

# *Cyber Security Essentials for Healthcare Providers*

**Miroslav Doncevic** M CyberSec, Grad Cert Cyber Sec, Cert NIST CSF Practitioner

**Tony Nicholson**, B App Sc (Computing), Director, Mint IT Solutions

[www.mintit.com.au](http://www.mintit.com.au)

# Agenda:

**Introduction:** The cyber security threat for healthcare providers data and business continuity

**Topic 1 :** Think before you click! *Social Engineering Attacks*

- Phishing - types of phishing attacks, consequences of phishing
- Business Email Compromise
- Safe email practices
- Think before you click send and think before you click post
- Follow the “need-to-know” principle

**Topic 2:** Access Controls - *Secure Identity Access Management*

- Unique, long and complex passwords
- Pass phrases
- Multi-factor Authentication (MFA/2FA)

**Topic 3:** Business Continuity - *The importance of having robust backup processes*

- 3-2-1-1 Data Backup method
- Immutable Backups
- Test Restore

**Topic 4:** Compliance - *Respond, Report, Protect Privacy*

- Understanding your obligations
- Responding to an incident
- Where to get help

Note - These topics have been derived from the Australian Digital Health Agency (ADHA)’s online learning module: <https://training.digitalhealth.gov.au>

- **Cyber security attacks resulting in data breaches and extortions are very, very, lucrative, so hackers continually evolve new tactics and are not going away.**
- **Massive ransomware and extortion attacks are regularly reported in news media, however many more successful cyber attacks target small organizations, including health service providers, which are not widely reported.**
- **The health service provider sector is again the number one target for malicious or criminal attackers according to the latest Notifiable Data Breaches Report by the Office of the Australian Information Commissioner (OAIC), with ransomware at the top of the list of cyber incidents.**
- **Practice managers must ensure that these absolutely essential cyber security standards based defences and mitigations are in place to have any chance to defend their clinic from cyber attacks and prevent becoming a data breach victim caught up in a cyber security catastrophe.**

Note - These topics have been derived from the Australian Digital Health Agency (ADHA)'s online learning module: <https://training.digitalhealth.gov.au>

## The Five Most Important Things to Know about Your Data:



### Know the value of your data

You need to know what value it has, not just for your organisation, and customers, but also the value to those who may wish to steal it.

All data has value to someone.



### Know who has access to your data

You need to know who has access both within an organisation and externally, like who has 'super user' admin rights in your organisation and within your trusted partners and vendors.



### Know where your data is

You need to know where your data is stored. Is it with a service provider? Have they provided your data to other third parties? Is it onshore, off-shore or in a cloud?



### Know who is protecting your data

You need to know who is protecting your valuable data. What operational security processes are in place? Where are they? Can you contact them if you need to?



### Know how well your data is protected

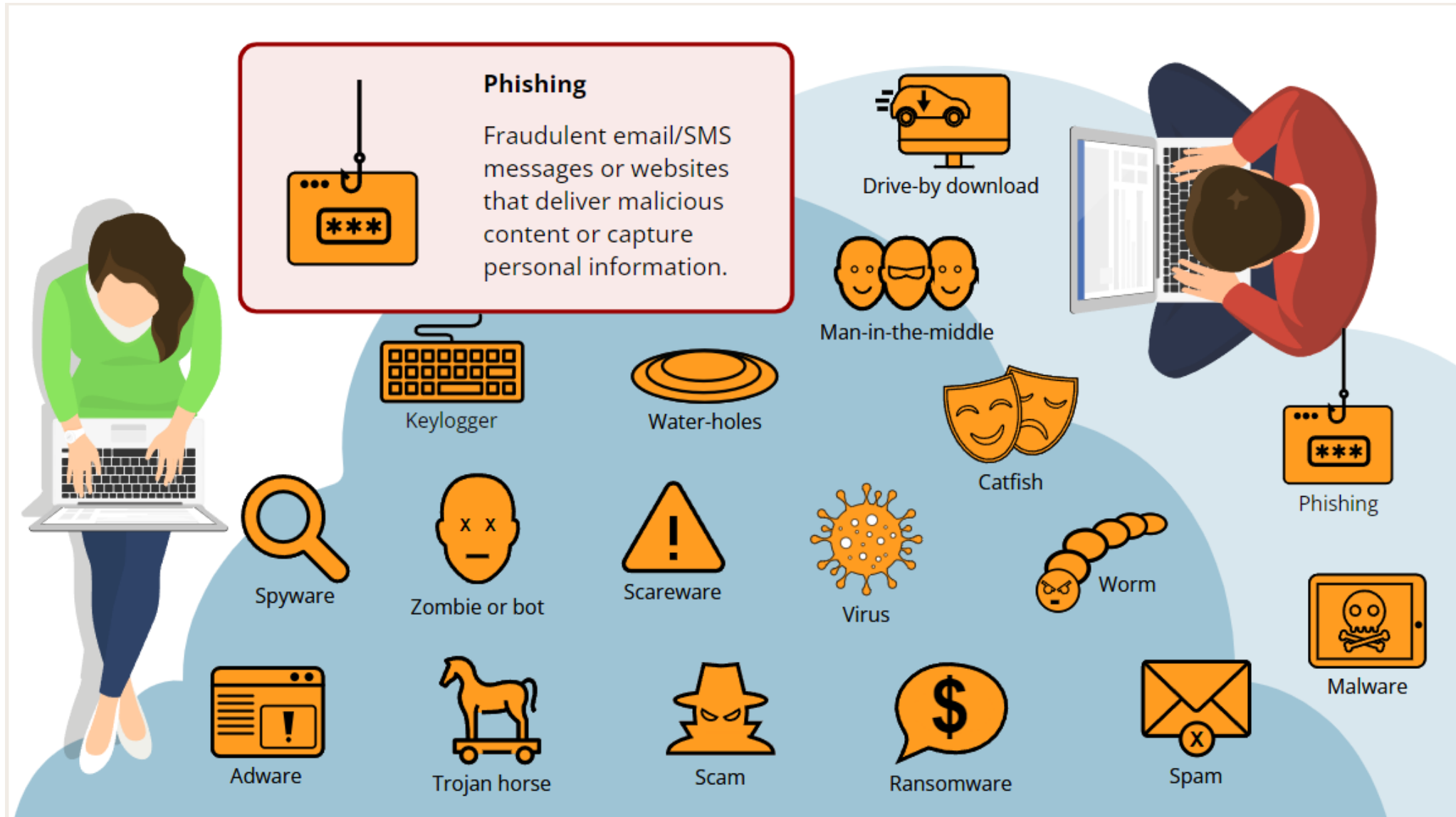
You need to know what your security professionals are doing to protect your data 24/7. Is your data being adequately protected by your employees, business partners and third party vendors who have access to it?

Source: <https://www.telstra.com.au/content/dam/tcom/business-enterprise/security-services/pdf/5-knows-of-cyber-security.pdf>

# Introduction: Cyber threats in 2024



# Introduction: Cyber attacks



Source: <https://training.digitalhealth.gov.au>

# Cyber Risks in 2023: all about the money!



- \$8 trillion USD a year
- \$667 billion USD a month
- \$154 billion USD a week
- \$21.9 billion USD a day
- \$913 million USD an hour
- \$15.2 million USD a minute
- \$255,000 USD a second



<https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/>

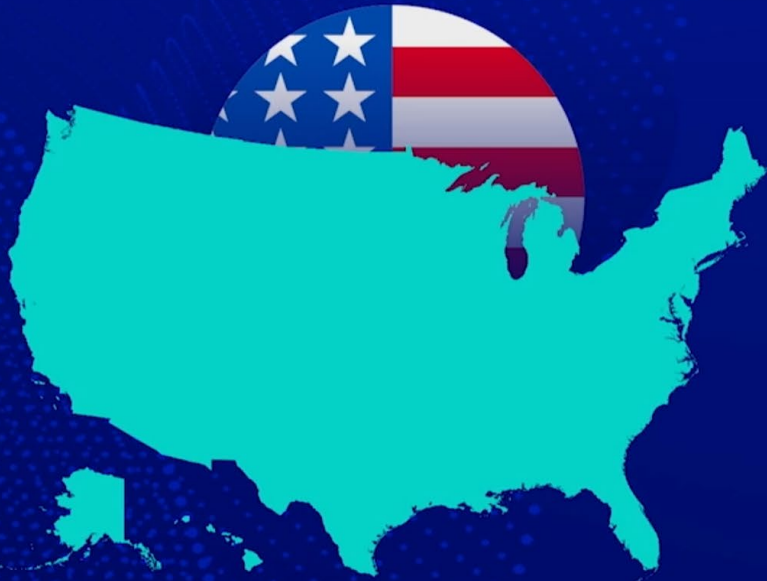
<https://www.esentire.com/resources/library/2022-official-cybercrime-report>



# Cyber Risks in 2024: all about the money!

## Cybercrime is **BIG Business**

UNITED STATES



CHINA



CYBERCRIME



Source: <https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/>



# Cyber Threats in 2024: all about the money!

GDP Comparisons (www.statista.com)	
USA 2024	USD\$28.176 trillion
China 2024	USD\$18.560 trillion
Cyber crime 2024	USD\$10.5 trillion
Australia 2024	USD\$1.685 trillion

If it were measured as a country, then cybercrime would be the world's third-largest economy after the U.S. and China.

Steve Morgan,  
founder of Cybersecurity Ventures



Source: <https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/>

<https://www.esentire.com/resources/library/2022-official-cybercrime-report>

# Top Cyber Risks 2024 :

- *Social Engineering:*
  - *Phishing, Spearphishing, Whaling, Business Email Compromise, SMSishing, Vishing, Impersonation*
- *Ransomware*
- *Triple Extortion – Multi Faceted Extortion*
- *Supply Chain attacks*
- *Data Leakage/Insider Threat*
- *Credential Theft*
- *Network Perimeter and Endpoint security:*
  - Working From Home?*
- *Denial of Service (DoS) and*
- *Distributed Denial of Service (DDoS)*
- *Insider Threat*

# Cyber Risks 2024 – all powered by Gen AI:

- Social Engineering:
  - Phishing, Spearphishing, Whaling, Business Email Compromise, SMSishing, Vishing, Impersonation
- Ransomware
- Triple Extortion – Multi Faceted Extortion
- Supply Chain attacks
- Data Leakage/Insider Threat
- Credential Theft
- Network Perimeter and Endpoint security:
  - Working From Home?
- Denial of Service (DoS) and
- Distributed Denial of Service (DDoS)
- Insider Threat



# Top Cyber Risks 2024 : Generative AI

The release of ChatGPT 3.5 in late 2022 with natural language processing using Deep Learning through transformer neural networks, and trained on Large Language Models (LLMs) has spearheaded the rapid release of chatbots such as Microsoft Bing/Copilot, Google Bard/Gemini, and a plethora of others, with more to come...

The AI referred to here is more specifically Artificial General Intelligence, or more commonly called Generative AI (GAI), and it's component parts;

- Machine Learning (ML)
- Large Language Models (LLMs)
- Human Language AI
- Deep Learning, powered by Neural Networks



There are very real accuracy, ethical, legal, indemnity, privacy, confidentiality, intellectual property, *and* cyber security concerns with using Gen AI tools in a healthcare setting.

Cyber threat actors are also using Gen AI to find vulnerabilities, for social engineering attacks, and to hack into networks for data theft and extortion...

**PROCEED WITH CAUTION!**

# Top Cyber Risks 2024 : Generative AI

Beyond the hype cycle and the predicted productivity gains, there are many expert voices raising concerns and urging government regulation to prevent GAI causing harm to humans.

AI limitations are well documented with negative aspects of GAI, for example, AI fabrications, the so called 'AI hallucinations', AI biases, privacy concerns, misinformation, and disinformation, deep fakes, AI driven cyber attacks, etc.



**“AI has emerged as a powerful force in cybersecurity, shaping the strategies of both attackers and defenders.**

**Cybercriminals can now use AI-powered tools to craft convincing phishing emails, orchestrate deepfake attacks, and develop malware with adaptive capabilities, rendering many traditional defence mechanisms obsolete.**

Source: <https://www.infosecurity-magazine.com/blogs/ai-5g-new-era-of-cybersecurity/>

# Top Cyber Risks 2024 : Generative AI

“But with advances in attacks come new forms of defense.

AI can play a pivotal role in identifying anomalies and potential threats.

For example, AI's proficiency in automating incident response processes can transform cybersecurity with rapid detection, analysis, and response to security incidents become achievable at a pace that manual processes cannot match, minimizing the impact of cyberthreats..”



...”The automation prowess of AI accelerates cyberthreats, empowering attackers to identify and exploit weaknesses at unprecedented speed, posing challenges to defenders striving to keep pace.

AI-driven evasion techniques add another layer of complexity to cyberthreats. Polymorphic malware, capable of altering its code structure to evade detection, exemplifies how AI enables attackers to continuously outsmart conventional security measures.”

Source: <https://www.infosecurity-magazine.com/blogs/ai-5g-new-era-of-cybersecurity/>



# Australian Government Guidance on use of GEN AI for APS:



Home > Interim guidance on government use of public generative AI tools - November 2023

## Interim guidance on government use of public generative AI tools - November 2023

Updated on 22 November 2023

### Notice

*This guidance will be iterative. It is provided for government agencies to implement within their organisation. APS staff should follow their agency's policies and guidance on using generative AI tools in the first instance.*

*Feedback from public consultation on the responsible use of AI in Australia will be used to inform consideration across government on appropriate regulatory and policy responses that may include future iterations of this guidance.*

### Guidance for Australian Public Service (APS) staff

Generative AI tools present new and innovative opportunities for government. However, due to their rapid evolution and uptake, the risks involved in their use need to be considered and assessed.

The breadth of government activities includes developing policy advice for ministers, delivering programs to industry, providing services to the community and providing regulatory oversight. As such, the risk of using generative AI tools for official activities is context-specific and requirements will differ depending on how they are deployed.

Users should first and foremost align with their departmental or agency ICT obligations and policies. The DTA encourages departments and agencies to review their policies related to AI in line with this advice.

This guidance will be supplemented in due course with a risk framework to assist with the risk assessment process.

### Golden rules

As you consider using generative AI tools in your work, you should assess the potential benefits and risks for each use case and take appropriate steps to mitigate them.

The principles, tactical guidance and use cases that follow will guide responsible application of these tools. Above all, apply these two **golden rules**.

- You should be able to explain, justify and take ownership of your advice and decisions.
- Assume any information you input into public generative AI tools<sup>1</sup> could become public. Don't input anything that could reveal classified, personal or otherwise sensitive information.

### Principles in practice

This section provides guidance to help APS staff adhere to [Australia's AI Ethics Principles](#) when using generative AI tools, and is organised into sub-sections as follows:

- 1.Accountability
- 2.Transparency and explainability
- 3.Privacy protection and security
- 4.Fairness and human-centred values
- 5.Human, societal and environmental wellbeing

APS staff are encouraged to read and understand [Australia's AI Ethics Principles](#).

# Top Cyber Risks 2024 : Generative AI

## THE WEEKEND AUSTRALIAN

Sunday, March 3, 2024 | Today's Paper | Mind Games

All sections

HOME THE NATION WORLD BUSINESS COMMENTARY SPORT ARTS ALL

HOME / NATION / POLITICS



### ChatGPT for criminals to turbo charge scams, say Australian Federal Police



Australians are at risk from malicious AI that could lead to a new generation of scams, federal police warn. Picture: AAP

EXCLUSIVE  
By DAVID MURRAY  
NATIONAL CRIME  
CORRESPONDENT

7:11PM JANUARY 30, 2024  
3 COMMENTS

An Australian Federal Police submission to a federal cybercrime inquiry flags AI models such as **FraudGPT** and **WormGPT** as a growing threat.

The models are similar to ChatGPT, but are devoid of restrictions on answering questions about illegal activity.

They provide a suite of tools that can craft spear-phishing emails “with perfect grammar and spelling”, aimed at stealing sensitive information such as login details, the AFP says.

The tools can also assist in voice phishing for “hi Mum, hi Dad scams”, business email compromise attacks, generating malware and testing for security vulnerabilities.

“The development of malicious AI models by threat actors is in its early stages, but already proving effective and lowers the entry threshold for burgeoning cyber criminals who may lack the technical proficiencies or resources to establish their own cyber criminal tradecraft,” the submission states.

The Australian Institute of Criminology also warns: “AI is already being leveraged by criminal actors to upscale and enhance criminal activities, exploit human-centric vulnerabilities and lower the barriers and costs to engaging in criminal activities.”

With Australians reeling from major hacks on corporations including Medibank and Optus, the federal parliamentary joint committee on law enforcement is conducting an inquiry into the capability of agencies to respond to cybercrime.

When **WormGPT’s** existence was revealed in July, it was described by cyber security firm SlashNext as being “similar to ChatGPT but with no ethical boundaries or limitations”.

**FraudGPT** has reportedly been advertised on the dark web as an “unrestricted alternative for ChatGPT”.

The AFP says current trends such as Ransomware-as-a-Service (RaaS) and Malware-as-a-Service (Maas) have allowed more people to launch cyber attacks and scams. “The frequency and severity of cybercrime incidents are expected to increase as a result, placing new demands on the AFP as a law enforcement agency,” the submission states.

Malicious artificial intelligence could lead to a cybercrime explosion, ushering in a new generation of ultra-sophisticated scams, federal police warn.

Source: <https://www.theaustralian.com.au/nation/politics/chatgpt-for-criminals-to-turbo-charge-scams-say-australian-federal-police/news-story/6dfcbdc500381f3569762a68adf12dfe>

# Top Cyber Risks 2024 : Generative AI

## THE WEEKEND AUSTRALIAN

Sunday, March 3, 2024 | Today's Paper | Mind Games

≡ All sections

HOME THE NATION WORLD BUSINESS COMMENTARY SPORT ARTS All

HOME / NATION / POLITICS



### ChatGPT for criminals to turbo charge scams, say Australian Federal Police

**EXCLUSIVE**  
By DAVID MURRAY  
NATIONAL CRIME  
CORRESPONDENT

7:11PM JANUARY 30, 2024  
3 COMMENTS



Australians are at risk from malicious AI that could lead to a new generation of scams, federal police warn. Picture: AAP

Other recent hacks were carried out on Victoria’s court system and the St Vincent’s Health network.

Malicious AI was also used to create increasingly realistic deepfakes, lifelike child abuse material and believable disinformation content, the AFP says.

“AI is an emerging technology in child exploitation matters and as it improves, the material is - becoming more lifelike. This type of material is known as deepfakes, which involve manipulating images, audio and video using AI.”

The AIC’s submission to the inquiry states almost one in every two Australians surveyed had been a victim of at least one type of cybercrime in the previous 12 months.

“Cybercrime targeting individual computer users is most frequently a high volume, low yield crime,” the AIC states.

“The high rate of victimisation means that, even with the relatively small median losses per victim, the overall cost to Australian individuals is likely to be enormous.”

The impact of losses was “potentially catastrophic and can have long-term effects on victims”.

Cyber criminals were quick to adopt emerging technologies for criminal purposes, the AIC states.

“Artificial intelligence has the potential to facilitate better-targeted, more frequent and widespread criminal attacks, and is already being used for password guessing, CAPTCHA-breaking and voice cloning,” the submission states.

Source: <https://www.theaustralian.com.au/nation/politics/chatgpt-for-criminals-to-turbo-charge-scams-say-australian-federal-police/news-story/6dfcbdc500381f3569762a68adf12dfe>



# Social Engineering:



Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Source: <https://www.imperva.com/learn/application-security/social-engineering-attack/>

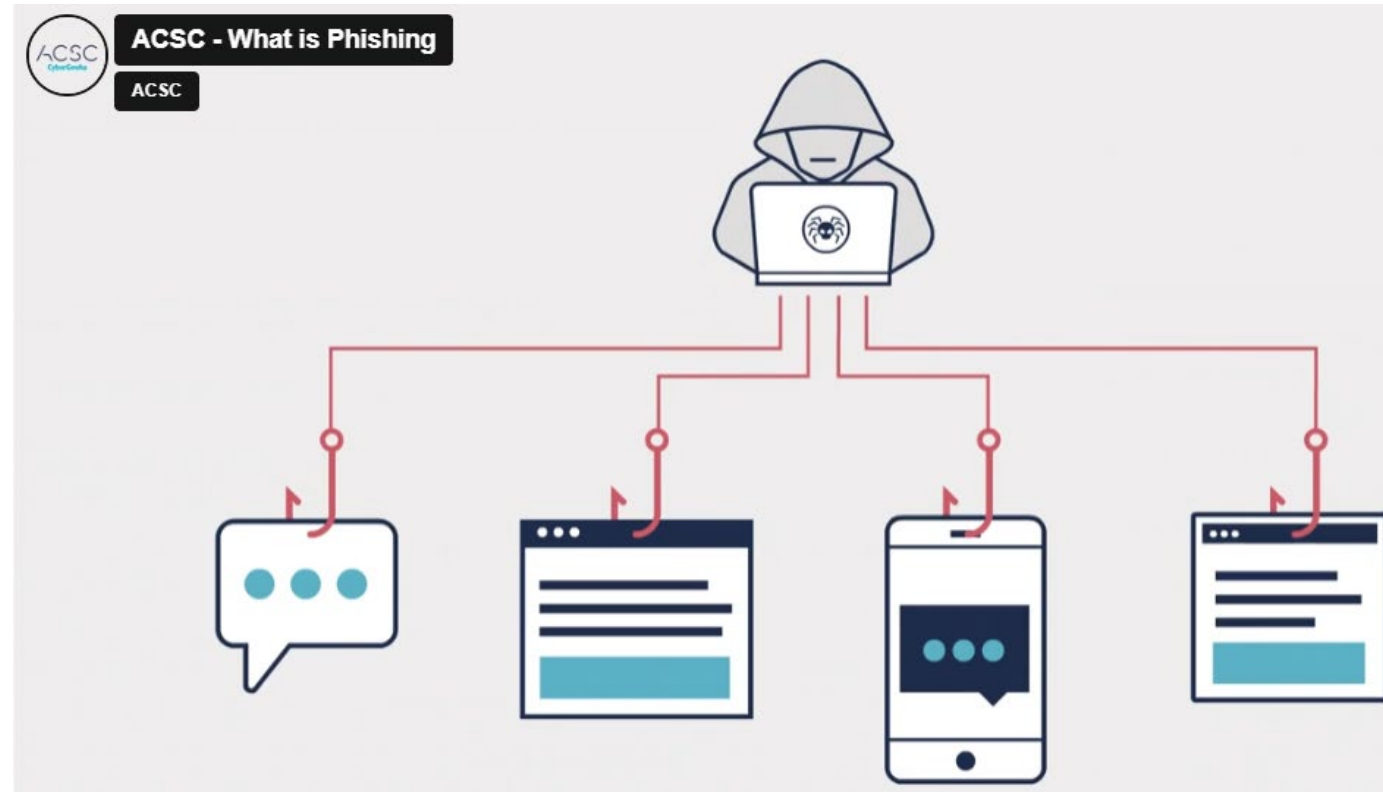
# Social Engineering:

The DATA your clinic collects, uses, and holds is very valuable to the clinic, patients, other connected healthcare providers, government agencies, AND TO CYBER CRIMINALS.

Social Engineering attacks are all about using DECEPTION to MANIPULATE or FOOL computer users, i.e., humans, into performing an action which will give sensitive information such as login credentials, or give access to data by the attacker, most often for ransomware, data theft, extortion, and other nefarious reasons.

Social Engineering attacks vary, but fall into four broad categories:

- Phishing
- SMiShing
- Vishing
- Impersonation



## Humans are The Weak Link:

What makes social engineering especially dangerous is that it relies on human error, rather than vulnerabilities in software and operating systems.

Mistakes made by legitimate users are much less predictable, making them harder to identify and thwart than a malware-based intrusion.

Source: <https://www.imperva.com/learn/application-security/social-engineering-attack/>





# The Social Engineering Attack Cycle:

Social engineering attacks happen in one or more steps:

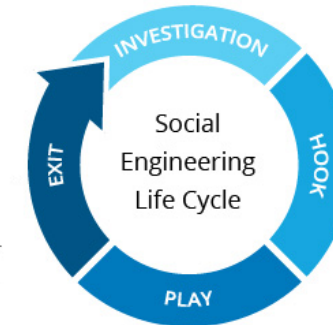
A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack.

Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

Source: <https://www.imperva.com/learn/application-security/social-engineering-attack/>

## Preparing the ground for the attack:

- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).



## Closing the interaction, ideally without arousing suspicion:

- Removing all traces of malware.
- Covering tracks.
- Bringing the charade to a natural end.

## Deceiving the victim(s) to gain a foothold:

- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

## Obtaining the information over a period of time:

- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

# Social Engineering Attacks:



**Phishing**  
(email/website)

From myGov <refund@my.gov.au> ☆  
Subject You have an outstanding refund from MyGov !  
To [redacted] ☆



Dear Customer

You have an outstanding refund from MyGov. Our transaction management system detects that you are entitled to receive this payment.

**Your refund is available online : 640.98 AUD**

Registration number	100088684468
Payment method	Direct debit at maturity
Datum	09/01/2023

To accept the fast online payment click on the following link and save the refund information : <https://login.my.gov.au/las/mygov-login>

Kind Regards,  
The MyGov-Team



## Phishing

Phishing, a play on ‘fishing’, being the metaphor of using a baited hook or lure that tricks the fish into biting, and getting hooked, in this case, cyber attackers deceiving the unwitting human with fraudulent email messages into giving confidential information, such as IT systems login credentials, passwords/passphrases, credit card details, enticing the human to open an attachment, (which contains malicious content), or a link to visit a fake website that will ask the user to provide login information, i.e., online banking logins, or that downloads malicious content into the user’s computer/device upon being opened.

Usually the fake emails pretend to be from various large organisations we trust or have relationships with, to make the phish more believable, i.e., Telstra, AGL, Australia Post, Australian Federal Police, ATO, myGov, etc., all of which are getting much more realistic and consequently, becoming harder to detect as fakes.

**Phishing is the highest method for malicious actors gaining access to accounts after compromised or stolen credentials and ransomware, according to the most recent OAIC Notifiable Data Breaches Report July-December 2023, OAIC, (2024).**

Image Source: <https://www.mailguard.com.au/blog/new-scam-email-promises-mygov-refund-of-640-98>

# Social Engineering Attacks:



## Phishing Variants:

Phishing attacks against businesses, government and other organisations are also known as **Business Email Compromise (BEC)**, usually for money transfer frauds.

**Spearphishing** attacks are phishing attacks that specifically target an individual, or a specific organisation, or a group in an organisation.

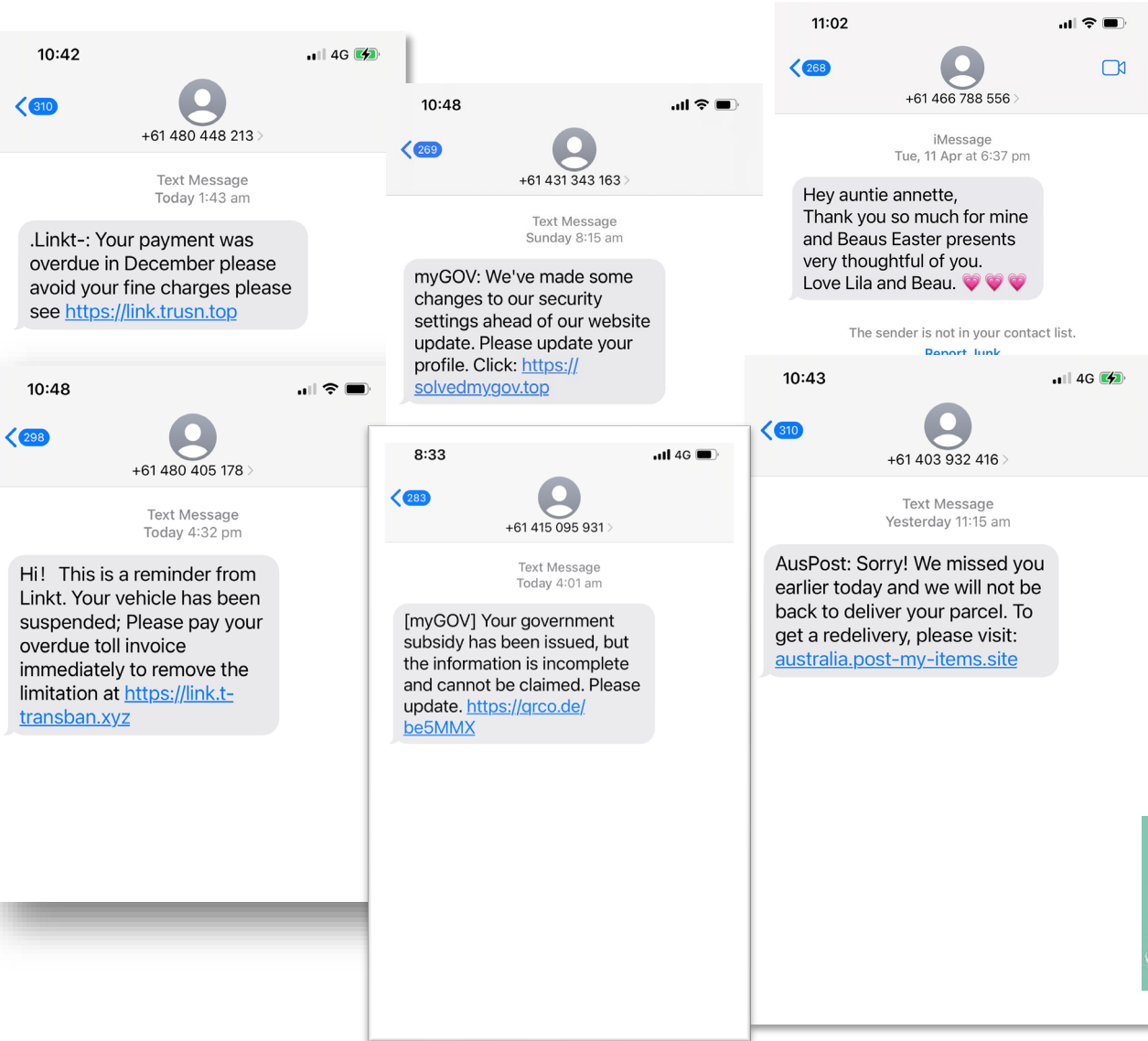
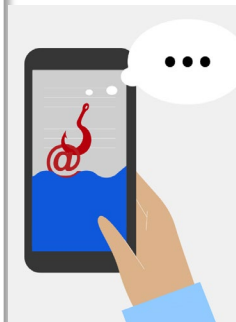
**Whaling**, is again, a specifically targeted attack on a senior official or manager (or 'big fish')

## SMiShing

Smishing, (**SMS-ishing**), where the attacker uses SMS text messages to entice the recipient into clicking a link, thus sending the attacker confidential information from the smart phone or downloading malicious programs to the smartphone.

## Vishing

Another variant, **Voice** phishing is the use of telephony to deceive or manipulate the victim as in the other forms of Social Engineering.



# Other Social Engineering Attacks:

## **Impersonation**

People are still tricked by an attacker that impersonates someone else, usually an authority figure such as a manager, that the victim has heard of but doesn't know, a law enforcement officer, an IT technician, etc. Impersonators of course are also called a 'con artist'.

## **Pretexting**

This is crucial to the deception or manipulation, and is quite simply the “fake story the bad actor weaves during the phish”, with making the story a “believable scenario”.

## **Baiting**

This is where the Social Engineer “dangles something tempting in front of you, hoping that you'll take action”, or the “bait”.

## **Tailgating**

Gaining access to restricted areas (such as an IT operations room) by “tailgating behind an employee”, with of course a clever pretext.

## **Quid Pro Quo**

The Social Engineer “offers a benefit to the target in exchange for information or access”

*Above quotes from mitnicksecurity.com, (2022)*

## **Pig Butchering**

...”Pig butchering scams originated in China, where they came to be known by the Chinese version of the phrase shāzhūpán because of an approach in which attackers essentially fatten victims up and then take everything they've got. These scams are typically cryptocurrency schemes, though they can involve other types of financial trading as well. Scammers cold-contact people on SMS texting or other social media, dating, and communication platforms...”

Source: LILY HAY NEWMAN SECURITY JAN 2, 2023 Hacker Lexicon: What Is a Pig Butchering Scam?

<https://www.wired.com/story/what-is-pig-butchering-scam>

# Other Social Engineering Attacks: Social Media Platforms

**usecure** blog

## How Hacker's Use Social Media For Social Engineering Attacks

Emma Woods

“...Social media has now become a gold mine of easily-accessible information for online crime, packed with sensitive and (what should be) personal data - providing the perfect ingredients for social engineering attacks” ...

...Known as Open Source Intelligence [OSINT]

**Here are the top things your employees need to avoid sharing on social media:**

- **Location**
- **Job role**
- **work email address**
- **Credentials(login details)**
- **Screenshot of conversations**
- **phone numbers and addresses**
- **Your financial status**



Source: <https://blog.usecure.io/social-media-the-key-ingredients-for-social-engineering-attacks>

# Other Social Engineering Attacks: Social Media Platforms

sennovate blog

## Understand How Social Media Is Fuelling Social Engineering Attacks

6 March, 2023

**“...Social media has now become an easy way to access the sensitive information for online crime, including the personal data and professional data. It provides all the things to attackers for social engineering attacks.” ...**

...Having a tendency to overshare is the main problem of social media, this however, only opens up many opportunities for a social engineer to plan an attack. The more information they have shared, the better the attack can be planned by a social engineer. In this way, social media gives enough “fuel” to start a fire, then there is a higher chance of the social engineering attacks success.” ...



Source: <https://sennovate.com/understand-how-social-media-is-fuelling-social-engineering-attacks/>



# Social Engineering

Remember the Human Factor –

i.e. : humans click on fake emails and links, use weak passwords, etc. ...

**Social engineering is involved in over 90% of all cyber attacks.**

Source: [https://purplesec.us/learn/why-social-engineering-works/?utm\\_source=newsletter&utm\\_medium=email&utm\\_campaign=why\\_is\\_social\\_engineering\\_effective&utm\\_term=2023-03-15](https://purplesec.us/learn/why-social-engineering-works/?utm_source=newsletter&utm_medium=email&utm_campaign=why_is_social_engineering_effective&utm_term=2023-03-15)

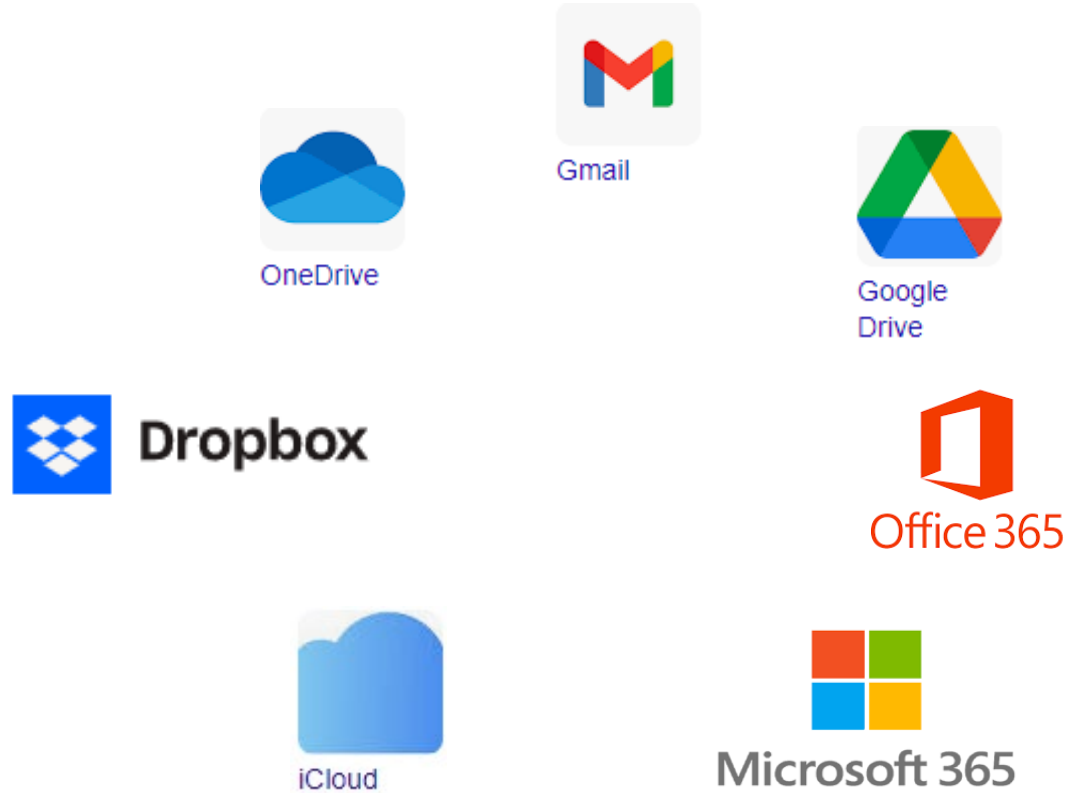


*“Notably, phishing and spear phishing continue to be the most common and highly effective methods by which entities are being compromised—whether large or small—in Australia or internationally.”*

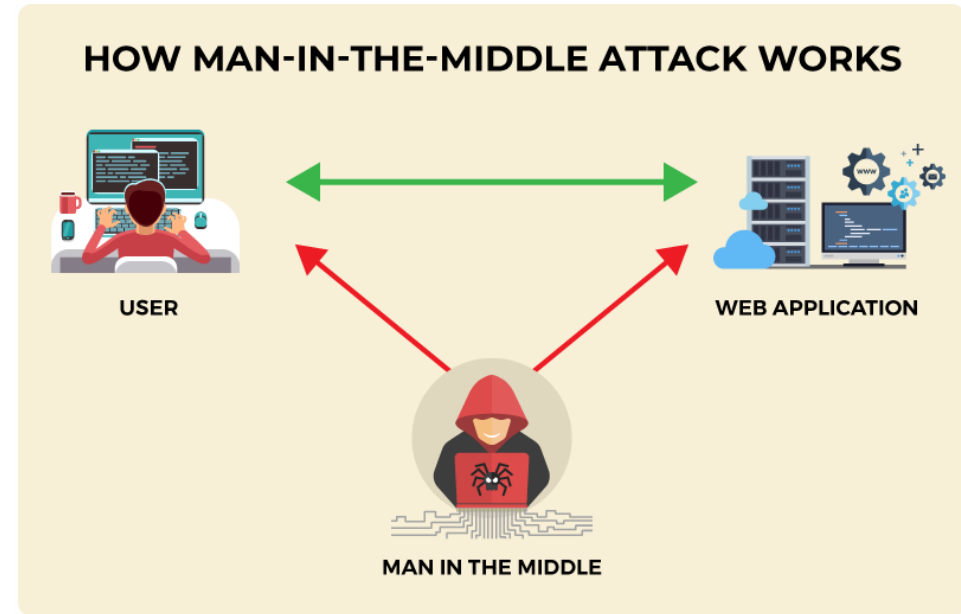
Source: <https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics/ndb-scheme-12-month-insights-report.pdf>

***a continuous program of  
cyber security training for all users  
is critical!***

“But my emails and data are safe in the cloud”... :



## Case Study: Man in The Middle Attack



(Source: CISO Mag)

# Cyber Risks 2024: Ransomware



Source: <https://www.barracuda.com/reports/ransomware-insights-report-2023>

# Cyber Risks 2024: Ransomware

“Ransomware is continually evolving and it’s really hard to keep track of all the different strains” says John Moretti, CISSP, CCSK & CEH, Principal Solutions Architect at eSentire.

“While each ransomware variant has different ways of spreading, all ransomware variants rely on similar social engineering tactics to deceive users and hold their data hostage.”

<https://www.esentire.com/resources/library/2022-official-cybercrime-report>

*"One single vulnerability is all an attacker needs."*

*Window Snyder, Chief Security Officer, Fastly*

# Social Engineering Case Study 2021 - Conti Ransomware :

The Register®

SECURITY

## Irish Health Service ransomware attack happened after one staffer opened malware-ridden email

34

PWC report shows long list of missed opportunities to shut out extortion crims

Gareth Corfield

Fri 10 Dec 2021 // 21:05 UTC

**Ireland's Health Service Executive (HSE) was almost paralysed by ransomware after a single user opened a malicious file attached to a phishing email, a consultancy's damning report has revealed.**

**Issued today, the report from PWC (formerly known as PriceWaterhouseCoopers) said that the hugely harmful Conti ransomware infection was caused because of the simplest attack vector known to infosec: spam.**

PWC said, in the report's executive summary:

**"The Malware infection was the result of the user of the Patient Zero Workstation clicking and opening a malicious Microsoft Excel file that was attached to a phishing email sent to the user on 16 March 2021."**

[https://www.theregister.com/2021/12/10/ireland\\_health\\_conti\\_ransomware\\_attack\\_report/](https://www.theregister.com/2021/12/10/ireland_health_conti_ransomware_attack_report/)



Feidhmeannas Seirbhíse Sláinte  
Health Service Executive



Redacted

<https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf>



# Healthcare's cyber resilience under siege as attacks multiply

## + HELP NET SECURITY



Mirko Zorz, Director of Content, Help Net Security  
April 4, 2024

***What are the most common and dangerous cyber threats facing the healthcare sector in 2024?***

**“Cyber threats haven’t necessarily changed, but they’ve become more frequent in healthcare.**

**The most common threat to healthcare systems remains phishing attacks, sent in hopes that just one person, out of thousands, clicks a link or opens a file contained within the email.**

**That file or link gets the hackers’ foot in the door to the network and from there, they can either lock the system down with ransomware or steal data.**

Stolen data can be leveraged in a multitude of ways by criminals, ranging from medical ID theft to extorting from patients directly.

We saw a recent attack on Change Healthcare shut down the largest payer system in the U.S.

DDoS (distributed denial of service) attacks are also prevalent, but ransomware has certainly dominated headlines in recent years.

Many attacks against healthcare organizations come from outside the U.S., and the sophistication of these cyberattacks allows deeper access to systems or data within a system. We can likely expect these attacks to continue to grow in 2024.

Many of these instances are coming from bad actors offshore. While there’s not much one can do about being targeted, healthcare organizations can certainly take steps to strengthen their network’s cyber resilience as well as educate employees on how to be vigilant in detecting potential risks.”


Source: <https://www.helpnetsecurity.com/2024/04/04/eric-demers-madaket-health-healthcare-organizations-cyber-resilience/>



Eric Demers, CEO  
of Madaket Health

# Healthcare's cyber resilience under siege as attacks multiply

**+ HELP NET SECURITY**

 **Mirko Zorz**, Director of Content, Help Net Security  
April 4, 2024

***What are your recommendations for enhancing cyber resilience in the healthcare sector?***

**“...Cyberattacks will not stop and healthcare systems are in for a continuous battle. As such, healthcare organizations must do everything possible to ensure their systems are protected and access is appropriately restricted.** As these attacks happen, depending on what part of the data you’re working with or storing, working with partners, vendors or applications that allow you to manage high volumes of data while being up-to-date across that data can be helpful..”



**Eric Demers, CEO  
of [Madaket Health](#)**

Source: <https://www.helpnetsecurity.com/2024/04/04/eric-demers-madaket-health-healthcare-organizations-cyber-resilience/>

# Top Cyber Risks 2024 : Generative AI

Cyber attacks are more sophisticated than ever and IT leaders feel ill-equipped to handle emerging threats



Source: [https://www.keepersecurity.com/en\\_GB/top-data-threats-insight-report/](https://www.keepersecurity.com/en_GB/top-data-threats-insight-report/)

# Top Cyber Risks 2024 : Common cyber attacks



Source: [https://www.keepersecurity.com/en\\_GB/top-data-threats-insight-report/](https://www.keepersecurity.com/en_GB/top-data-threats-insight-report/)



# Fundamental cybersecurity best practices still vital:



## Conclusion

### Attacks are changing but fundamental cybersecurity best practices are not

Keeper's research illuminates the new and novel ways attackers are wreaking havoc on today's enterprises, mid market organisations and small businesses. With AI-powered attacks at the helm, the tools in cybercriminals' arsenals are growing more sophisticated. As technology continues to advance, fighting evolving threats requires constant adaptation.

Despite this ever-evolving threat landscape, the fundamental rules of protecting an organisation in the digital landscape remain relevant. Organisations should prioritise adoption of solutions that prevent the most prevalent cyber attacks, including password and PAM solutions. A password manager can mitigate risks by enforcing strong password practices, while PAM safeguards an organisation's vital assets by controlling and monitoring high-level access, collectively fortifying defences and minimising potential damage in the event that a successful cyber attack does occur. Integrating these solutions creates a layered security approach that stands the test of time – restricting unauthorised access and enhancing overall cybersecurity resilience – **now and in the future.**

Source: [https://www.keepersecurity.com/en\\_GB/top-data-threats-insight-report/](https://www.keepersecurity.com/en_GB/top-data-threats-insight-report/)



# Cyber Security Essentials:

The purpose of information / cyber security is to protect  
*and* maintain the

***CONFIDENTIALITY, INTEGRITY and AVAILABILITY***

of the computer systems and data assets

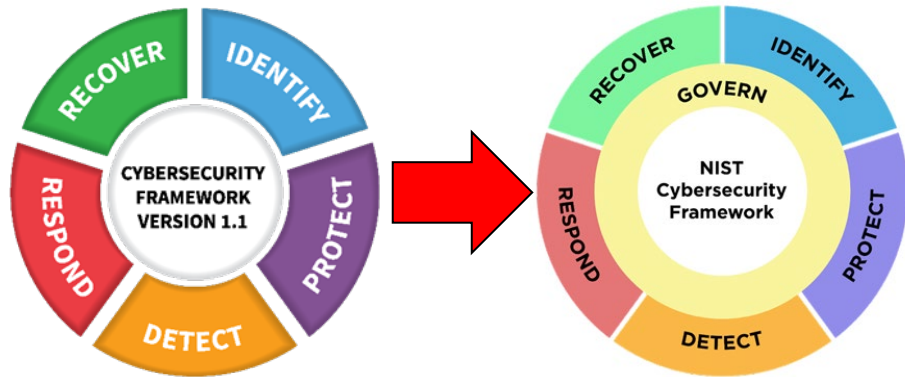


*The C.I.A. Triad for Cyber Security*

# Standards based Cyber Security:

## National Institute of Standards and Technology (NIST)

### Cyber Security Framework v1.1 /v2.0



NIST CSF v1.1

NIST CSF v2.0

<https://www.nist.gov/cyberframework>

## ISO/IEC 27001



<https://www.iso.org/isoiec-27001-information-security.html>

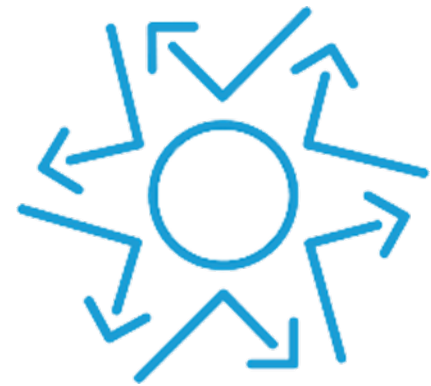
## CIS Controls v8



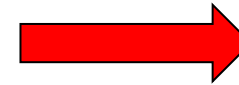
<https://www.cisecurity.org/controls/cis-controls-list>

# Essential Eight mitigation strategies

from the Australian Cyber Security Centre:



Aim for at least Maturity Level Two



## Introduction

The Australian Cyber Security Centre (ACSC) has developed prioritised mitigation strategies, in the form of the *Strategies to Mitigate Cyber Security Incidents*, to help organisations mitigate cyber security incidents caused by various cyber threats. The most effective of these are known as the Essential Eight.

## Maturity levels

To assist organisations in determining the maturity of their implementation of the Essential Eight, three maturity levels have been defined for each mitigation strategy. The maturity levels are defined as:

- Maturity Level One: Partly aligned with the intent of the mitigation strategy.
- **Maturity Level Two: Mostly aligned with the intent of the mitigation strategy.**
- Maturity Level Three: Fully aligned with the intent of the mitigation strategy.

## What maturity level to aim for

As a baseline organisations should aim to reach Maturity Level Three for each mitigation strategy. Where the ACSC believes an organisation requires a maturity level above that of Maturity Level Three, the ACSC will provide tailored advice to meet the specific needs of the organisation.

## Further information

The *Australian Government Information Security Manual (ISM)* assists in the protection of information that is processed, stored or communicated by organisations' systems. It can be found at <https://www.cyber.gov.au/acsc/view-all-content/ism>.

The *Strategies to Mitigate Cyber Security Incidents* complements the advice in the ISM. The complete list of strategies can be found at <https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents>.

## Contact details

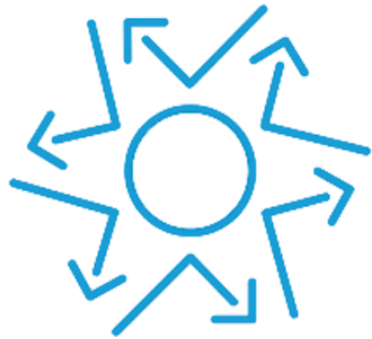
If you have any questions regarding this guidance you can contact us via 1300 CYBER1 (1300 292 371) or <https://www.cyber.gov.au/acsc/contact>.

[cyber.gov.au](https://www.cyber.gov.au)

# Essential Eight mitigation strategies

from the Australian Cyber Security Centre:

“The Essential Eight is a series of baseline mitigation strategies taken from the **Strategies to Mitigate Cyber Security Incidents** recommended for organisations. Implementing these strategies as a minimum makes it much harder for adversaries to compromise systems.”



<https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model>

ASD Essential Eight	
<b>1. Application Control</b>	Application control is implemented on all workstations to restrict the execution of executables, software libraries, scripts and installers to an approved set. Application control is implemented on all servers to restrict the execution of executables, software libraries, scripts and installers to an approved set.
<b>2. Patching Applications</b>	Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within two weeks of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions
<b>3. Configuring Microsoft Office macro settings</b>	Only allow signed MS Office macros, block untrusted macros in internet sourced documents, prevent users from changing macro security settings
<b>4. Application Hardening</b>	Web browsers are configured to block or disable support for Flash content, web advertisements, Java from the internet.
<b>5. Restricting Administrative Privileges</b>	Limit privileged users’ access to systems, applications and data repositories, reading emails, browsing the web and obtaining files via online services
<b>6. Patching Operating Systems</b>	Patch known security vulnerabilities in Operating Systems and firmware within 2 weeks of patch identification. Update or replace vendor unsupported versions
<b>7. Multi-Factor Authentication</b>	Multi Factor Authentication (MFA, also known as 2Factor Authentication), is required for all remote access and to authenticate all privileged users to protect against risky activities and credential theft
<b>8. Daily Backups</b>	To maintain the availability of uninfected critical data, <b>must be stored in a non-rewritable and non-erasable manner</b> – i.e. <b>IMMUTABLE</b> – <b>cannot be changed or erased</b> - and kept offline i.e. “ <b>air gapped</b> ”, and stored for three months or more, with restorations tested at regular intervals

# Essential Eight Maturity Model

<https://www.acsc.gov.au/publications/protect/essential-eight-maturity-model.pdf>

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
Application control	Application control is implemented on all workstations to restrict the execution of executables to an approved set. Application control is implemented on all servers to restrict the execution of executables to an approved set.	Application control is implemented on all workstations to restrict the execution of executables, software libraries, scripts and installers to an approved set. Application control is implemented on all servers to restrict the execution of executables, software libraries, scripts and installers to an approved set.	Application control is implemented on all workstations to restrict the execution of executables, software libraries, scripts and installers to an approved set. Application control is implemented on all servers to restrict the execution of executables, software libraries, scripts and installers to an approved set. Microsoft's latest recommended block rules are implemented to prevent application control bypasses.
Patch applications	Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within one month of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within two weeks of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. An automated mechanism is used to confirm and record that deployed application and driver patches or updates have been installed, applied successfully and remain in place. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.
Configure Microsoft Office macro settings	Microsoft Office macros are allowed to execute, but only after prompting users for approval. Microsoft Office macro security settings cannot be changed by users.	Only signed Microsoft Office macros are allowed to execute. Microsoft Office macros in documents originating from the internet are blocked. Microsoft Office macro security settings cannot be changed by users.	Microsoft Office macros are only allowed to execute in documents from Trusted Locations where write access is limited to personnel whose role is to vet and approve macros. Microsoft Office macros in documents originating from the internet are blocked. Microsoft Office macro security settings cannot be changed by users.
User application hardening	Web browsers are configured to block or disable support for Flash content.	Web browsers are configured to block or disable support for Flash content. Web browsers are configured to block web advertisements. Web browsers are configured to block Java from the internet.	Web browsers are configured to block or disable support for Flash content. Web browsers are configured to block web advertisements. Web browsers are configured to block Java from the internet. Microsoft Office is configured to disable support for Flash content. Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.
Restrict administrative privileges	Privileged access to systems, applications and information is validated when first requested. Policy security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.	Privileged access to systems, applications and data repositories is validated when first requested and revalidated on an annual or more frequent basis. Policy security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.	Privileged access to systems, applications and data repositories is validated when first requested and revalidated on an annual or more frequent basis. Privileged access to systems, applications and data repositories is limited to that required for personnel to undertake their duties. Technical security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.
Patch operating systems	Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within one month of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within two weeks of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. An automated mechanism is used to confirm and record that deployed operating system and firmware patches or updates have been installed, applied successfully and remain in place. Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.
Multi-factor authentication	Multi-factor authentication is used to authenticate all users of remote access solutions. Multi-factor authentication uses at least two of the following authentication factors: passwords, Universal 2nd Factor security keys, physical one-time password tokens, biometrics, smartcards, mobile app one-time password tokens, SMS messages, emails, voice calls or software certificates.	Multi-factor authentication is used to authenticate all users of remote access solutions. Multi-factor authentication is used to authenticate all privileged users and any other positions of trust. Multi-factor authentication uses at least two of the following authentication factors: passwords, Universal 2nd Factor security keys, physical one-time password tokens, biometrics, smartcards or mobile app one-time password tokens.	Multi-factor authentication is used to authenticate all users of remote access solutions. Multi-factor authentication is used to authenticate all privileged users and any other positions of trust. Multi-factor authentication is used to authenticate all users when accessing important data repositories. Multi-factor authentication uses at least two of the following authentication factors: passwords, Universal 2nd Factor security keys, physical one-time password tokens, biometrics or smartcards.
Daily backups	Backups of important information, software and configuration settings are performed monthly. Backups are stored for between one to three months. Partial restoration of backups is tested on an annual or more frequent basis.	Backups of important information, software and configuration settings are performed weekly. Backups are stored offline, or online but in a non-rewritable and non-erasable manner. Backups are stored for between one to three months. Full restoration of backups is tested at least once. Partial restoration of backups is tested on a bi-annual or more frequent basis.	Backups of important information, software and configuration settings are performed at least daily. Backups are stored offline, or online but in a non-rewritable and non-erasable manner. Backups are stored for three months or greater. Full restoration of backups is tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur. Partial restoration of backups is tested on a quarterly or more frequent basis.

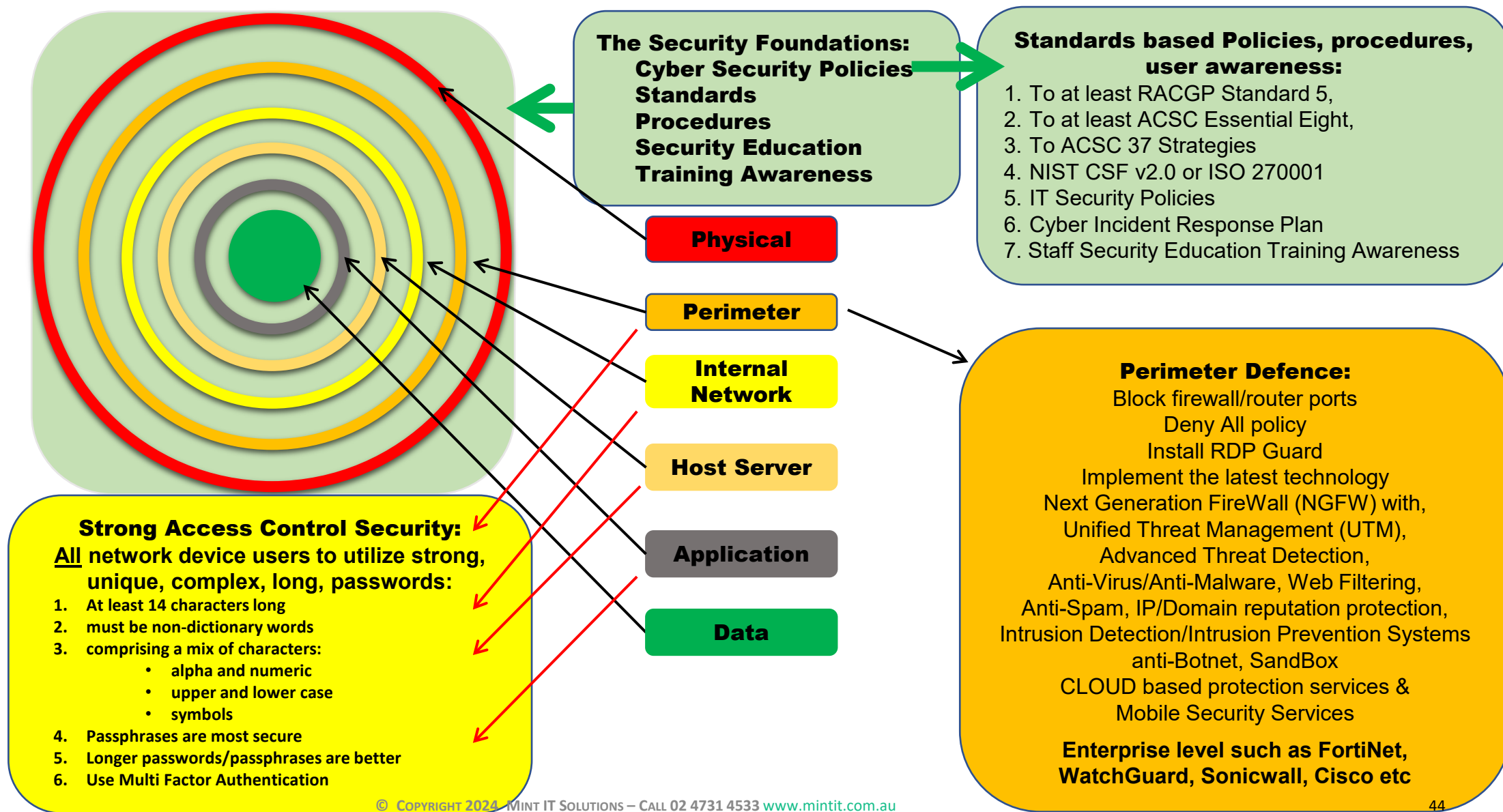


# The ASD 37 Check List: Is our Practice Cyber Secure?

ASD #	Relative Security Effectiveness	ACSC Australian Cyber Security Centre cyber.gov.au	ASD 37 Strategies to Mitigate Cyber Security Incidents Check List:	Our current state?	Yes	No	?	Suggested Mitigation Strategy Implementation Order (start with threats of most concern to the organisation)
<b>Mitigation Strategies to Prevent Malware Delivery and Execution:</b>								
ASD 01	Essential		Application control to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.					<p><b>Targeted cyber intrusions</b> (advanced persistent threats) and other external adversaries who steal data</p> <ol style="list-style-type: none"> <li>Implement 'essential' mitigation strategies to:                             <ol style="list-style-type: none"> <li>prevent malware delivery and execution</li> <li>limit the extent of cyber security incidents</li> <li>detect cyber security incidents and respond.</li> </ol> </li> <li>Repeat step 1 with 'excellent' mitigation strategies.</li> <li>Repeat step 1 with less effective mitigation strategies until an acceptable level of residual risk is reached.</li> </ol> <p><b>Ransomware and external adversaries who destroy data and prevent computers/networks from functioning:</b></p> <ol style="list-style-type: none"> <li>Implement 'essential' mitigation strategies to:                             <ol style="list-style-type: none"> <li>recover data and system availability</li> <li>prevent malware delivery and execution</li> <li>limit the extent of cyber security incidents</li> <li>detect cyber security incidents and respond.</li> </ol> </li> <li>Repeat step 1 with 'excellent' mitigation strategies.</li> <li>Repeat step 1 with less effective mitigation strategies until an acceptable level of residual risk is reached.</li> </ol> <p>Note that 'Hunt to discover incidents' is less relevant for ransomware that immediately makes itself visible.</p> <p><b>Malicious insiders who steal data:</b></p> <ol style="list-style-type: none"> <li>Implement 'Control removable storage media and connected devices' to mitigate data exfiltration.</li> <li>Implement 'Outbound web and email data loss prevention'.</li> <li>Implement 'essential' mitigation strategies to:                             <ol style="list-style-type: none"> <li>limit the extent of cyber security incidents</li> <li>detect cyber security incidents and respond.</li> </ol> </li> <li>Repeat step 3 with 'excellent' mitigation strategies.</li> <li>Implement 'Personnel management'.</li> <li>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.</li> </ol> <p>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.</p> <p><b>Malicious insiders who destroy data and prevent computers/networks from functioning:</b></p> <ol style="list-style-type: none"> <li>Implement 'essential' mitigation strategies to:                             <ol style="list-style-type: none"> <li>recover data and system availability</li> <li>limit the extent of cyber security incidents</li> <li>detect cyber security incidents and respond.</li> </ol> </li> <li>Repeat step 1 with 'excellent' mitigation strategies.</li> <li>Implement 'Personnel management'.</li> <li>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.</li> </ol>
ASD 02	Essential		Patch applications (e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers). Patch/mitigate computers with 'extreme risk' security vulnerabilities within 48 hours. Use the latest version of applications.					
ASD 03	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.					
ASD 04	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.					
ASD 05	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).					
ASD 06	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.					
ASD 07	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.					
ASD 08	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.					
ASD 09	Excellent		Operating system generic exploit mitigation e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET).					
ASD 10	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.					
ASD 11	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).					
ASD 12	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.					
ASD 13	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.					
ASD 14	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.					
ASD 15	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.					
ASD 16	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.					
ASD 17	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.					
<b>Mitigation Strategies to Limit the Extent of Cyber Security Incidents:</b>								
ASD 18	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.					
ASD 19	Essential		Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' security vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.					
ASD 20	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.					
ASD 21	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.					
ASD 22	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.					
ASD 23	Excellent		Protect authentication credentials. Remove CPassword values (MS14-025). Configure WDigest (KB2871997). Use Windows Defender Credential Guard. Change default passphrases. Require long complex passphrases.					
ASD 24	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).					
ASD 25	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).					
ASD 26	Very Good		Software-based application firewall, blocking outgoing network traffic that is not generated by approved/trusted programs, and denying network traffic by default.					
ASD 27	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.					
<b>Mitigation Strategies to Detect Cyber Security Incidents and Respond:</b>								
ASD 28	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.					
ASD 29	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).					
ASD 30	Very Good		Endpoint detection and response software on all computers to centrally log system behaviour and facilitate incident response. Microsoft's free SysMon tool is an entry level option.					
ASD 31	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.					
ASD 32	Limited		Network-based intrusion detection/prevention system using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.					
ASD 33	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.					
<b>Mitigation Strategies to Recover Data and System Availability:</b>								
ASD 34	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.					
ASD 35	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.					
ASD 36	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.					
<b>Mitigation Strategy Specific to Preventing Malicious Insiders:</b>								
ASD 37	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.					



# Cyber Security Basics - Defence in Depth / Layered Defence:



# Cyber hygiene is everyone's responsibility:

Remember the Human Factor –

*i.e. : you and your staff click on fake emails, attachments and links!*

## Malware Awareness Training

*Every staff member should have a basic understanding of cyber threats:*

- *Phishing attacks*
- *Social Engineering attacks*
- *Ransomware*
- *Safe Web Browsing*
- *Creating Strong Passwords / Passphrases*
- *Multi-Factor Authentication for strong Identity & Access Management*

# Cyber hygiene is everyone's responsibility:

Remember the Human Factor – i.e. : *humans click on fake emails, attachments and links!*

## Malware Awareness Training:

Remember to:

- *Think before you click, to stay safe online*
- *Adopt safe email practises to reduce the risk of a security incident or data breach*
- *Avoid sharing too much information when posting online*
- *Follow the “need to know” principle*
- *Be aware of who is around you*
- *Adopt a clear desk policy*
- *Lock your computer*
- *Don't use public Wi-Fi to access or send sensitive information.*

Source: <https://training.digitalhealth.gov.au>

# Preventing and Defending against Social Engineering attacks:

<b>People:</b>	<ol style="list-style-type: none"><li>1. implementing regular Security Education, Training and Awareness programs (SETA), including simulated phishing attacks, Social Network threat awareness (social media platforms are favourites for hackers – <i>they go where the most people are gathered.</i>)</li><li>2. track and test staff completion, understanding and comprehension progression.</li></ol>
<b>Process:</b>	<ol style="list-style-type: none"><li>1. implementing cyber security standards based security policies, standards, procedures, and guidelines – and making sure that all staff are made aware of them, both formally and informally.</li><li>2. to build a culture of cyber security.</li><li>3. implementing Business Continuity Plans, and.</li><li>4. develop and implement Incident Response policies and procedures, etc.</li></ol>
<b>Technical:</b>	<ol style="list-style-type: none"><li>1. implementing controls such as, Multi-Factor Authentication (MFA) for enhanced access control and authentication.</li><li>2. deploying the latest Extended Detection and Response (XDR) anti malware software systems with Artificial Intelligence (AI) and Machine Learning (ML) technologies.</li><li>3. installing Next Generation Firewalls (NGFW) for perimeter defence (and making certain the NGFW firewalls are configured correctly – just ask Medibank!).</li><li>4. DNS filtering to prevent access to “bad” websites.</li><li>5. implement enterprise grade email security which includes Heuristics based scanning, Cloud based AntiSpam Filtering and Phishing Detection, Content Filtering, Outbound Filtering, Impostor Email Protection, Data Loss Prevention, URL Defense (Sandboxing), Attachment Defense (Reputation Protection), Email Data Loss Prevention, Automated Email Encryption, Threat Protection for Microsoft Office 365, Social Media Account Protection, etc.</li></ol>

# Strong Access Controls:

## Enforce strong, complex credentials and MFA:

Source: [Nordpass \(2022\)](#)

Rank	Password	Time to crack it
1	123456	< 1 second
2	password	< 1 second
3	lizottes	3 hours
4	password1	< 1 second
5	123456789	< 1 second
6	12345	< 1 second
7	abc123	< 1 second
8	qwerty	< 1 second
9	12345678	< 1 second
10	holden	2 minutes

VS

**Strong Access Control Security:**  
**All network device users to utilize strong, unique, complex, long, passwords or pass phrases:**

1. At least 14 characters long
2. must be non-dictionary words
3. comprising a mix of characters:
  - alpha and numeric
  - upper and lower case
  - symbols
4. Passphrases are most secure
5. Longer passwords/passphrases are better
6. Use Multi Factor Authentication

Source: <https://training.digitalhealth.gov.au>

# Strong Access Controls:

## Enforce strong, complex credentials and MFA:

PASSWORD/ PASSPHRASE	TIME TO CRACK		EASY TO REMEMBER	COMMENTS
	Brute Force Attack	Dictionary Attack		
<b>password123</b>	Instantly Less than AU\$0.01	Instantly Less than AU\$0.01	Very Easy (too easy)	One of the most commonly used passwords on the planet.
<b>Spaghetti95!</b>	48 hours AU\$587.50	Less than half an hour AU\$6.10	Easy	Some complexity in the most common areas, and very short length. Easy to remember, but easy to crack.
<b>5paghetti!95</b>	24 hours AU\$293.70	Less than 1 hour AU\$12.20	Somewhat Easy	Not much more complexity than above with character substitution, and still short length. Easy to remember, but easy to crack.
<b>A&amp;d8j+!</b>	2.5 hours AU\$30.60	2.5 hours AU\$30.60	Very Difficult	Mildly complex, but shorter than the above passwords. Hard to remember, easy to crack (against BFA).
<b>I don't like pineapple on my pizza!</b>	More than 1 Year More than AU\$107,222.40	More than 40 days More than AU\$11,750.40	Easy	Excellent character length (35 characters). Complexity is naturally high given the apostrophe, exclamation mark and use of spaces. Very easy to remember, and very difficult to crack.

<https://www.cyber.gov.au/acsc/small-and-medium-businesses/acsc-small-business-guide>



# Digital Health security awareness training resources:

<https://training.digitalhealth.gov.au/>

This course will take approximately 1 hour 45 minutes to complete. You will need to complete all five modules to receive a certificate.



Australian Digital Health Agency - Online Learning Portal

## Australian College of Rural and Remote Medicine (ACRRM)



## Royal Australian College of General Practitioners (RACGP)

This module has been allocated 0.5 educational activities in the RACGP's Continuing Professional Development (CPD) Program for the 2023-25 triennium.



## Australian Association of Practice Management (AAPM)



## Australian Digital Health Agency - Online Learning Portal



For healthcare providers



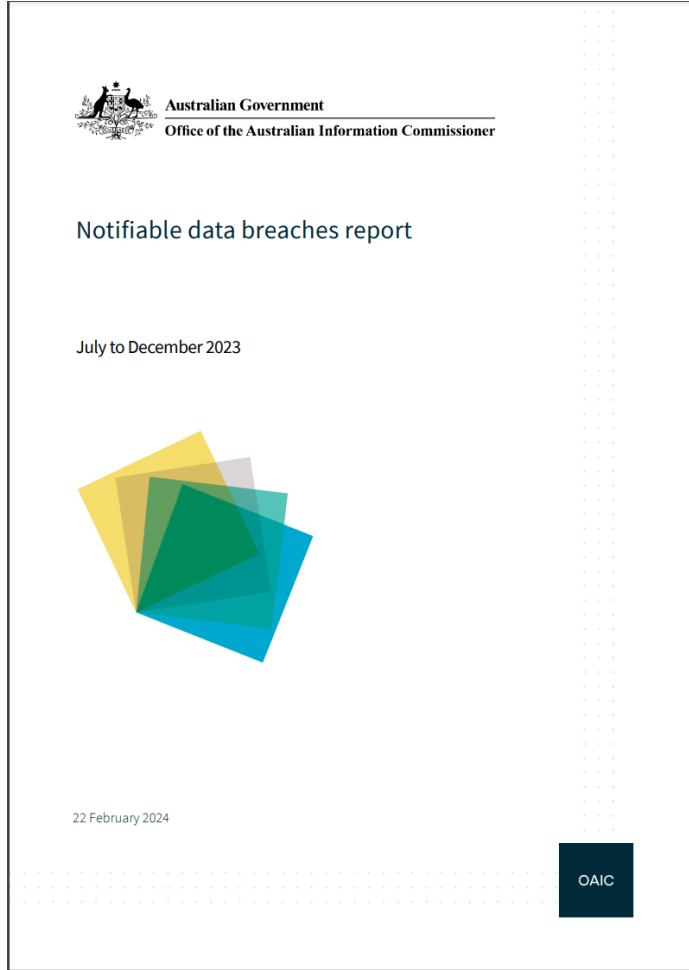
For everyone

# Digital Health security awareness training resources:

<https://training.digitalhealth.gov.au/>

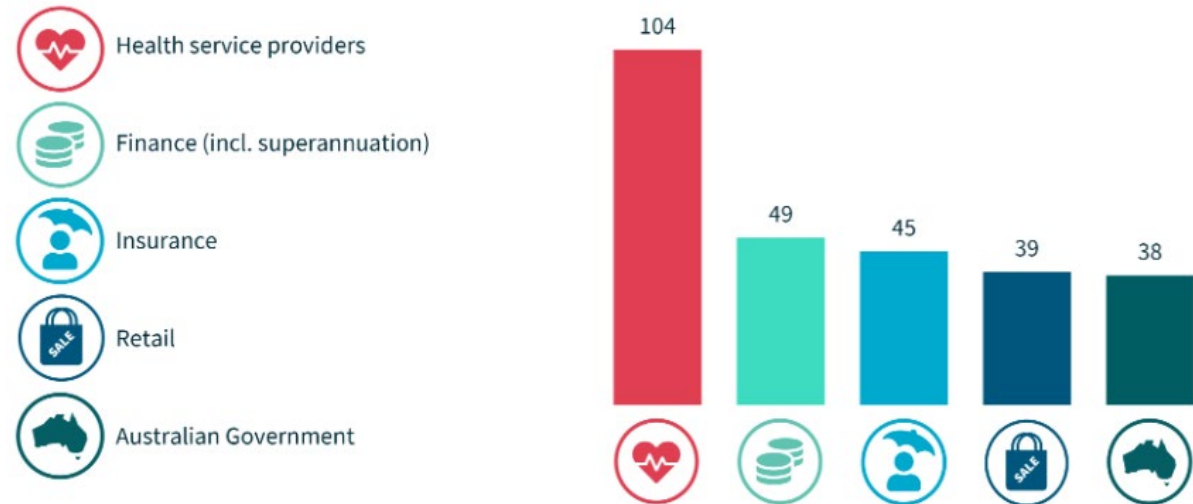


# Healthcare sector tops the Notifiable Data Breaches Report, again: July – December 2023:



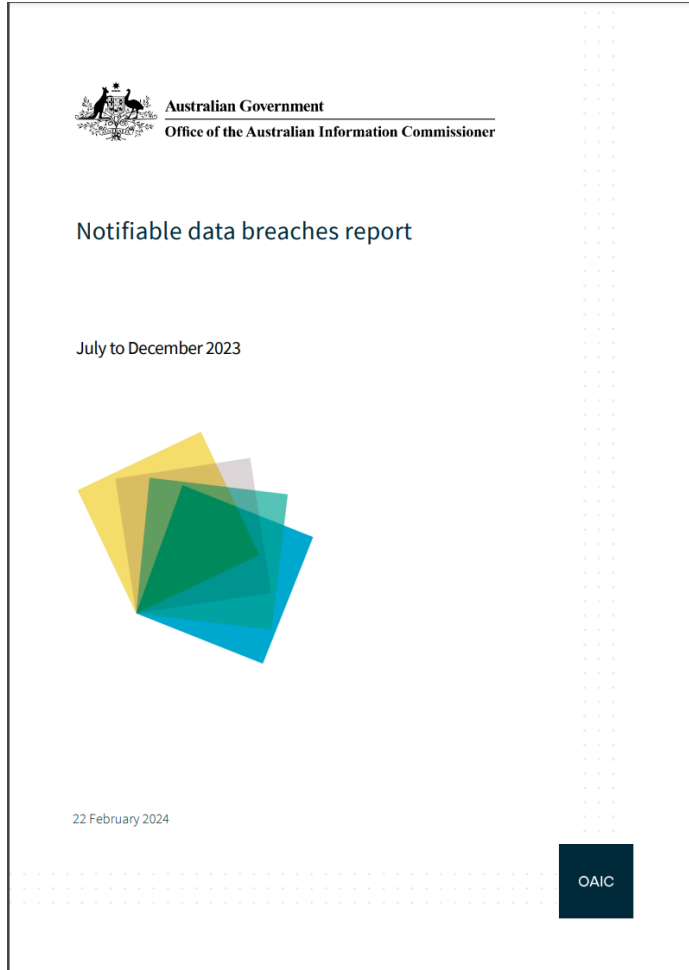
“The latest Office of Australian Information Commissioner (OAIC) Notifiable Data Breaches Report for July – December 2023 identifies healthcare providers at the top of the list” ...

## Top 5 sectors to notify data breaches



Source: <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-july-to-december-2023>

# Healthcare sector tops the Notifiable Data Breaches Report, again: July – December 2023:



## Cyber incidents

In this reporting period, phishing (28%, 59 notifications) took over from ransomware (27%, 57 notifications) as the top source of cyber incidents. Compromised credentials – through phishing, a brute-force attack or an unknown method – comprised 58% of all cyber incidents.

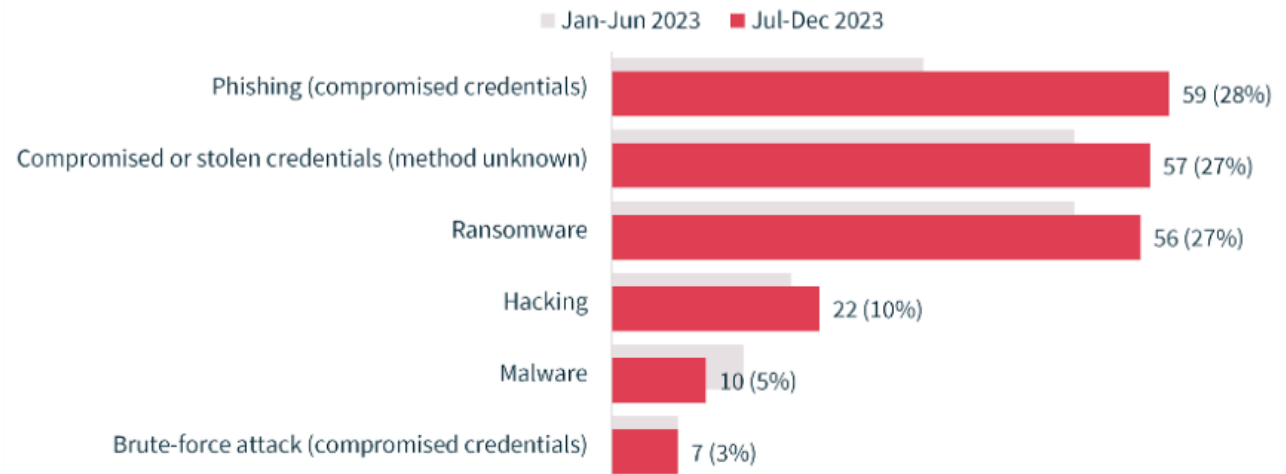
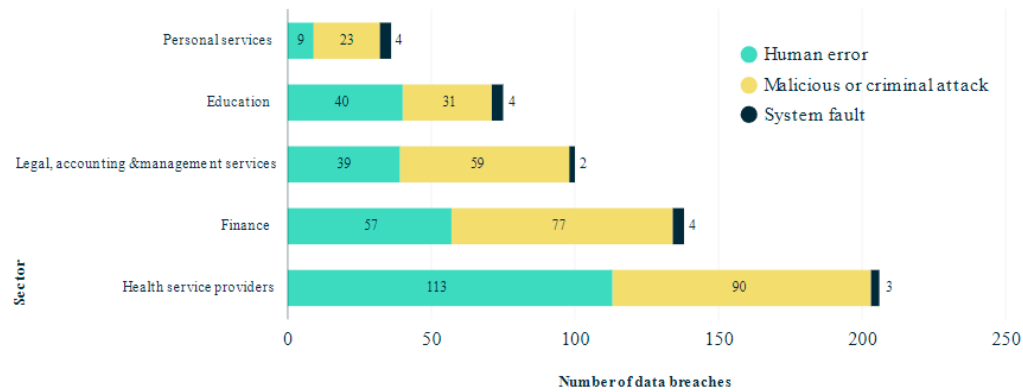


Chart 11: Cyber incident breakdown

Source: <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-july-to-december-2023>

# Healthcare sector tops the Notifiable Data breaches Report, again, and again: – from the start of Notifiable Data Breaches Scheme in 2018

Figure 7 – Sources of breaches—top five sectors, from 1 April 2018 to 31 March 2019



Top 5 industry sectors	NDBs received
Health service providers	15
Legal, Accounting & Management services	10
Finance (incl. superannuation)	8
Education	6
Charities	4

1 January – 31 March 2018

Top 5 industry sectors	Data breaches received
Health service providers <sup>[1]</sup>	45
Finance (incl. superannuation) <sup>[2]</sup>	35
Legal, accounting & management services	34
Education <sup>[3]</sup>	16
Personal services <sup>[4]</sup>	13

1 July – 30 September 2018

Table 2.A – Top 5 industry sectors by notifications in the quarter

Top 5 industry sectors	Number of data breaches received
Health service providers <sup>[1]</sup>	49
Finance <sup>[2]</sup>	36
Legal, Accounting & Management services	20
Education <sup>[3]</sup>	19
Business and Professional Associations	15

1 April – 30 June 2018

Table 2.A – Top five sectors by notifications in the quarter

Top five sectors	NDBs received
Health service providers <sup>[1]</sup>	54
Finance (incl. superannuation) <sup>[2]</sup>	40
Legal, accounting and management services	23
Education <sup>[3]</sup>	21
Mining and manufacturing	12

1 October – 30 December 2018

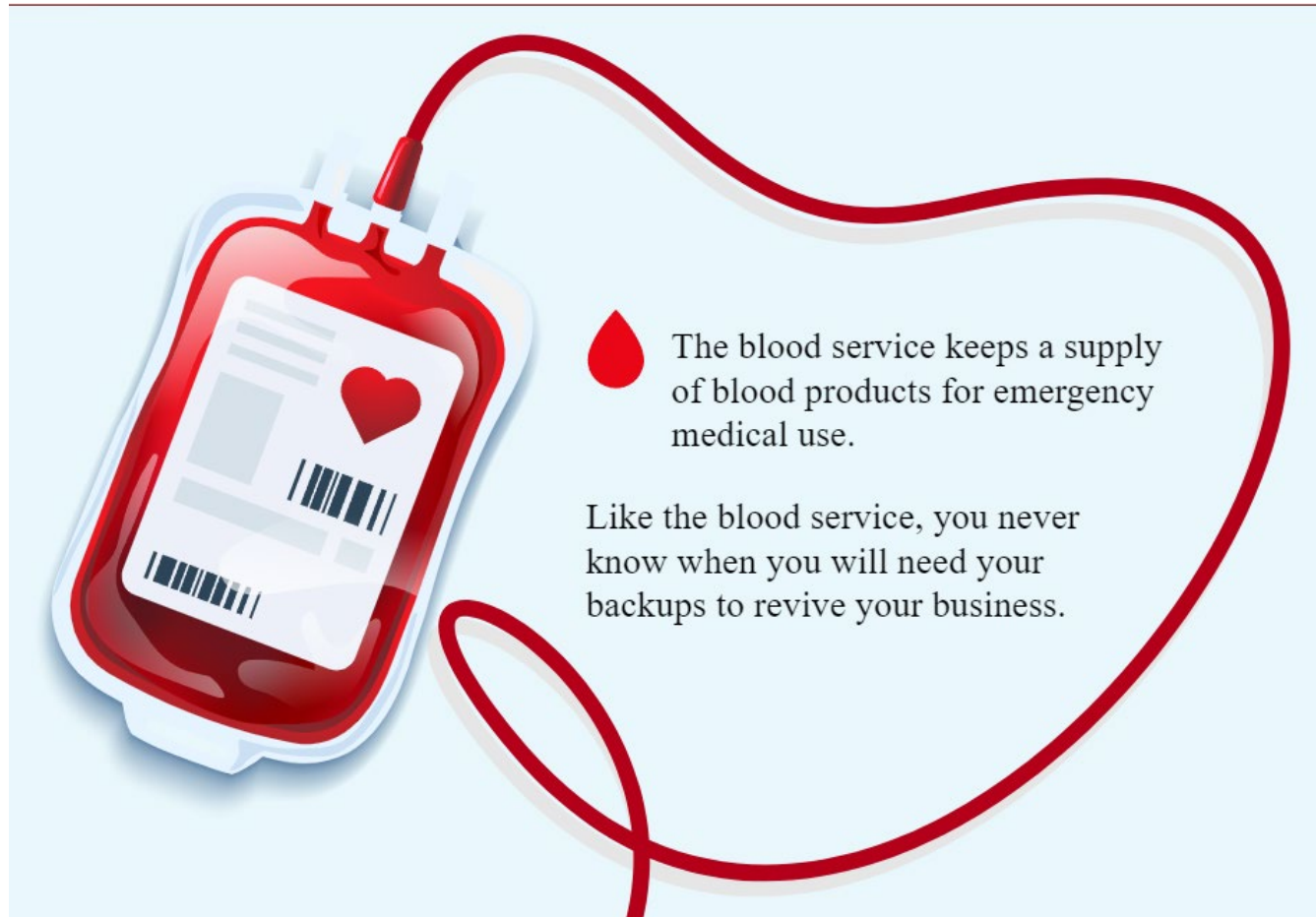
Source: <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications>





# BACKUP BACKUP BACKUP:

An essential preventive activity for the health and business continuity of a general practice



Source: <https://training.digitalhealth.gov.au>





# BACKUP BACKUP BACKUP:

## The new 3 – 2 – 1 – 1 Data Backup rule:

A simple but still very effective backup strategy for data backup is to follow the 3-2-1-1 rule. This should be the minimum backup strategy for clinical data and complete system configuration:



Network Attached Storage (NAS) is a network attached external disk array with multiple hard drives



USB 3.0 hard drives for full off-site backup

**Secure online cloud-based data centre backups for off-site backup is the modern alternative to USB disks**

<p><b>3</b> - copies of data kept at all times</p>	<p>primary data copy <i>and</i> 2 additional copies:</p> <ol style="list-style-type: none"> <li>1. Server with RAID Array, <i>plus</i></li> <li>2. Network Attached Storage (NAS), <i>plus</i></li> <li>3. Off site USB or On-line backup or even better</li> <li>4. Off-site USB <i>plus</i> On-Line backup</li> </ol>
<p><b>2</b> - different media used</p>	<p>originally hard drives and magnetic tape, floppy drives and optical media for backups, however server hard drives and other physically separated hard disk storage such as a NAS and external USB hard drives / Secure On-line cloud-based data centre backups are more practical today</p>
<p><b>1</b> - copies kept offsite plus, multiple archive copies</p>	<p>1x full system backup copy on separate, multiple media such as USB 3.0 hard drives for each day clinic is open or trading, rotated off site daily, maintaining an “air gap” (i.e. disconnected from the network),</p>
<p><b>1</b> – IMMUTABLE multiple archive copies kept offsite</p>	<p>On IMMUTABLE media – i.e. non-rewritable, non-erasable, with monthly archive copies held for up to a year in quarantine, plus a spare USB drive in case one fails. Also consider Managed On-Line backup to a secure datacentre with same IMMUTABLE principles.: “air gapped”, non-rewritable, non-erasable, 3 copies, and long archive retention</p>



# BACKUP BACKUP BACKUP:

## Backup Case 1:

We were contacted by the practice manager at approximately 9:30am regarding their inability to access clinical software.

On examination of the server, it was determined that the data had been maliciously encrypted.

There was no onsite backup process in place however there was a cloud-based offsite backup of the clinical software database files only. This meant that the server operating system would need to be reinstalled from scratch prior to recovery of the data files, potentially causing a long delay in the practice being able to resume operations.

As an interim measure, another computer was prepared, and the recovered files were installed onto this computer to allow the practice to manage appointments and carry out limited consultations. This was in place by early afternoon that day.

Meanwhile, the systems software was reinstalled onto the server and the clinical data files were recovered to the server.

The server was back in place and available for use in the morning of the following day...



*Secure online cloud-based data centre backups using specialized backup software for off-site backup is the modern alternative to rotating off-site USB disks*



# BACKUP BACKUP BACKUP:

## Backup Case 2:

Following notification by the practice that they were unable to use Medical Director, it was found that the server and some PCs had been encrypted in a ransomware attack.

This practice was utilizing specialized backup management software, which was configured to automatically take backups every night. The backup files contained a copy of the entire server, including the operating system and the clinical database files. The files were being stored on external USB hard drives which were being swapped and cycled off-site on a daily basis. The backup files on the off-site USB hard drives were not encrypted.



Because the specialized backup software was in use at this practice, the encrypted server was formatted to erase the ransomware, then we were able to effectively attach the external USB drive containing the backup files to another computer and then transfer the backup data back to the clean server to bring the practice back online.

*USB 3.0 hard drives for full off-site backup*

# Essential Eight Maturity Model

<https://www.acsc.gov.au/publications/protect/essential-eight-maturity-model.pdf>

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
Application control	Application control is implemented on all workstations to restrict the execution of executables to an approved set. Application control is implemented on all servers to restrict the execution of executables to an approved set.	Application control is implemented on all workstations to restrict the execution of executables, software libraries, scripts and installers to an approved set. Application control is implemented on all servers to restrict the execution of executables, software libraries, scripts and installers to an approved set.	Application control is implemented on all workstations to restrict the execution of executables, software libraries, scripts and installers to an approved set. Application control is implemented on all servers to restrict the execution of executables, software libraries, scripts and installers to an approved set. Microsoft's latest recommended block rules are implemented to prevent application control bypasses.
Patch applications	Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within one month of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within two weeks of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. An automated mechanism is used to confirm and record that deployed application and driver patches or updates have been installed, applied successfully and remain in place. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.
Configure Microsoft Office macro settings	Microsoft Office macros are allowed to execute, but only after prompting users for approval. Microsoft Office macro security settings cannot be changed by users.	Only signed Microsoft Office macros are allowed to execute. Microsoft Office macros in documents originating from the internet are blocked. Microsoft Office macro security settings cannot be changed by users.	Microsoft Office macros are only allowed to execute in documents from Trusted Locations where write access is limited to personnel whose role is to vet and approve macros. Microsoft Office macros in documents originating from the internet are blocked. Microsoft Office macro security settings cannot be changed by users.
User application hardening	Web browsers are configured to block or disable support for Flash content.	Web browsers are configured to block or disable support for Flash content. Web browsers are configured to block web advertisements. Web browsers are configured to block Java from the internet.	Web browsers are configured to block or disable support for Flash content. Web browsers are configured to block web advertisements. Web browsers are configured to block Java from the internet. Microsoft Office is configured to disable support for Flash content. Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.
Restrict administrative privileges	Privileged access to systems, applications and information is validated when first requested. Policy security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.	Privileged access to systems, applications and data repositories is validated when first requested and revalidated on an annual or more frequent basis. Policy security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.	Privileged access to systems, applications and data repositories is validated when first requested and revalidated on an annual or more frequent basis. Privileged access to systems, applications and data repositories is limited to that required for personnel to undertake their duties. Technical security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.
Patch operating systems	Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within one month of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within two weeks of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. An automated mechanism is used to confirm and record that deployed operating system and firmware patches or updates have been installed, applied successfully and remain in place. Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.
Multi-factor authentication	Multi-factor authentication is used to authenticate all users of remote access solutions. Multi-factor authentication uses at least two of the following authentication factors: passwords, Universal 2nd Factor security keys, physical one-time password tokens, biometrics, smartcards, mobile app one-time password tokens, SMS messages, emails, voice calls or software certificates.	Multi-factor authentication is used to authenticate all users of remote access solutions. Multi-factor authentication is used to authenticate all privileged users and any other positions of trust. Multi-factor authentication uses at least two of the following authentication factors: passwords, Universal 2nd Factor security keys, physical one-time password tokens, biometrics, smartcards or mobile app one-time password tokens.	Multi-factor authentication is used to authenticate all users of remote access solutions. Multi-factor authentication is used to authenticate all privileged users and any other positions of trust. Multi-factor authentication is used to authenticate all users when accessing important data repositories. Multi-factor authentication uses at least two of the following authentication factors: passwords, Universal 2nd Factor security keys, physical one-time password tokens, biometrics or smartcards.
Daily backups	Backups of important information, software and configuration settings are performed monthly. Backups are stored for between one to three months. Partial restoration of backups is tested on an annual or more frequent basis.	Backups of important information, software and configuration settings are performed weekly. Backups are stored offline, or online but in a non-rewritable and non-erasable manner. Backups are stored for between one to three months. Full restoration of backups is tested at least once. Partial restoration of backups is tested on a bi-annual or more frequent basis.	Backups of important information, software and configuration settings are performed at least daily. Backups are stored offline, or online but in a non-rewritable and non-erasable manner. Backups are stored for three months or greater. Full restoration of backups is tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur. Partial restoration of backups is tested on a quarterly or more frequent basis.

# Compliance:

## Privacy Act 1988, Notifiable Data Breach Scheme, My Health Records Act 2012...

- APP 1 — Open and transparent management of personal information
- APP 2 — Anonymity and pseudonymity
- APP 3 — Collection of solicited personal information
- APP 4 — Dealing with unsolicited personal information
- APP 5 — Notification of the collection of personal information
- APP 6 — Use or disclosure of personal information
- APP 7 — Direct marketing
- APP 8 — Cross-border disclosure of personal information
- APP 9 — Adoption, use or disclosure of government related identifiers
- APP 10 — Quality of personal information
- ➔ **APP 11 — Security of personal information**
- APP 12 — Access to personal information
- APP 13 — Correction of personal information

Source: <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/>



# Compliance:

## Privacy Act 1988, Notifiable Data Breach Scheme, My Health Records Act 2012...

### APP 11 — Security of personal information

11.1 **APP 11 requires an APP entity to take active measures to ensure the security of personal information it holds**, and to actively consider whether it is permitted to retain personal information.

11.2 An APP entity that holds personal information must take **reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure** (APP 11.1).

11.3 An APP entity must take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for any purpose for which the personal information may be used or disclosed under the APPs. This requirement does not apply where the personal information is contained in a Commonwealth record or where the entity is required by law or a court/tribunal order to retain the personal information (APP 11.2).

Source: <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-11-app-11-security-of-personal-information>



## Privacy Act 1988, Notifiable Data Breach Scheme, My Health Records Act 2012...

### **“reasonable steps” explained by APP 11:**

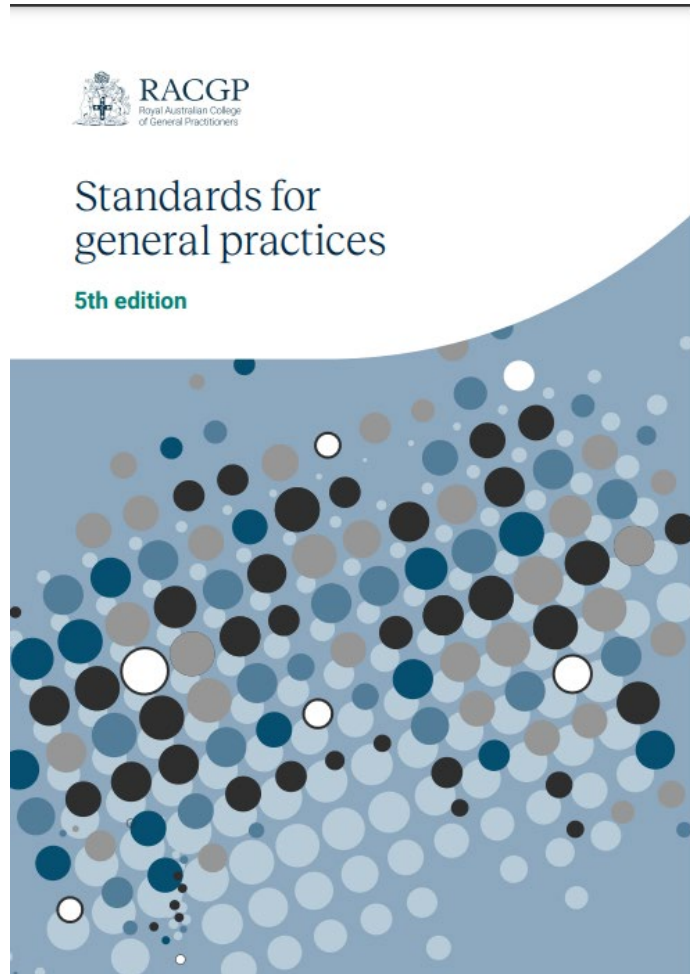
Source: <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-11-app-11-security-of-personal-information>

#### **APP 11.8 Reasonable steps should include, where relevant, taking steps and implementing strategies in relation to the following:**

- governance, culture and training
- internal practices, procedures and systems
- ICT security
- access security
- third party providers (including cloud computing)
- data breaches
- physical security
- destruction and de-identification
- standards.

*Also, see the OAIC's Guide to securing personal information:*

Source: <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information>



## Information management

Our practice has an effective system for managing patient information.

Information management refers to the management, storage and disposal of records (paper and electronic), and the technology used to do this. You are required to comply with the relevant state/territory and federal laws relating to the collection, storage, use, disclosure and disposal of patients' health and personal details.

### Indicators

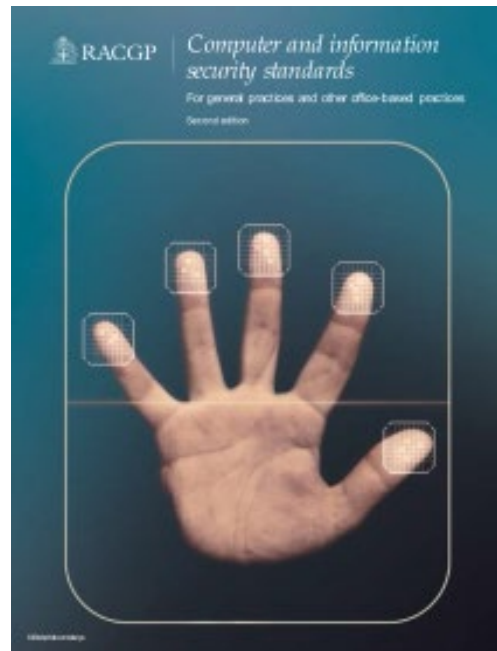
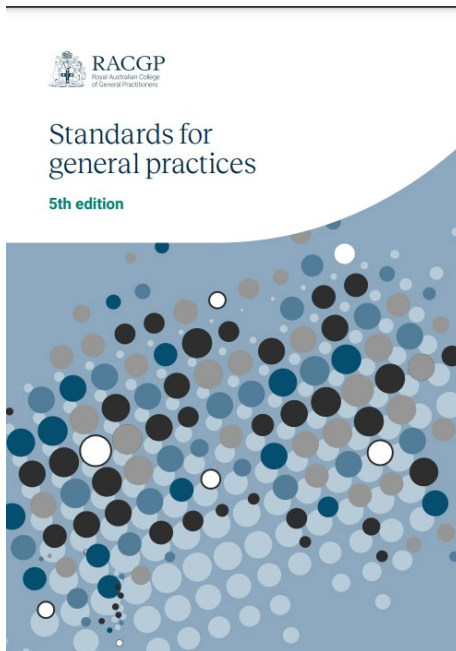
- C6.4 A** ▶ Our practice has a team member who has primary responsibility for the electronic systems and computer security.
- C6.4 B** ▶ Our practice does not store or temporarily leave the personal health information of patients where members of the public could see or access that information.
- C6.4 C** ▶ Our practice's clinical software is accessible only via unique individual identification that gives access to information according to the person's level of authorisation.
- C6.4 D** ▶ Our practice has a business continuity and information recovery plan.
- C6.4 E** ▶ Our practice has appropriate procedures for the storage, retention, and destruction of records.
- C6.4 F** ▶ Our practice has a policy about the use of email.
- C6.4 G** ▶ Our practice has a policy about the use of social media.

Source: <https://www.racgp.org.au/running-a-practice/practice-standards/standards-5th-edition/standards-for-general-practices-5th-ed/core-standards/core-standard-6/criterion-c6-4-information-security>

## RACGP Standards 5th Edition & CISS 2ND Edition :

### *Criterion C6.4 D*

*Our practice has a business continuity and information recovery plan.*



### **Business continuity and information recovery**

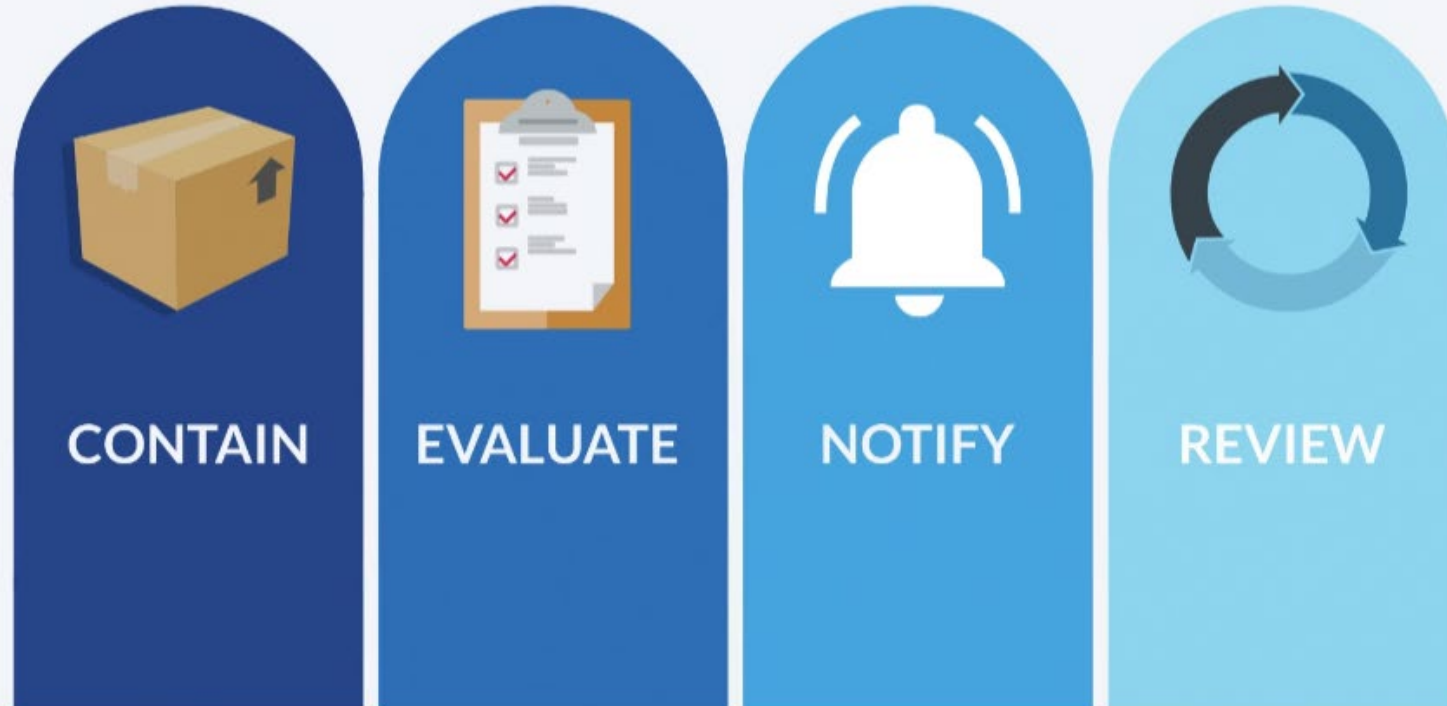
**If your practice uses computers to store patient health information, you must have a business continuity plan to protect information in the event of an adverse incident, such as a system crash or power failure.**

### **The business continuity and information recovery plan needs to include:**

- the processes by which all critical information relating to the practice's operations (such as appointments, billing and patient health information) will be frequently backed up
- a schedule of regular tests so that backups are being correctly created and can be accessed and read as expected
- details of the secure offsite location where the backup information is stored
- standard letters of agreement that external IT providers sign to indicate their commitment to comply with the requirements of the CISS.

Source: <https://www.racgp.org.au/running-a-practice/practice-standards/standards-5th-edition/standards-for-general-practices-5th-ed/core-standards/core-standard-6/criterion-c6-4-information-security>

## Responding to an incident



Source: Australian Digital Health Agency (ADHA)'s online learning module: <https://training.digitalhealth.gov.au>

# Compliance for healthcare clinics:

# Incident Response

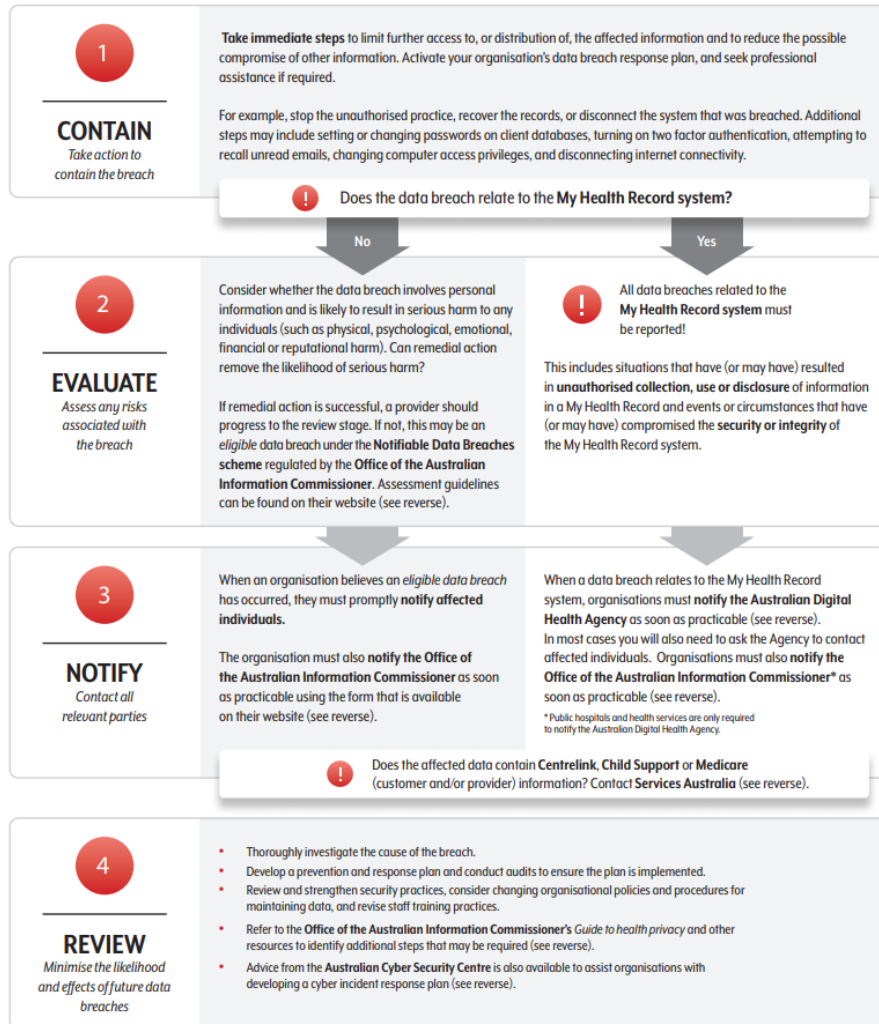


Australian Government

## DATA BREACH ACTION PLAN

### FOR HEALTH SERVICE PROVIDERS

A data breach occurs when information held by an organisation is compromised or lost, or is accessed or disclosed without authorisation. For example, unauthorised access to health records, or lost client data.



Source: <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/health-service-providers/data-breach-action-plan-for-health-service-providers>



## CONTACT INFORMATION

### Office of the Australian Information Commissioner (OAIC)

The OAIC oversees the Notifiable Data Breaches scheme and privacy aspects of the My Health Record system. For more information on notifiable data breaches:

Web: [oaic.gov.au/data-breach-preparation-and-response](http://oaic.gov.au/data-breach-preparation-and-response)

Assessing an eligible data breach  
Web: [oaic.gov.au/data-breach-response-steps](http://oaic.gov.au/data-breach-response-steps)

Report a notifiable data breach  
Web: [oaic.gov.au/report-a-data-breach](http://oaic.gov.au/report-a-data-breach)

Report a My Health Record data breach  
Web: [oaic.gov.au/my-health-record-data-breach](http://oaic.gov.au/my-health-record-data-breach)

Guide to health privacy  
Web: [oaic.gov.au/guide-to-health-privacy](http://oaic.gov.au/guide-to-health-privacy)

Enquiries  
Web: [oaic.gov.au/contact-us](http://oaic.gov.au/contact-us)  
Phone: 1300 363 992

### Services Australia (Medicare)

You may wish to contact Services Australia to discuss options for protecting customers' Medicare, Centrelink or Child Support records. If there is a risk of compromise to these records, Services Australia may place additional security measures on records.

As a provider you may email us for assistance and support on protecting your customers' Medicare information and your provider credentials used for Medicare. Please note, this mailbox is for providers only.  
Email: [protectyouridentity@servicesaustralia.gov.au](mailto:protectyouridentity@servicesaustralia.gov.au)

Impacted customers can discuss these options by contacting Services Australia's Scams and Identity Theft Helpdesk between 8:00am-5:00pm Australian Eastern Time, Monday to Friday.  
Phone: 1800 941 126

### Australian Digital Health Agency (My Health Record system)

All data breaches related to the My Health Record system must be reported to the Australian Digital Health Agency. The Agency will contact affected healthcare recipients, when this is required under the *My Health Records Act 2012*. Where a significant number of people are affected, the general public will be notified.

Web: [myhealthrecord.gov.au/for-healthcare-professionals/how-to/manage-data-breach](http://myhealthrecord.gov.au/for-healthcare-professionals/how-to/manage-data-breach)

Email: [MyHealthRecord.Compliance@digitalhealth.gov.au](mailto:MyHealthRecord.Compliance@digitalhealth.gov.au)

Phone: 1800 723 471

### Australian Cyber Security Centre (ACSC)

The ACSC leads the Australian Government's efforts to improve cyber security, with the role of helping to make Australia the safest place to connect online. For advice on what to consider in developing an incident response plan:

Web: [cyber.gov.au/advice/developing-an-incident-response-plan](http://cyber.gov.au/advice/developing-an-incident-response-plan)

Report a cyber security incident  
Web: [cyber.gov.au/report](http://cyber.gov.au/report)

Alert service: Sign up to the ACSC's Stay Smart Online free alert service on the latest online threats and how to respond at [staysmartonline.gov.au](http://staysmartonline.gov.au)

You can also seek support from Australia's national identity and cyber support service, **IDCARE** by calling **1300 432 273**

**Thank you for your time.**

**Questions?**

**Tony Nicholson**, B App Sc (Computing), Director, Mint IT Solutions

**Miroslav Doncevic** M CyberSec, Grad Cert Cyber Sec, Cert NIST CSF Practitioner



**Ph: 02 4731 4533**