

 **HotDoc** | CPD WEBINAR


Cybersecurity 101: Change Your Culture, Not Your Budget



HOSTED BY
Henry McLaughlin



Wed 15 Feb
12:30pm AEDT



In the spirit of reconciliation, HotDoc acknowledges the Traditional Custodians of country throughout Australia and their connections to land, sea and community.

We pay our respect to their elders past and present and extend that respect to all Aboriginal and Torres Strait Islander peoples today.



Healthcare ICT Specialists



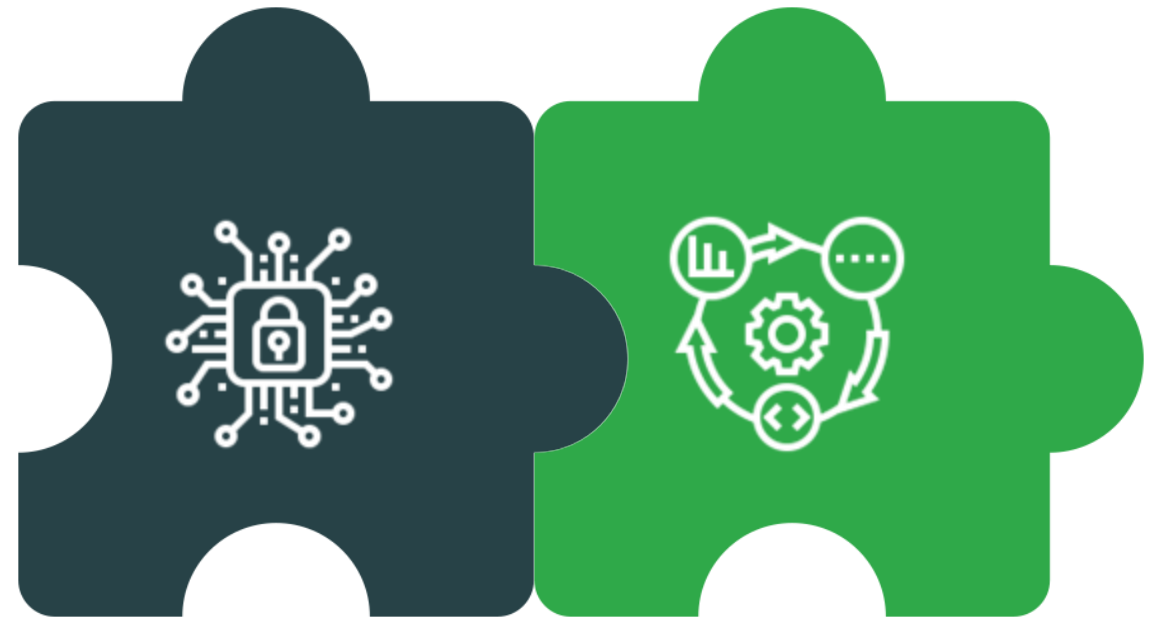
www.greenumbrella.com.au

Improving Technology in General Practice

2023 Cybersecurity Education



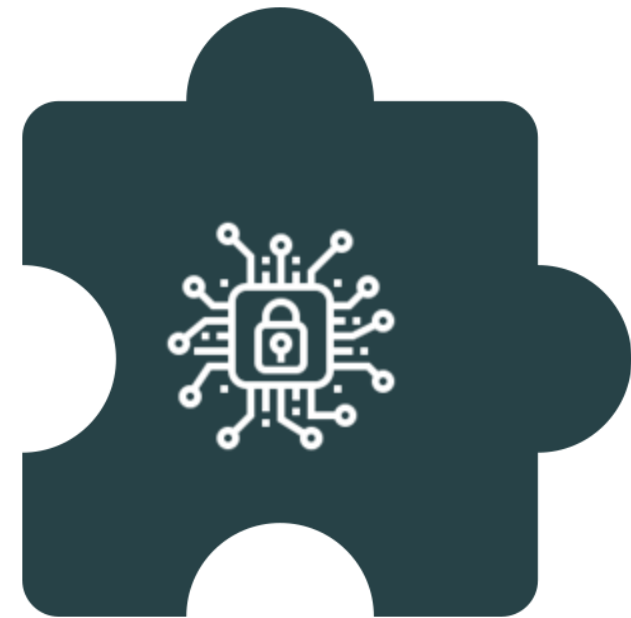
- Cyber security hardens against cyber attacks
- Business continuity and disaster recovery maximises capacity to recover from cyber attacks.



Cyber Security

Business Continuity
Disaster Recovery

Cyber Security, In General Practice



Cyber Security

Cyber Security **Defined**



- Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.
- Cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

Legislation: Notifiable Data Breaches



[Home](#) ▶ [Privacy law](#) ▶ [The Privacy Act](#) ▶



Notifiable Data Breaches scheme

On this page

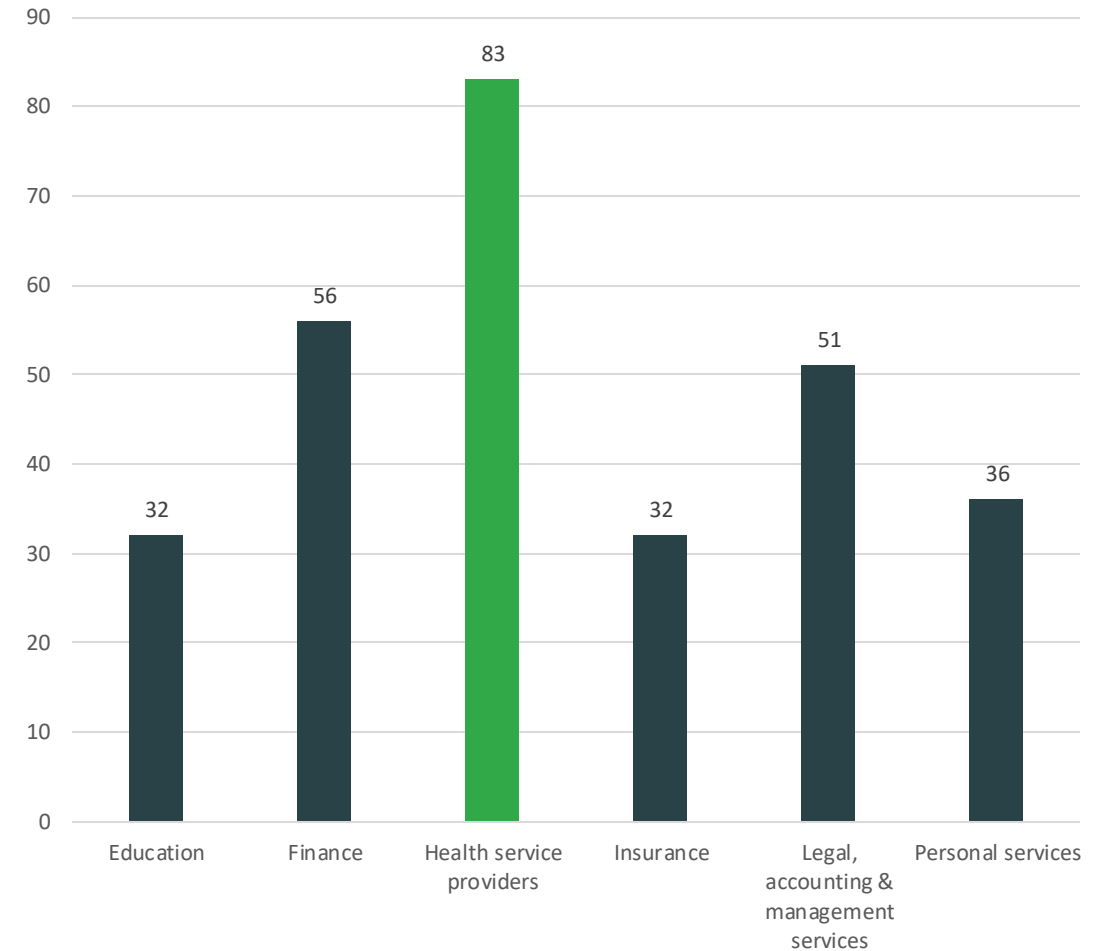
- [Overview](#)
- [Who must comply with the NDB scheme](#)
- [Which data breaches require notification](#)
- [Assessing suspected data breaches](#)
- [How to notify](#)
- [The role of the OAIC](#)
- [Data breach response summary diagram](#)
- [Additional resources](#)
- [Quarterly statistics](#)

Feb 2018

Privacy Amendment (Notifiable Data Breaches) Act 2017

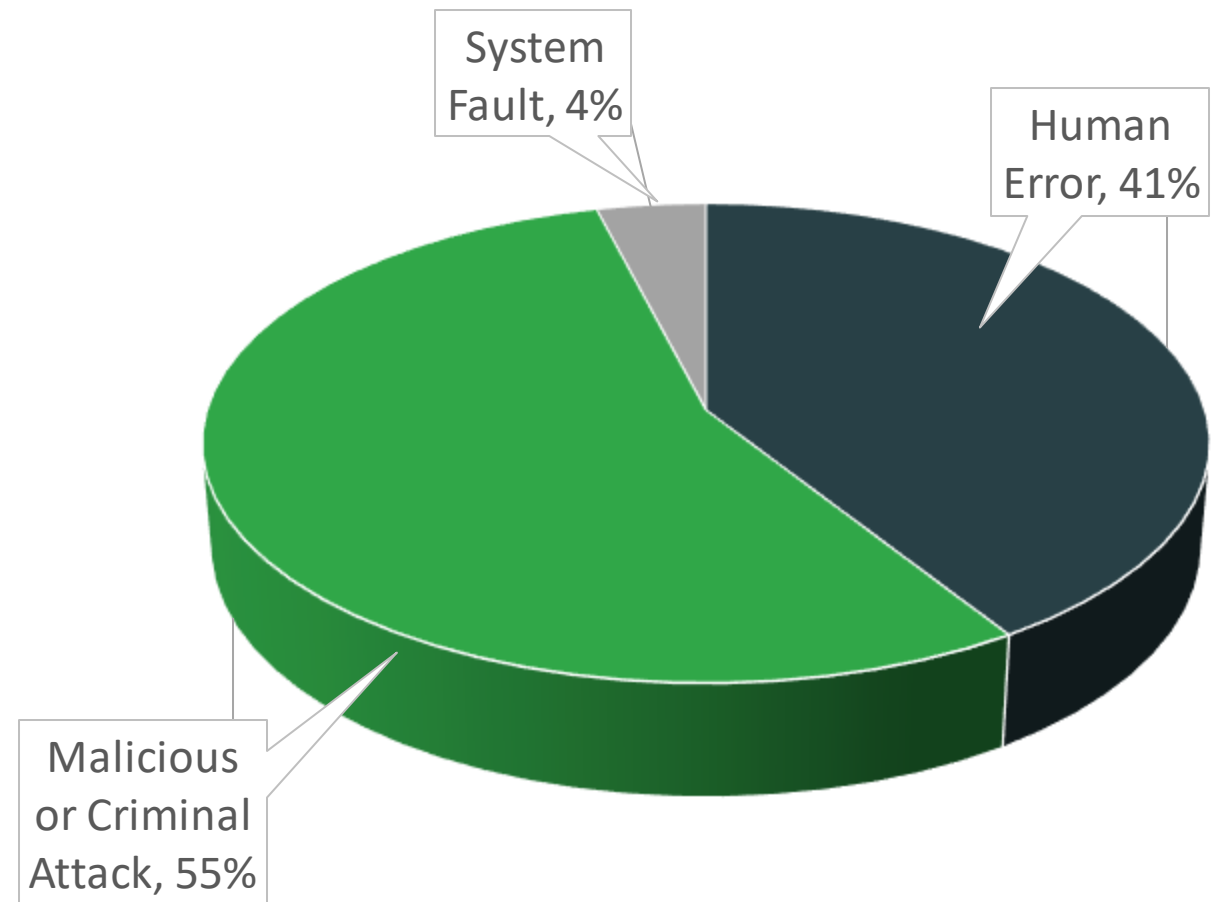
Source Of Breaches

Top Five Sectors



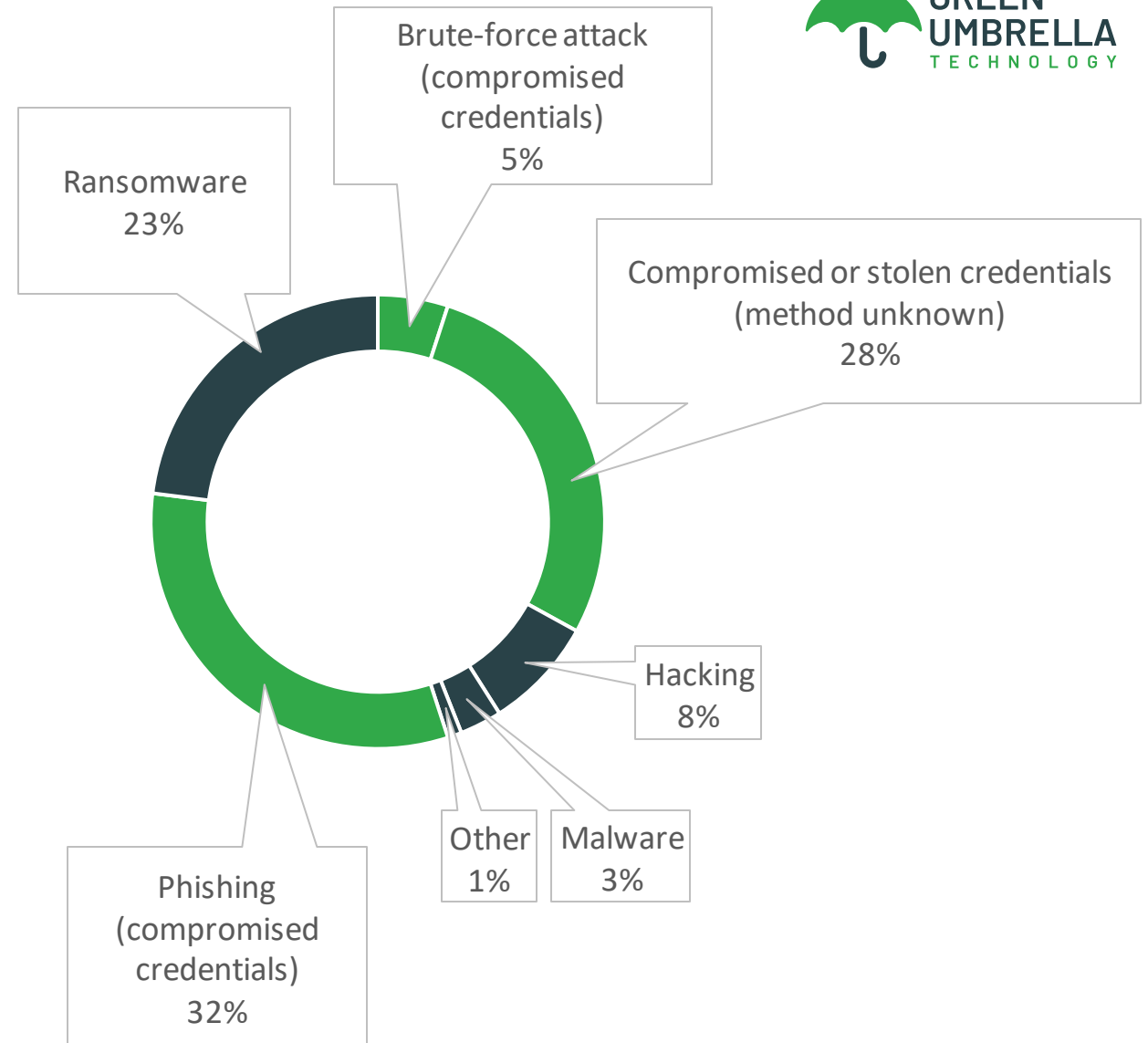
Source Of Breaches

All Sectors



Cyber Incident Breaches

All Sectors



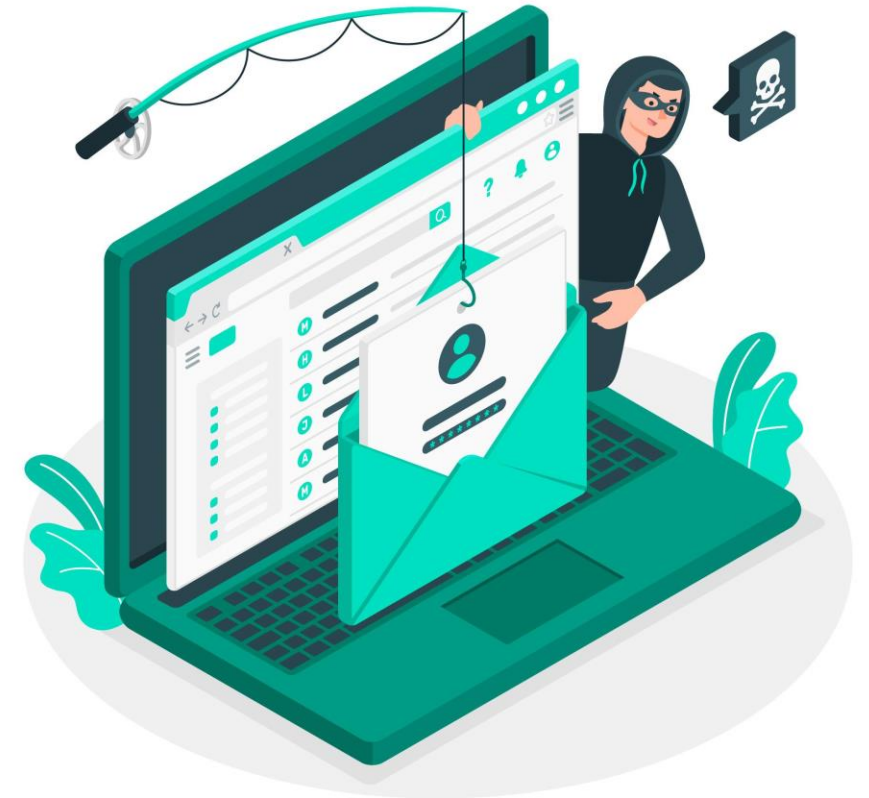
Primary Cyber Incident Compromised Credentials

Collectively equate to 65%

- Phishing attacks @ 32%
- Brute force attacks @ 5%
- Compromised or stolen @ 28%

Mitigated Via

- Web filtering
- Email filtering
- Strong password policies
- Two factor authentication



Phishing Explained

#1



Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.

AKA spot the difference

Brute Force Explained

In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly.

The attacker systematically checks all possible passwords and passphrases until the correct one is found.

#4



25 Most Common Passwords

123456

1234567

666666

!@\$%^&*

password

qwerty

abc123

charlie

123456789

iloveyou

football

aa123456

12345678

princess

123123

donald

12345

admin

monkey

password1

11111

welcome

654321

qwerty123

Password Management



- Users required to juggle multiple passwords for multiple systems
- Never use the same password for multiple systems
- Passwords need to be complex yet manageable
- Passwords should expire and be changed periodically (limited life)
- Develop & adopt a company password policy
- Use a Password Manager

USE A PASSWORD MANAGER

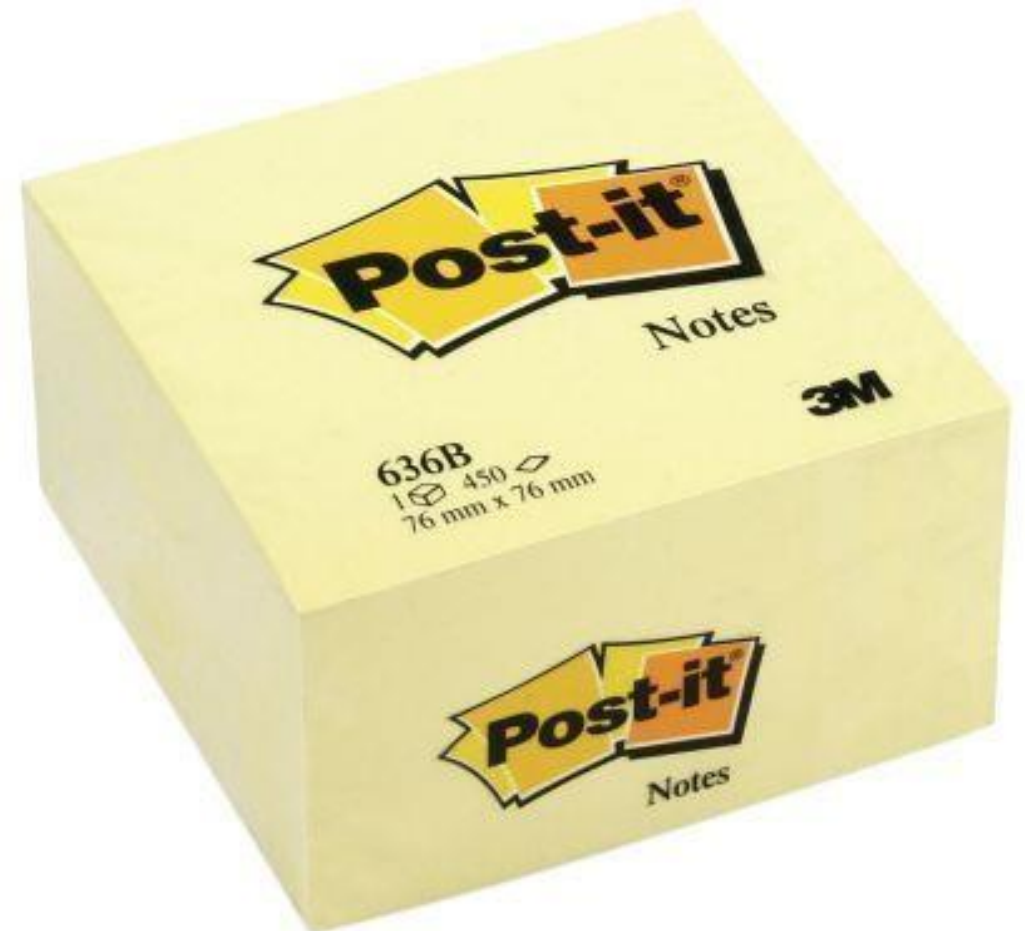
Password Complexity

- Uppercase
- Lower case
- Special Characters
- Numeric digits

h=RqdWudxUN2FnF]

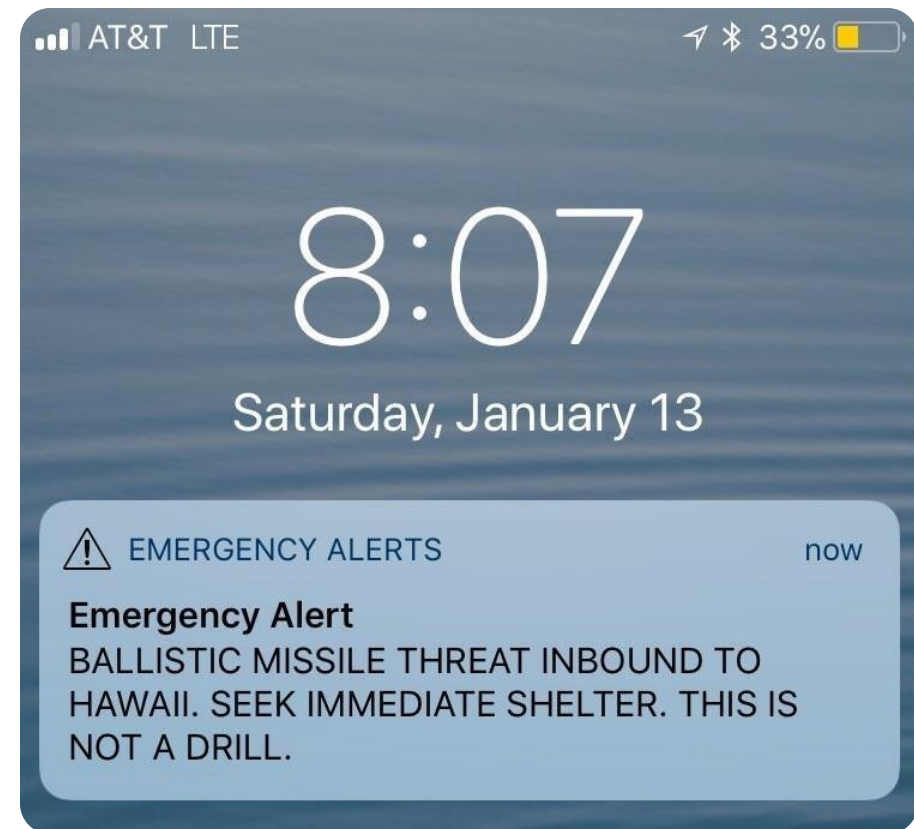


Hidden Cyber Security Risk

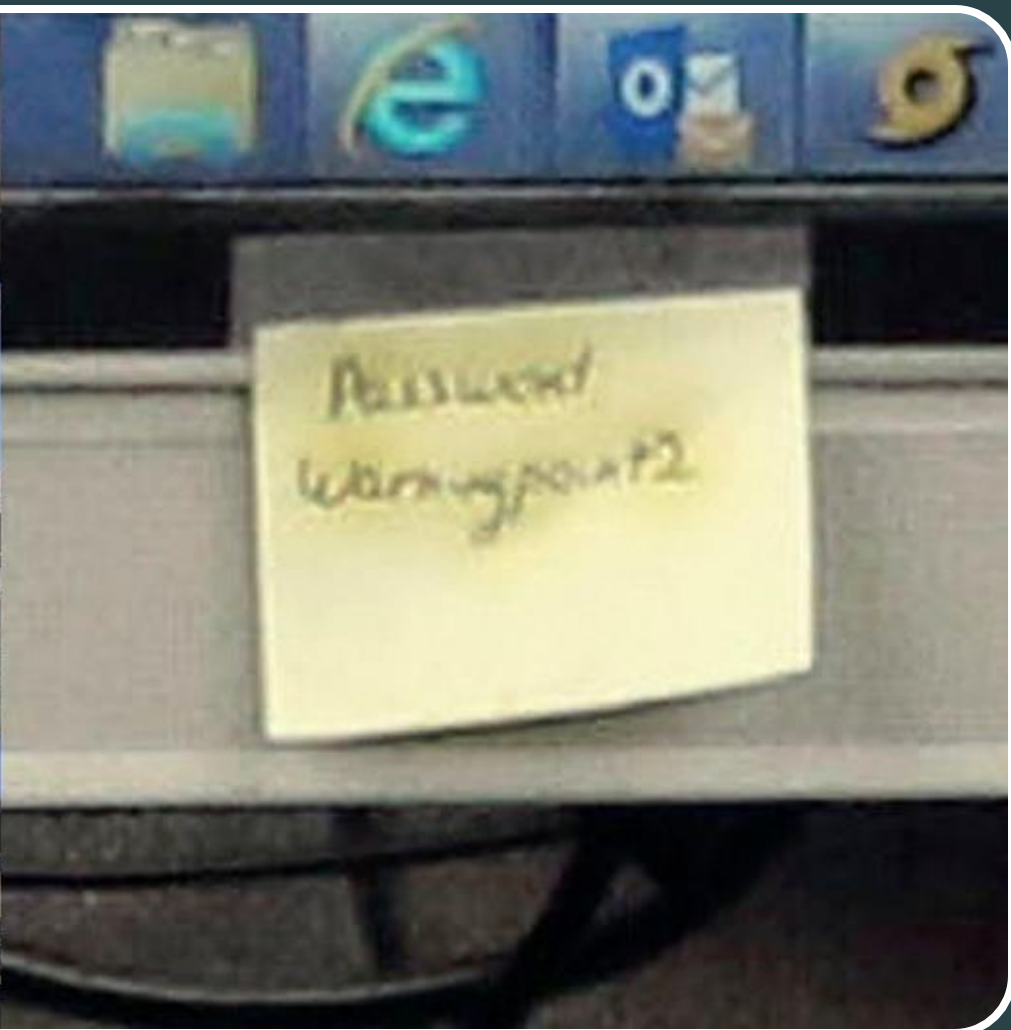


2018

Hawaii False Missile Alert







Have You Been Breached?



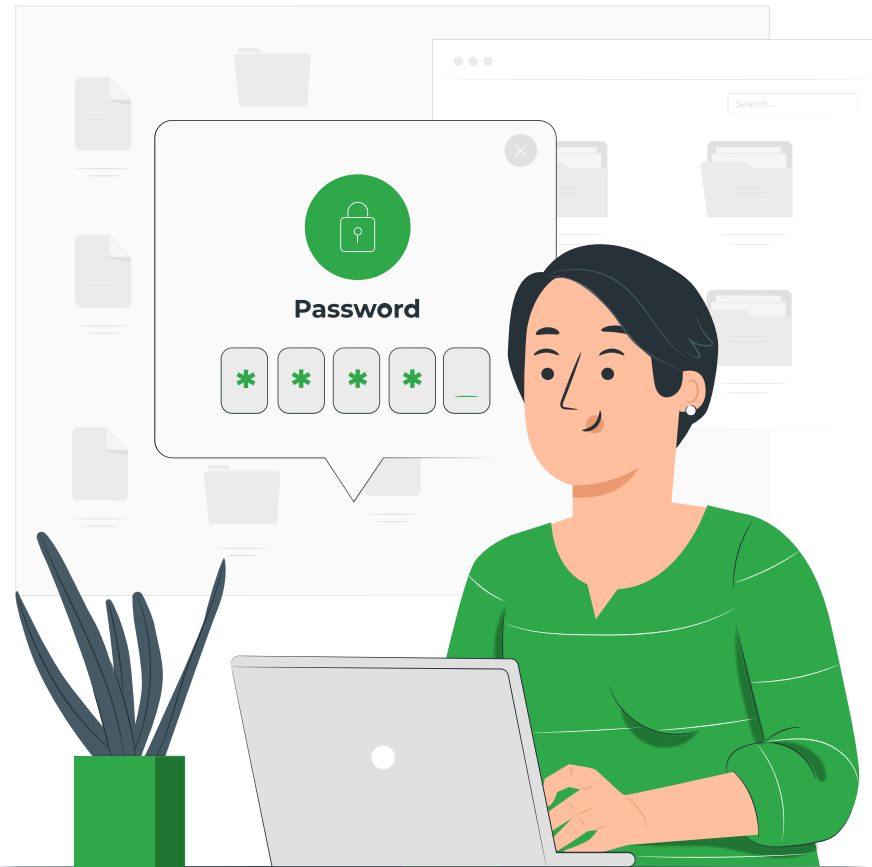
“How far prepared are you? It’s no longer a case of if a threat happens but when. It may have happened already, you may have not found it yet.”

- IBM Australia Industry Security Leader Stephen Burmester



<https://haveibeenpwned.com>

Password Managers



- Password management is easy with the right tools
- Multiple password managers available:
- Green Umbrella Technology uses MyGlue internally.

LastPass...

 KEEPER

1Password

 Sticky
Password

 DASHLANE

 PASSWORD
BOSS

 RoboForm
FOR BUSINESS

 NordPass

#3

Cyber Incident Ransomware

- Across Australia & New Zealand , an estimated 6% of small-medium businesses fell victim to ransomware in 2016-2017
- The total amount of ransom paid from these attacks...

\$12.6 million

Ransomware Explained



Ransomware is a type of malicious software from crypto-virology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid

Mitigated Via

- Web filtering
- Email filtering
- Application whitelisting
- BCDR

```
uu$:$:$:$:$uu
uu$$$$$$$$$$$$$$$$uu
u$$$$$$$$$$$$$$$$uu
u$$$$$$$$$$$$$$$$uu
u$$$$$$$$$$$$$$$$uu
u$$$$$$$$*   *$$$*   *$$$$$u
*$$$$$*       u$u       $$$*$
$$$u          u$u          u$$$
$$$u          u$$$$u       u$$$
*$$$$u$$$$$   $$$uu$$$$$*
*$$$$$$$*     *$$$$$$$*
u$$$$$$$$u$$$$$$$u
u*$*$*$*$*$*$u
uuu          $$u$ $ $ $ $u$$          uuu
u$$$$$      $$u$u$u$u$u$$$          u$$$$$
$$$$$uu     *$$$$$$$$$*           uu$$$$$$
u$$$$$$$$$   ****          uuu$$$$$$$$$
$$$$$**$$$$$$$$$uuu   uu$$$$$$$$$**$$$$$*
**          **$$$$$$$$$u   **$***
uuuu **$$$$$$$$$u
u$$$uu$$$$$$$$$u   **$$$$$$$$$uu$$$$$
$$$$$$$$$***          **$$$$$$$$$$$*
*$$$$$*                *$$$$$**
$$$*          PRESS ANY KEY!          $$$*
```

Blacklisting Vs Whitelisting



“There are applications we know are safe. There are applications we know are not safe. But there are also applications we don’t know are not safe”

- Henry McLaughlin

	Blacklisting	Whitelisting
Know are safe	Permitted	Permitted
Know are not safe	Blocked	Blocked
Don't know are not safe	Permitted	Blocked

Business Continuity and Disaster Recovery In General Practice



Business Continuity
Disaster Recovery

Continuity Terminology





Thank You!



hello@greenumbrella.com.au

JOIN THE CONVERSATION



Our community has over 4,600 healthcare professionals to share ideas, discuss hot topics and collaborate with.

Join here <https://www.facebook.com/groups/fortheloveofhealthcare>