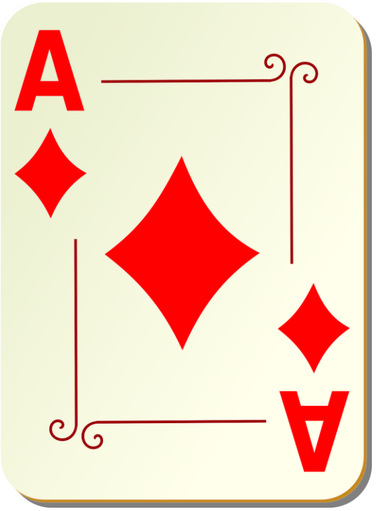


- **List your software assets**
- **Scan for vulnerabilities**
- **Automate patching from a centralised repository**

Patch Applications

- **List your Operating Systems**
- **Scan for vulnerabilities**
- **Automate patching from a centralised repository**

Patch Operating Systems

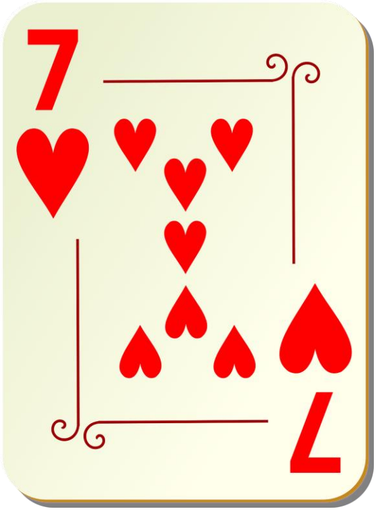


- **We’ve all done this.**
- **Right?**
- **What about situations where you can’t take a phone?**

Multi Factor Authentication

- **Role-Based Access Control**
- **Start with Tier 0**
- **Use PAM and PAWs and MFA!**

Restrict Administrative Privileges

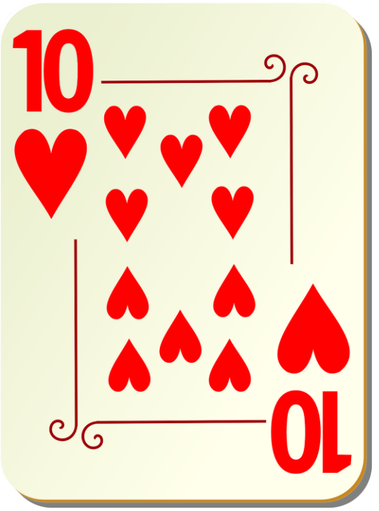


- **Start with a Standard Operating Environment**
- **List your approved Apps**
- **Manage changes and updates**

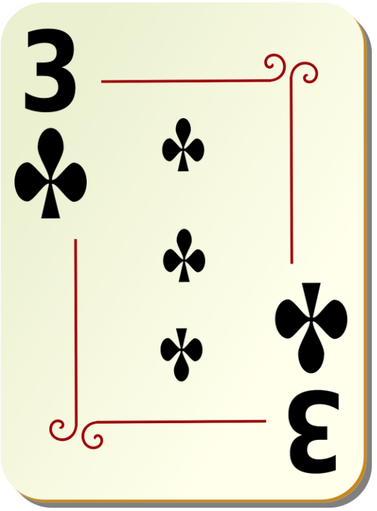
Application Control

- **Identify all Macros in use**
- **Give up trying to find them all**
- **Sign your trusted Macros and block all others.**

Restrict Microsoft Office Macros



- **Start with a SOE**
- **Lock it down**
- **Have robust and rapid support in place, especially at the start**



- **3-2-1**
- **Test and validate. Business Continuity and Incident Exercises.**
- **Can you restore as quickly as the “business” expects?**

Regular Backups


A
K
K
A
JK


Greed
Enchantment
, Pay 2 life: Draw a card.
What is a sliver of one's soul compared to unimaginable wealth?
Terminal Agony
Sorcery
Destroy target creature.
Madness (If you discard this card, discard it into exile. When you do, cast it for its madness cost or put it into your graveyard.)
His mouth melted to slag, yet somehow he kept screaming.
Garth One-Eye
Legendary Creature — Human Wizard
: Choose a card name that hasn't been chosen from among Disenchant, Braingeyser, Terror, Shivan Dragon,
Mishra's Factory
Land
Creature — Elf Druid
Sterling Grove
Enchantment
Strike It Rich
Sorcery
Lightning Spear
Artifact — Equipment
Equipped creature gets +1/+0 and has trample.
, Sacrifice Lightning Spear: It deals 3 damage to any target.
Equip 1
When wielded, it begs to be released.
Scalding Tarn
Land
Combine Chrysalis
Artifact
Vectis Gloves
Artifact — Equipment
Flame Blitz
Enchantment
At the beginning of your end step, Flame Blitz deals 5 damage to each planeswalker.
Cycling 2 (2, Discard this card: Draw a card.)
"Blast it, not again!"
Suspend 3—1 (Rather than cast this card from your hand, pay 1 and exile it with three time counters on it. At the beginning of your upkeep, remove a time counter. When the last is removed, cast it without paying its mana cost.)
Search target opponent's library for a creature card and put that card onto the battlefield under your control. Then that player shuffles.
Sojourner's Companion
Creature — Zombie
When Nested Shambler dies, create X tapped 1/1 green Squirrel creature tokens, where X is Nested Shambler's power.
Home is where the heart was.
1/1
Creature — Beast
Whenever one or more +1/+1 counters are put on Herd Baloth, you may create a 4/4 green Beast creature token.
Baloth social structure is simple:
Artifact Creature — Gargoyle
Flying
: Marble Gargoyle gets +0/+1 until end of turn.
Creature — Vampire Soldier
Enchantment
Sacrifice Seal of Removal: Return target creature to its owner's hand.
Artifact Land
Creature — Goblin Shaman
Exalted (Whenever a creature you control attacks alone, that creature gets +1/+1 until end of turn.)
: Add , , or .
He protects the fetid bog from light, life, and the hideous sound of laughter.
Haste
Echo—Discard a card. (At the beginning of your upkeep, if this came under your control since the beginning of your last upkeep, sacrifice it unless you pay its echo cost.)
Caution: Audience in front
Glimmer Bairn
Creature — Human Druid

- **Minimise Attack Surface**
- **Patch Apps and OS**
- **Implement Strong Authentication and Access Controls**

Server Application Hardening

- **DMARC**
- **Monitor it**

Block Spoofed Emails

- **Good Idea**
- **Can be hard to achieve**

Network Segmentation

- **Have a SIEM and IPS, IDS, EDR, XDR, ETC**
- **Monitor it**

Continuous Incident Detection and Response

- **Use Human Resources Data**
- **Establish a solid off-boarding procedure**

Blueprint for Secure Cloud

- Better practice guidance
- Configuration guides and templates

Foundations for modern defensible architecture

- Zero trust principles
- Secure-by-design practices

Thank You