Disaster Preparedness – Cybersecurity & Data Security

Peter Mullen – Digital Health Officer

CYBERSECURITY & DATA SECURITY

Background

In 2022 Hunter New England and Central Coast PHN commissioned Semantic Consulting to conduct the Health-e Together Digital Care Survey for general practice and in 2023 also The PHN also commissioned a similar survey for allied health practices which is currently in the reporting phase.

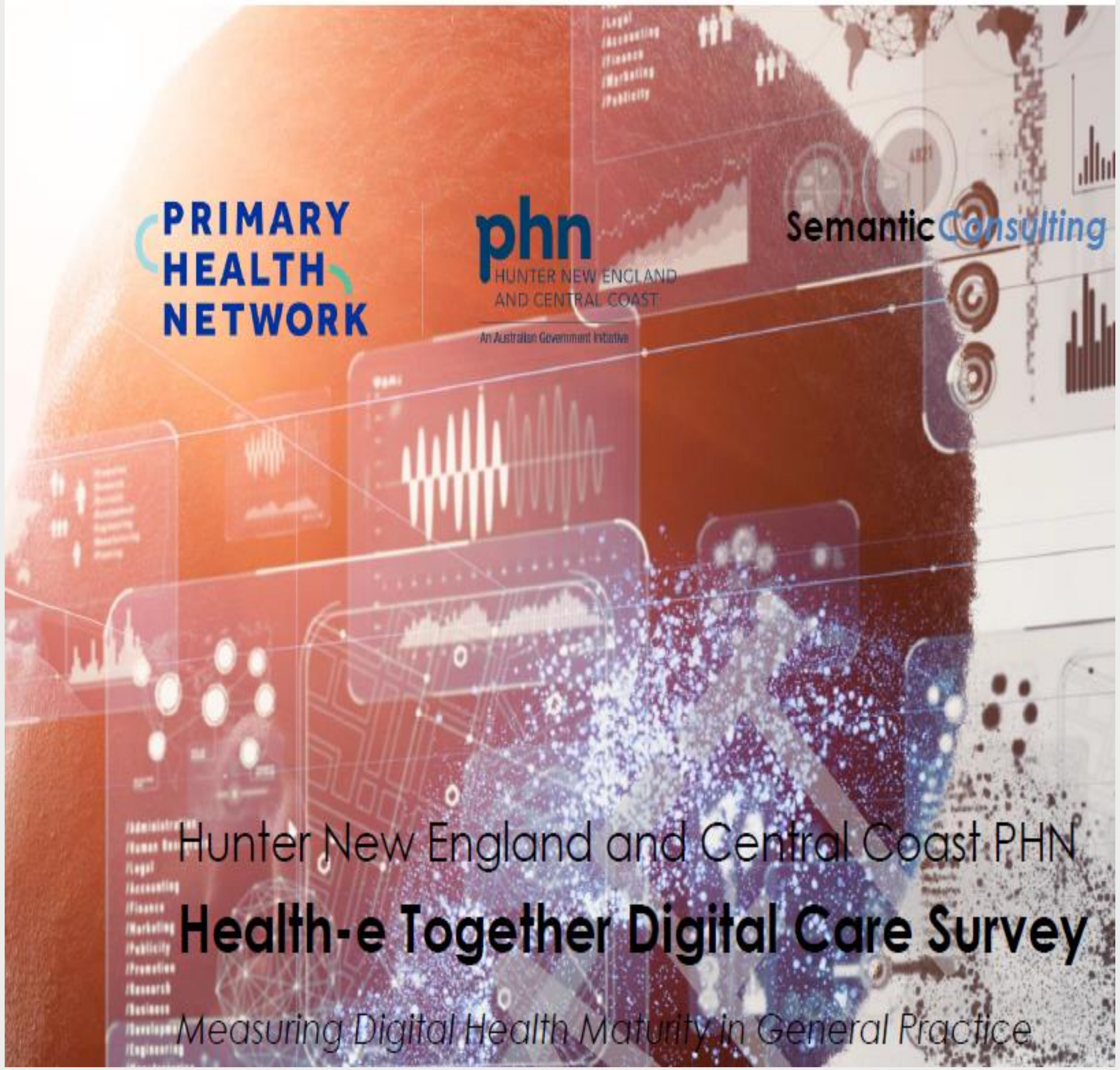
What was the General Practice Health-e Together Digital Care Survey?

- Online survey consisting of 40 customised, targeted questions, including free text response options.

Why did we run the surveys?

Who participated in the general practice survey?

- 211 of 382 practices across The PHN footprint.
- 206 provided responses.
- The survey was typically completed by practice managers or practice owner/doctors.



PRIMARY HEALTH NETWORK

phn HUNTER NEW ENGLAND AND CENTRAL COAST

An Australian Government Initiative

Semantic Consulting

Hunter New England and Central Coast PHN

Health-e Together Digital Care Survey

Measuring Digital Health Maturity in General Practice

THE PHN HEALTH-E TOGETHER DIGITAL CARE SURVEY FOR GENERAL PRACTICE RESULTS OVERVIEW

Background

In regard to cybersecurity the final report noted:

‘Critical work is required on cybersecurity and disaster recovery – Knowledge and practice about cybersecurity and disaster recovery continues to be problematic and requires specific attention to address critical vulnerabilities.”

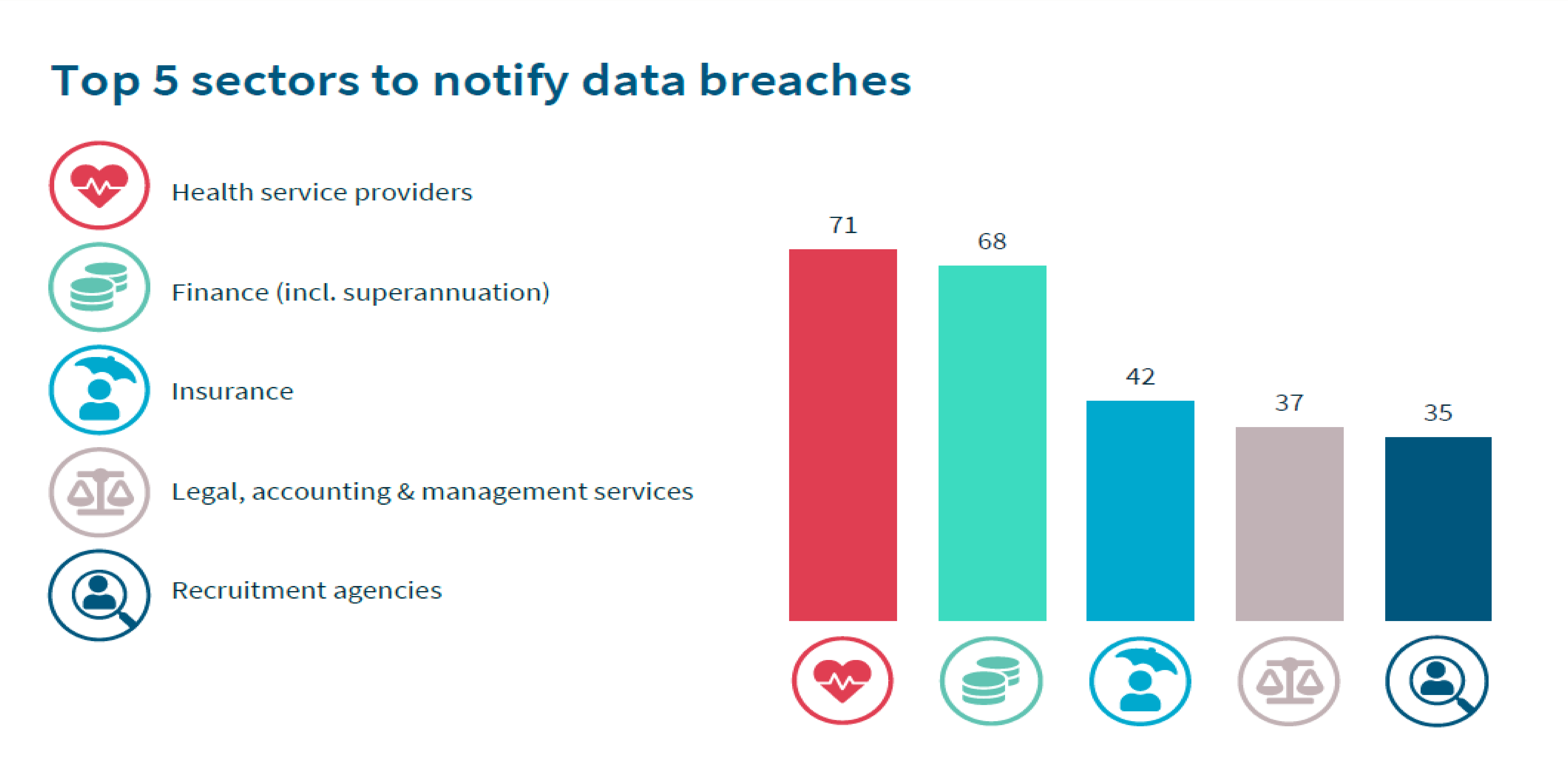
Credit: metamorworks via Shutterstock

CYBERSECURITY & DATA SECURITY

Data Security – Is your data secure?

Who is the threat and why health industry data?

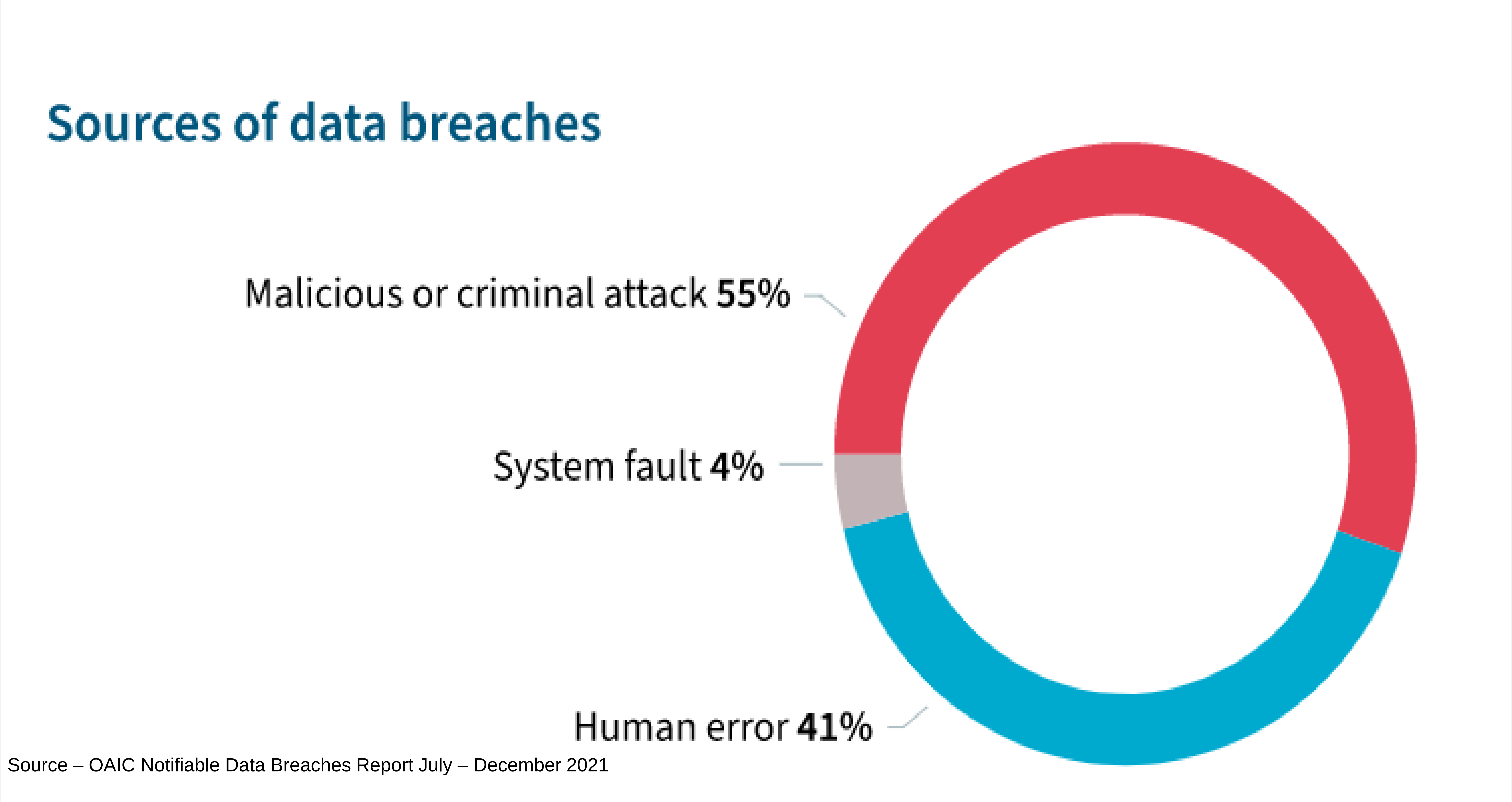
Image Source Ozrimoz/Shutterstock



Top 5 sectors to notify data breaches

Source – OAIC Notifiable Data Breaches Report July – December 2022

CYBERSECURITY & DATA SECURITY

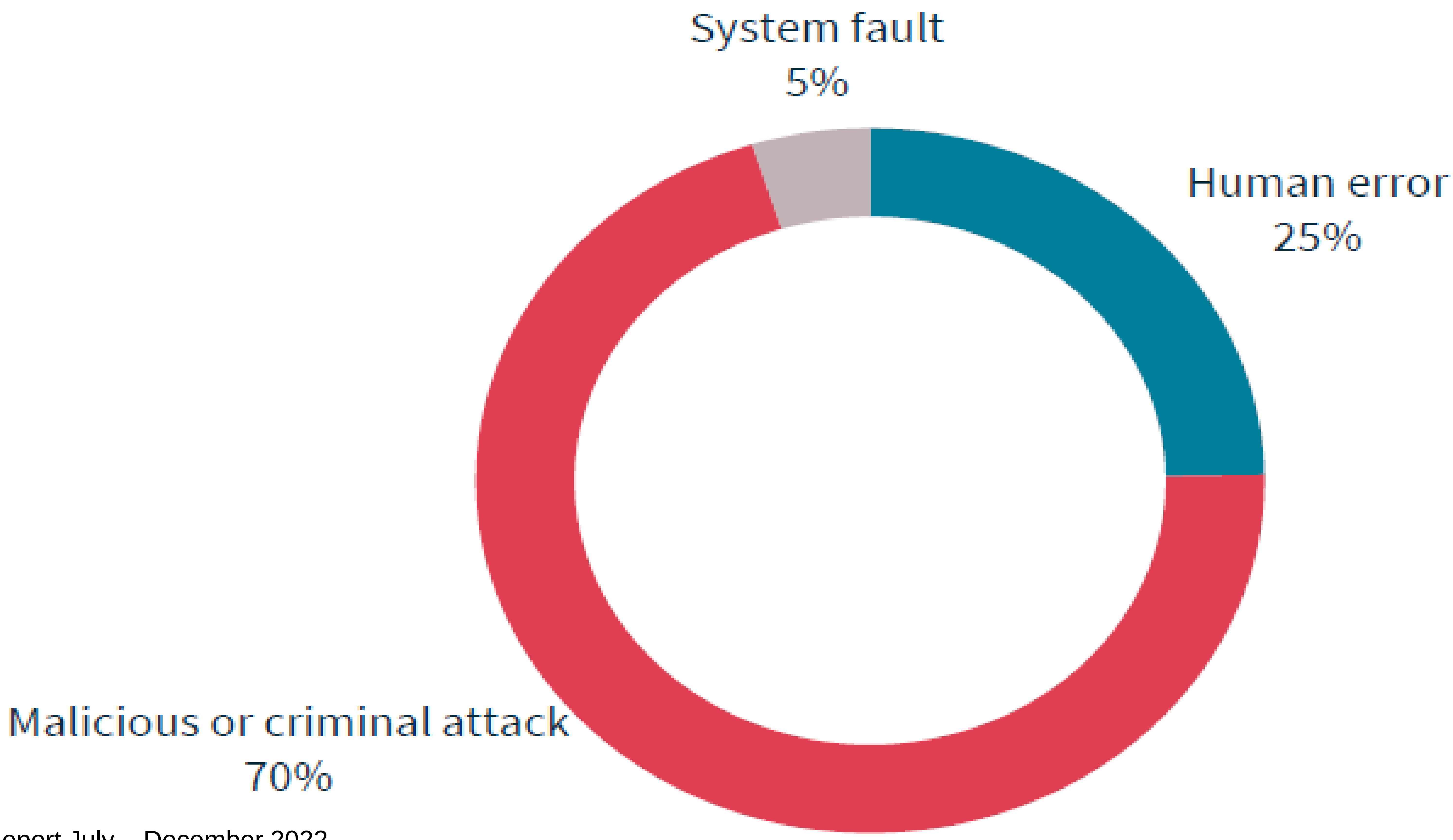


Sources of data breaches

Source – OAIC Notifiable Data Breaches Report July – December 2021

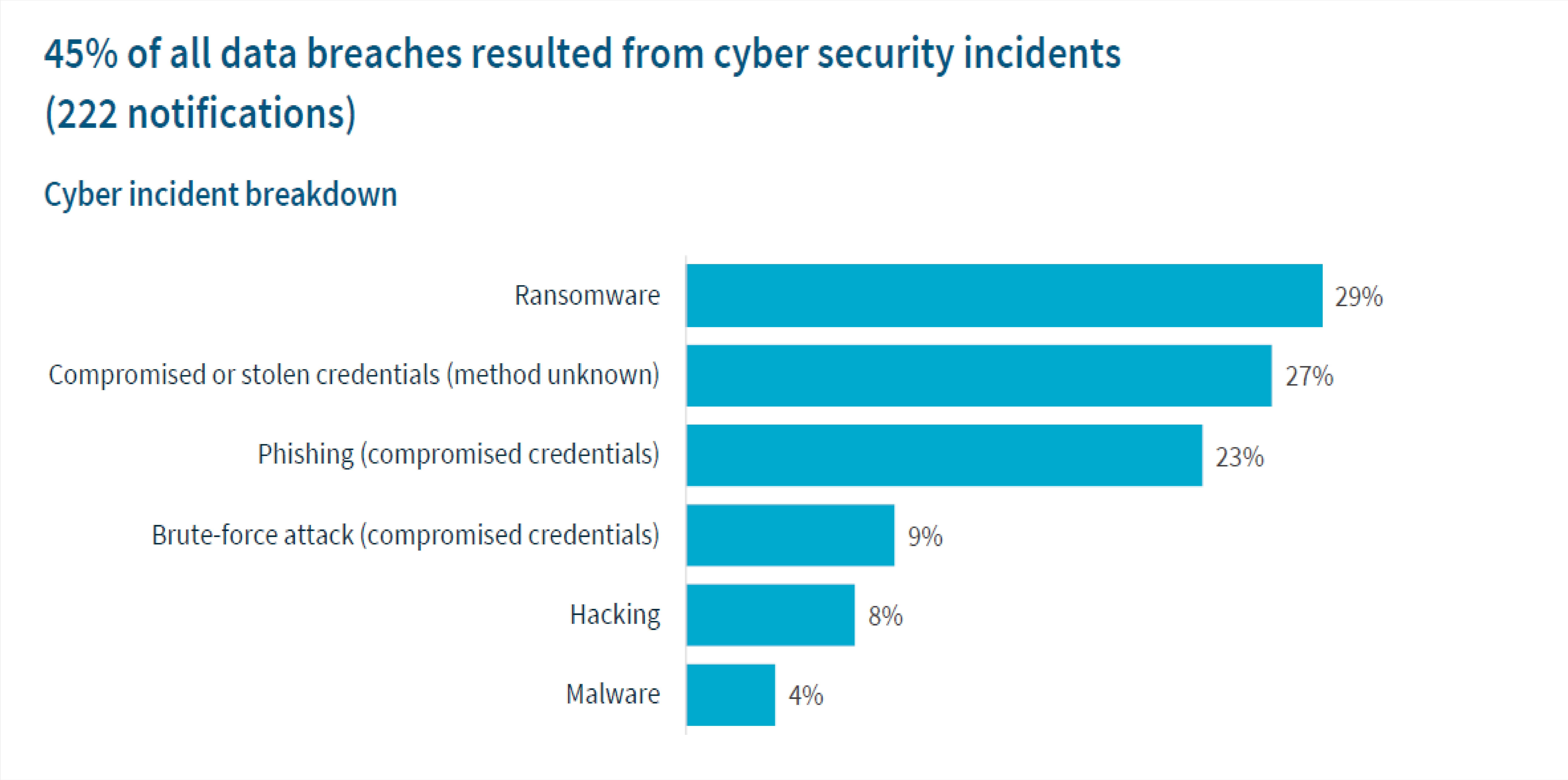
CYBERSECURITY & DATA SECURITY

Sources of data breaches



Source – OAIC Notifiable Data Breaches Report July – December 2022

CYBERSECURITY & DATA SECURITY



45% of all data breaches resulted from cyber security incidents (222 notifications)

Cyber incident breakdown

Source – OAIC Notifiable Data Breaches Report July – December 2022

CYBERSECURITY & DATA SECURITY

Data Security – Is your data secure?

Common cyber threats

#1 Compromised Credential Attacks

- Phishing
- Malware
- Brute Force Attack
- Compromised or stolen credentials

Mitigated by

- Web filtering
- Email filtering
- Strong password policies
- Multi factor authentication
- Business continuity and disaster recovery plan

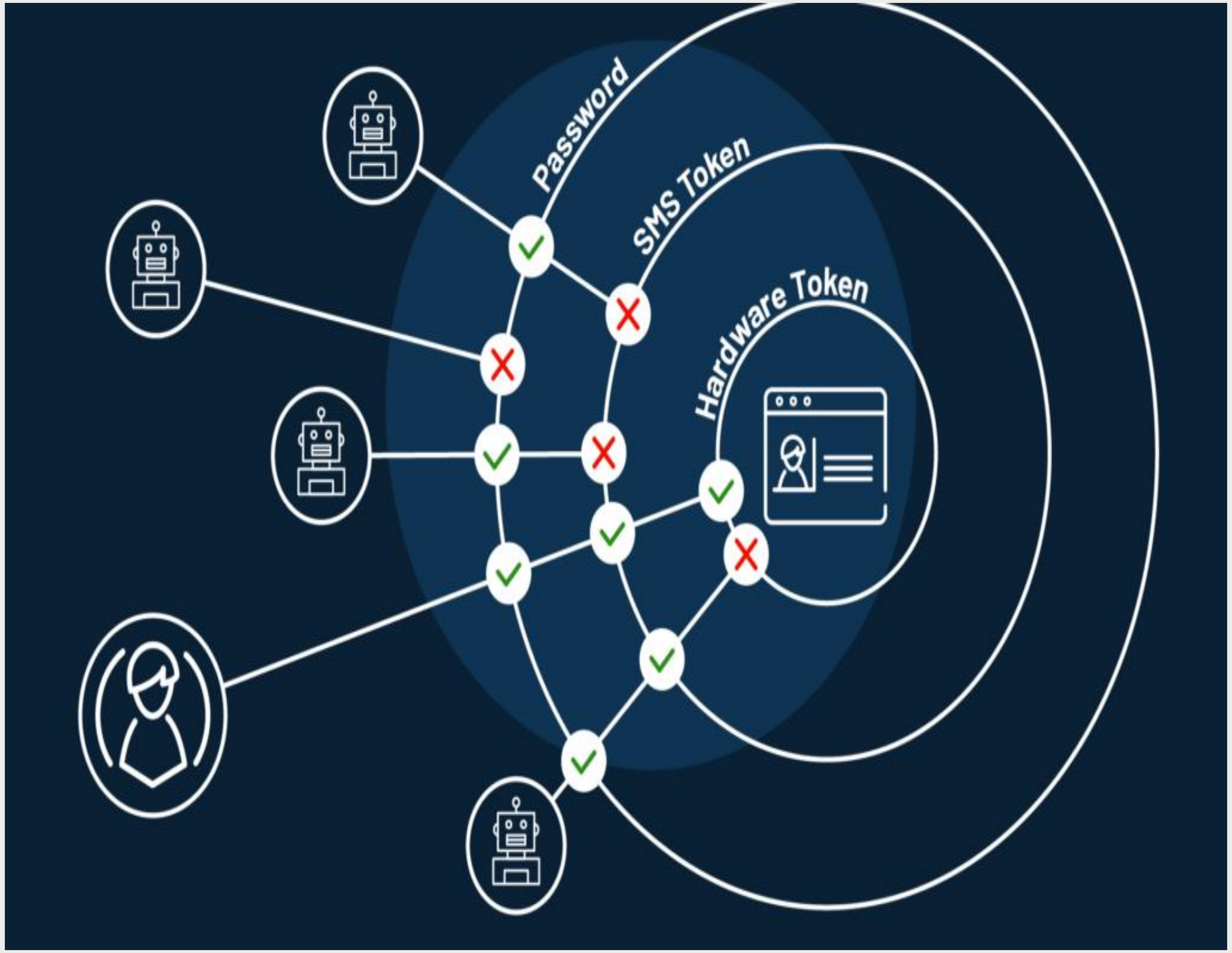
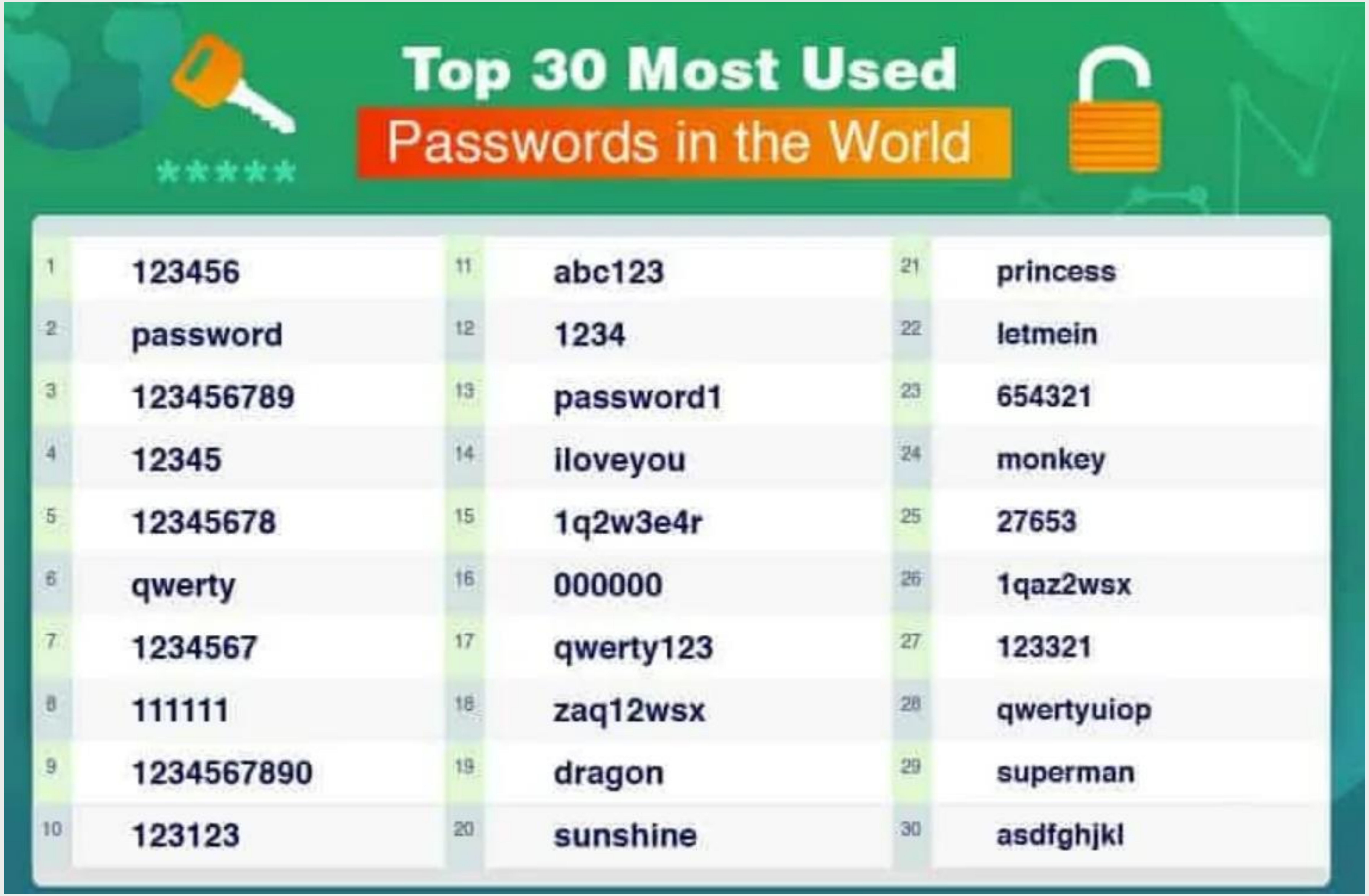


Image Source OwnZap Infsec

CYBERSECURITY & DATA SECURITY

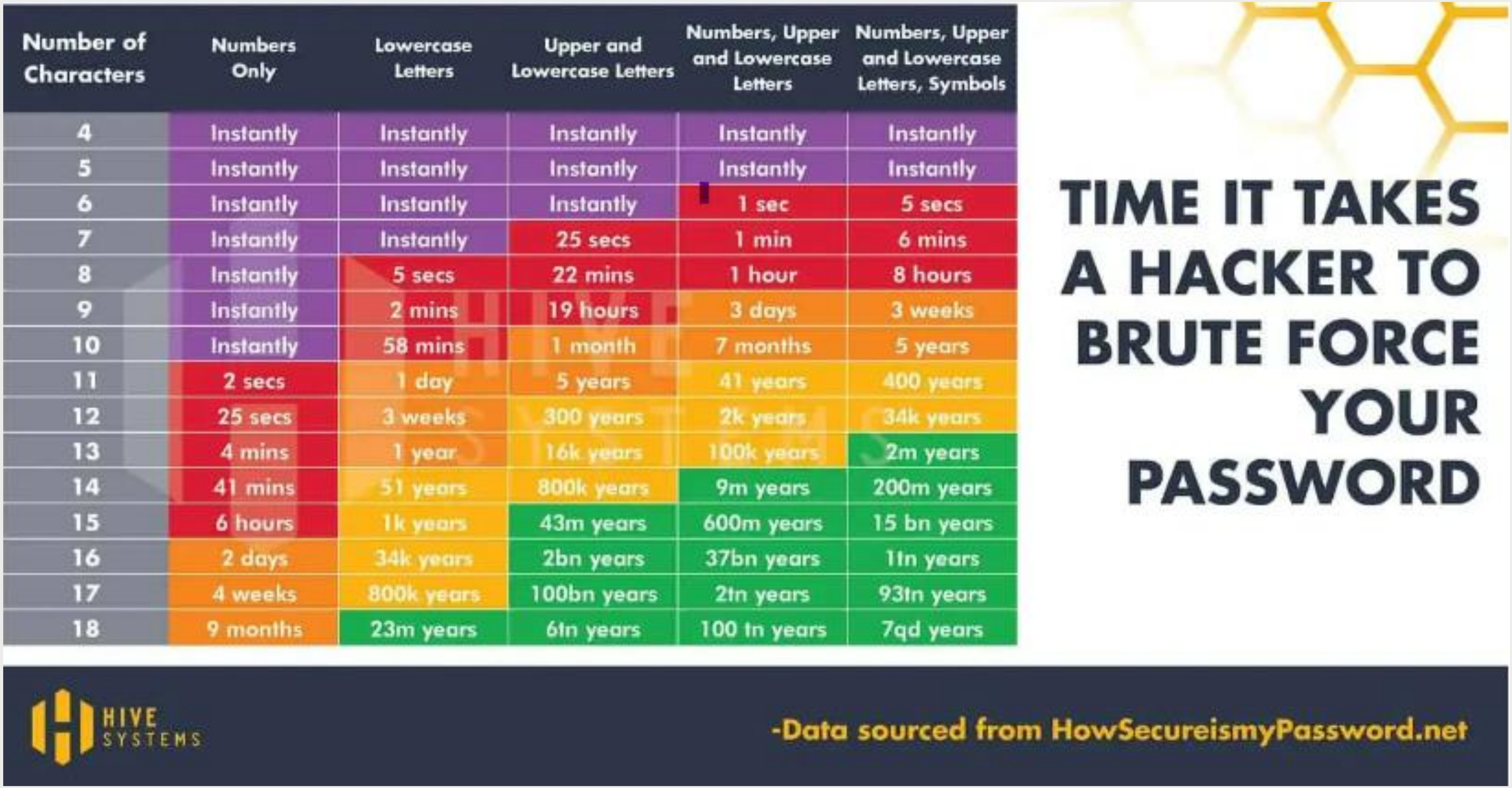


Top 30 Most Used Passwords in the World

1	123456	11	abc123	21	princess
2	password	12	1234	22	letmein
3	123456789	13	password1	23	654321
4	12345	14	iloveyou	24	monkey
5	12345678	15	1q2w3e4r	25	27653
6	qwerty	16	000000	26	1qaz2wsx
7	1234567	17	qwerty123	27	123321
8	111111	18	zaq12wsx	28	qwertyuiop
9	1234567890	19	dragon	29	superman
10	123123	20	sunshine	30	asdfghjkl

Source – safetydetectives.com

CYBERSECURITY & DATA SECURITY



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

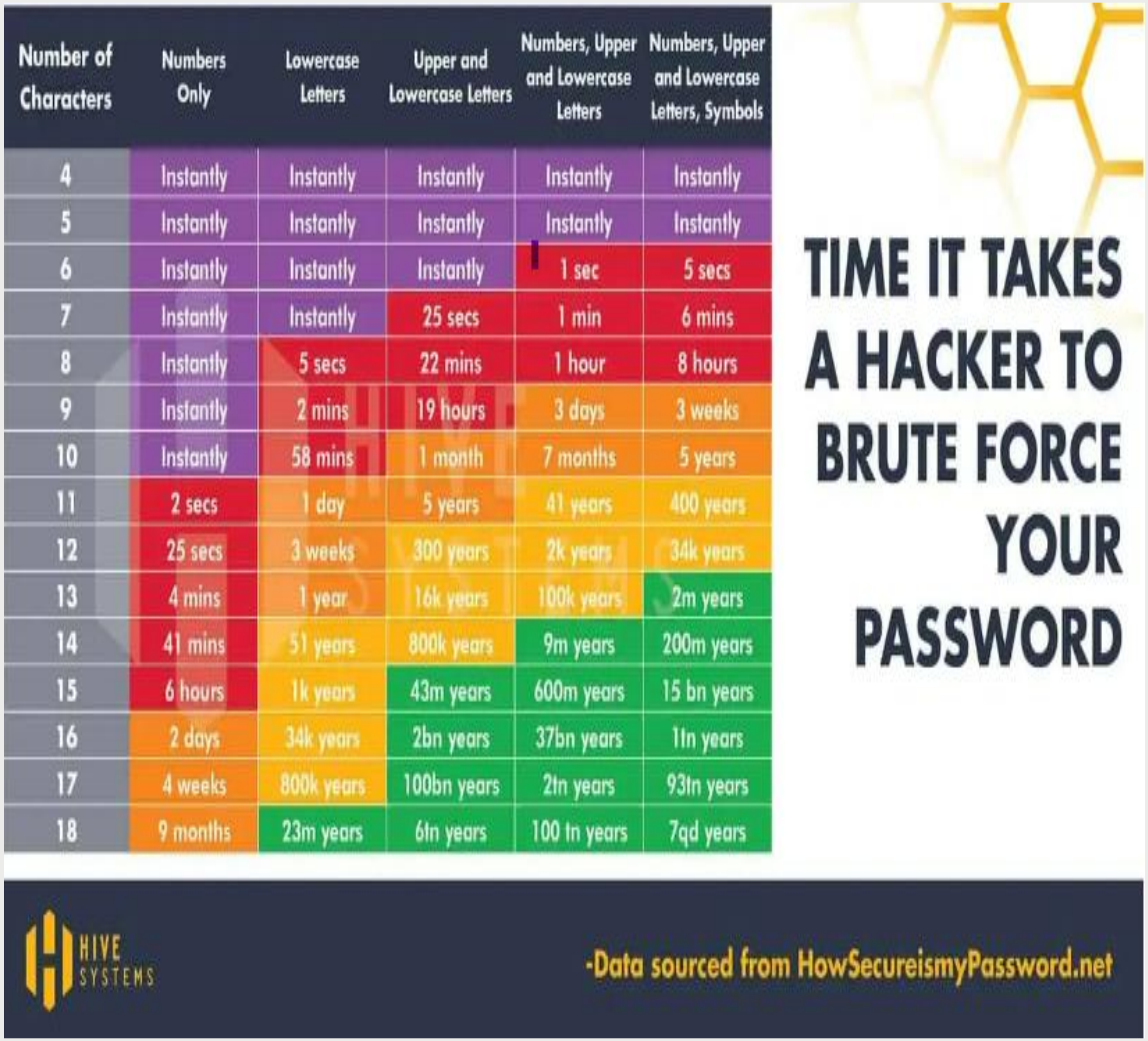
HIVE SYSTEMS

-Data sourced from HowSecureismyPassword.net

CYBERSECURITY & DATA SECURITY

Passphrase Security – Is your data secure?

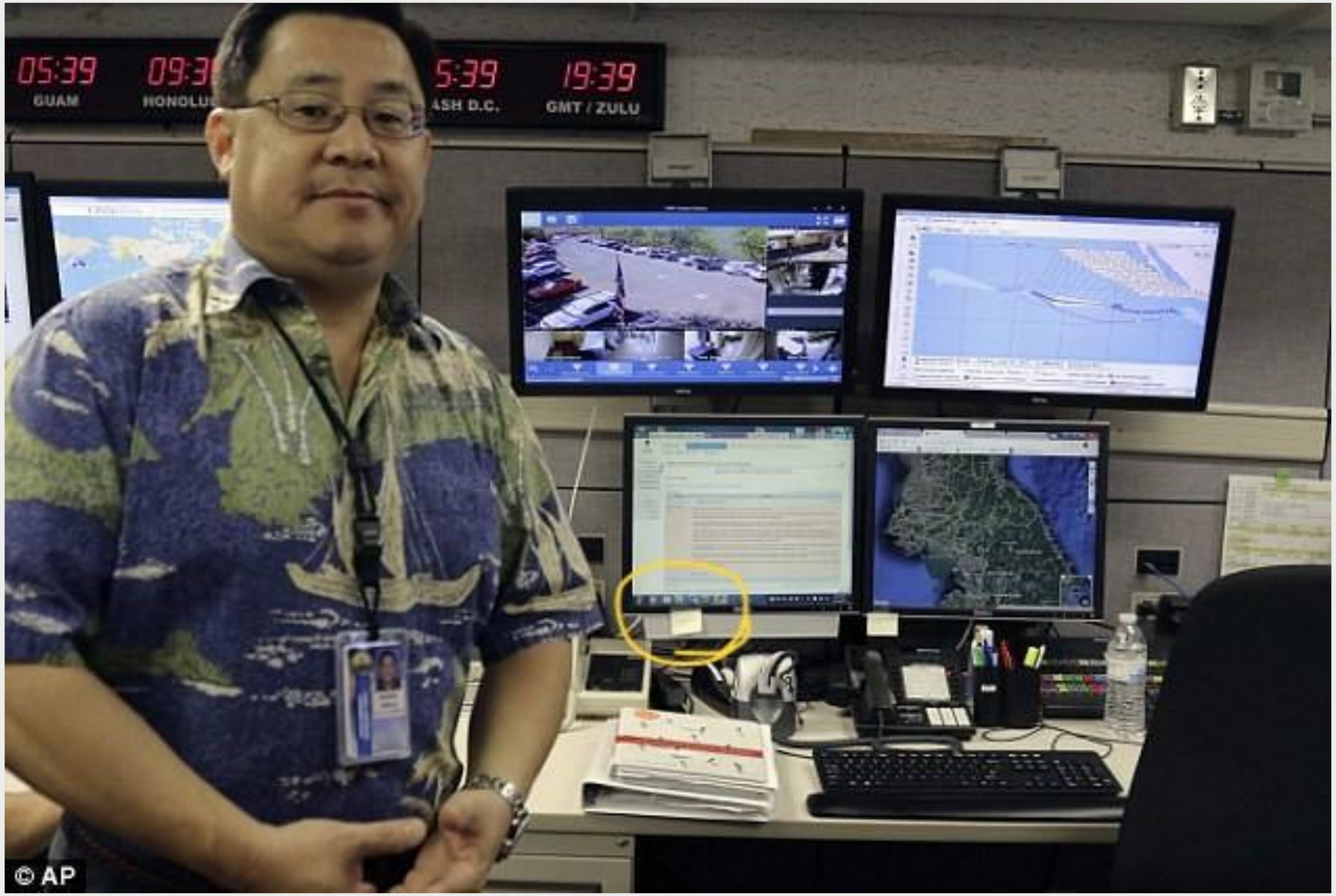
- HNECCPhn (8 Characters – 22 Minutes)
- Gr33nC@kes? (11 characters – 400 yrs)
- T3rrib!ecoFF33 (14 characters – 200m yrs)
- Be5Tpresent@tionevR (19 characters – 7qd yrs+)

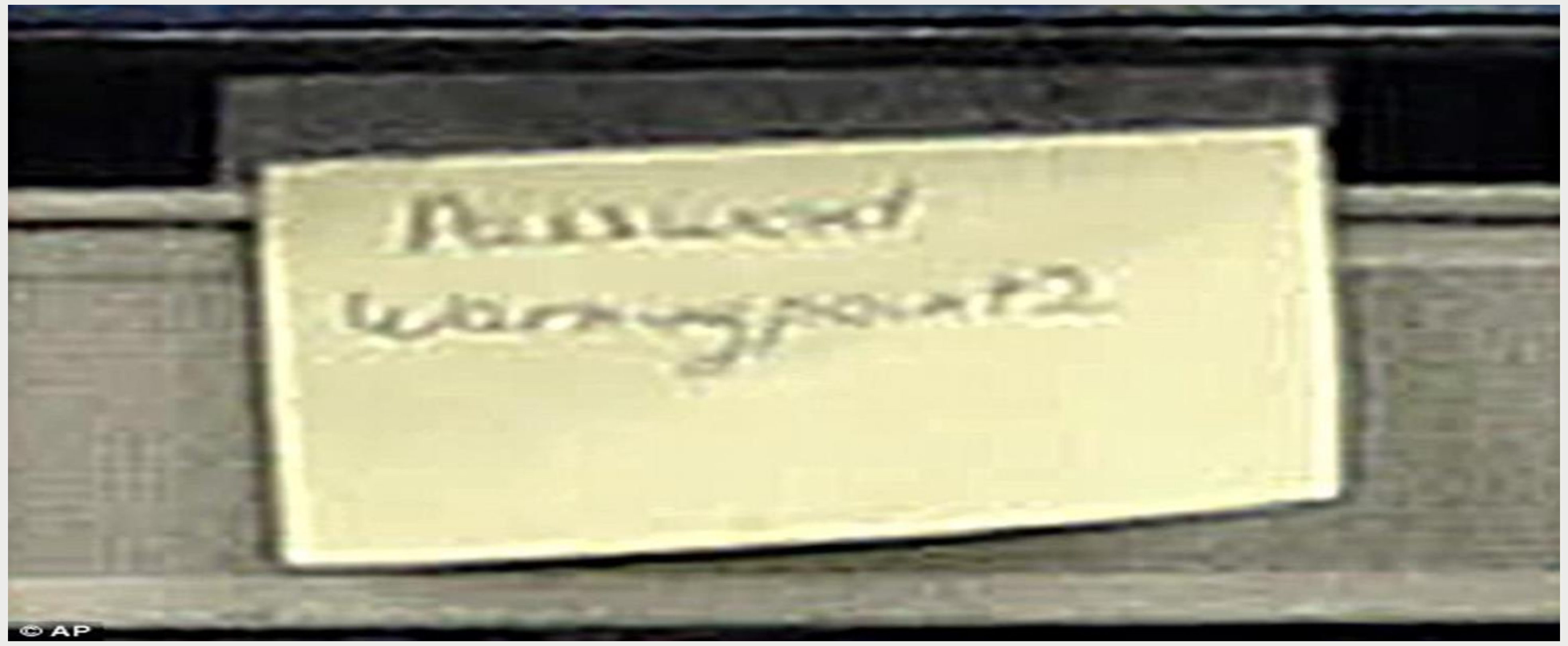


TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

-Data sourced from HowSecureismyPassword.net





Images Source: Daily Mail.co.uk

CYBERSECURITY & DATA SECURITY

Data Security – Is your data secure?

#2 Ransomware

Ransomware is a type of malware designed to prevent or limit access to a user’s system by locking the screen or files until a ransom is paid.

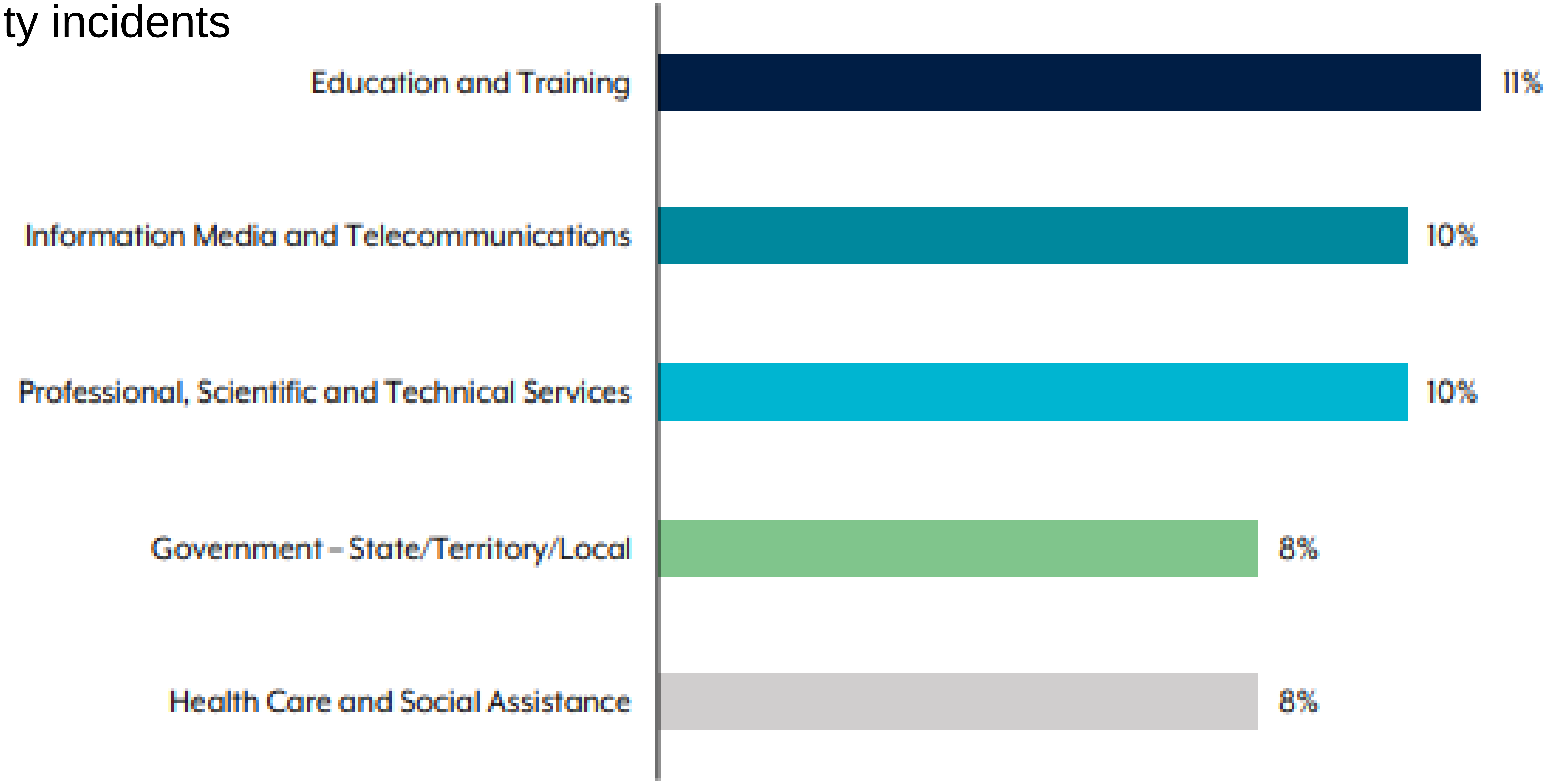
Mitigated by

- Web filtering
- Email filtering
- Application whitelisting
- Business continuity and disaster recovery plan

Image Source: Adobe Stock

CYBERSECURITY & DATA SECURITY

Top 5 reporting sectors for ransomware-related cyber security incidents



Source – Australian Cyber Security Centre - Cyber Threat Report 2021-22

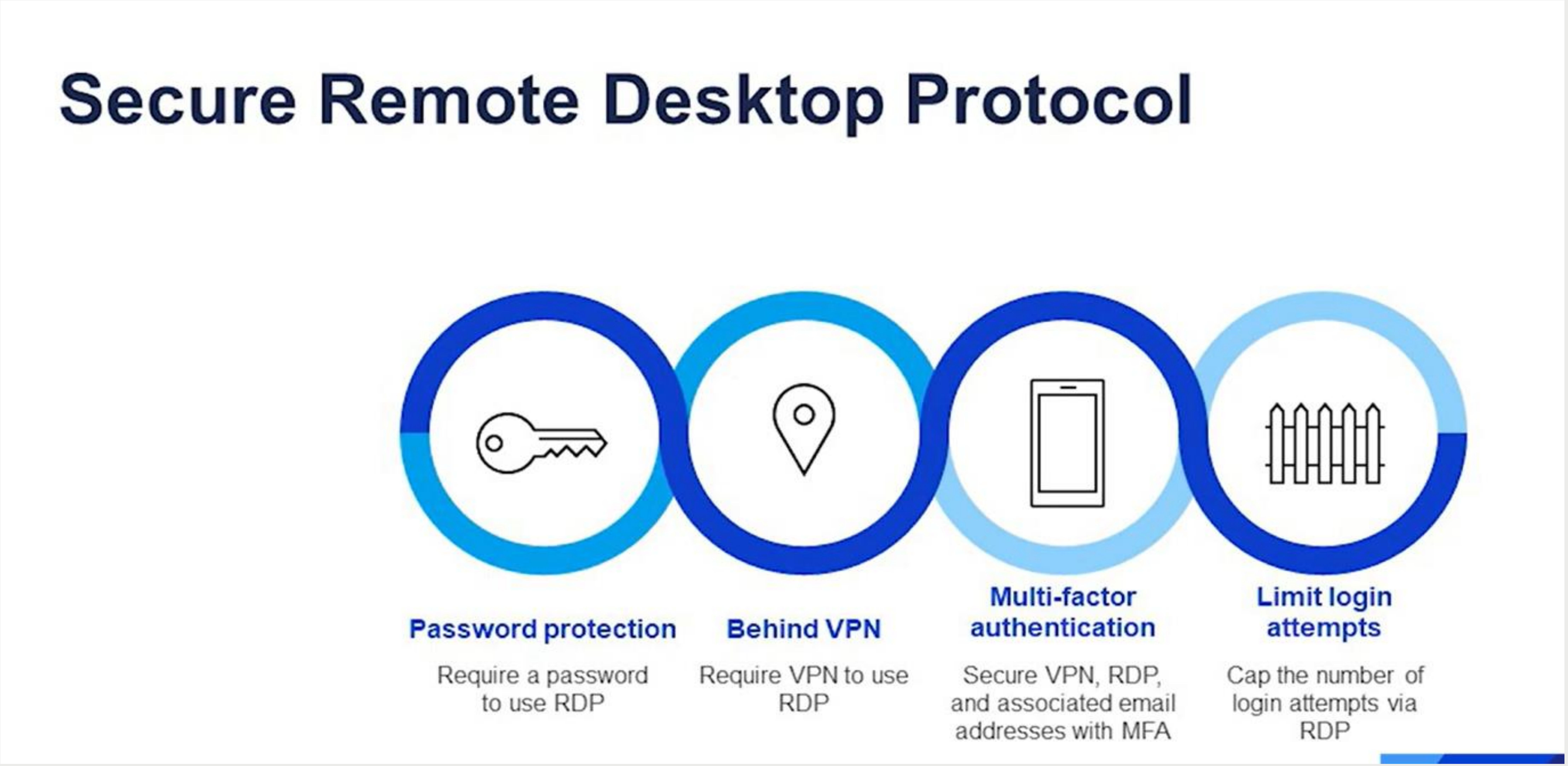
CYBERSECURITY & DATA SECURITY

Data Security – Is your data secure?

- Security software – Is it fit for purpose and updated?
- Secure Messaging – Is it used to send & receive or just receive? Should you have capability for both?
- Are you sending encrypted eReferrals?
- What do you use email for and do any emails you send or receive contain patient information?
- Fax/eFax – Is your fax secure? Does your eFax use email and if so is this secure or encrypted?
- IT Hygiene – USB's and other mediums
- Are staff trained and regularly updated about cybersecurity?

Image source: dataversity.net

CYBERSECURITY & DATA SECURITY



Secure Remote Desktop Protocol

Password protection

Require a password to use RDP

Behind VPN

Require VPN to use RDP

Multi-factor authentication

Secure VPN, RDP, and associated email addresses with MFA

Limit login attempts

Cap the number of login attempts via RDP

Source: Malwarebytes

CYBERSECURITY & DATA SECURITY

User permissions

- Do they allow staff to work effectively within their job scope?
- Who requires administrator level access & who doesn’t?

Software

- Keep all software up to date and running on the latest version.
- Don’t unduly delay software upgrades (CMS/OS/BIOS/Drivers).

Backups

- Are they done daily and stored offsite?
- Cloud storage vs Physical Drive.
- What is backed up?
- Secondary Server.
- Have you tested your data recovery from your backup?

Image Source: Adobe stock

Image Source: Adobe stock

CYBERSECURITY & DATA SECURITY

Policies & Procedures

- Does what you say you do in your Policies & Procedures Manuals match what you and your team actually do day to day?
- Disaster Recovery and Business Continuity Plans - Storage, knowledge and availability.

IT Consultants/Suppliers

- Do you use an IT supplier or do you do it yourself?
- Does your IT consult with you or just do the work and send an invoice?
- Do you or your practice manager know your IT administrator passwords?
- Does your IT Consultant work for you or do you work for them?

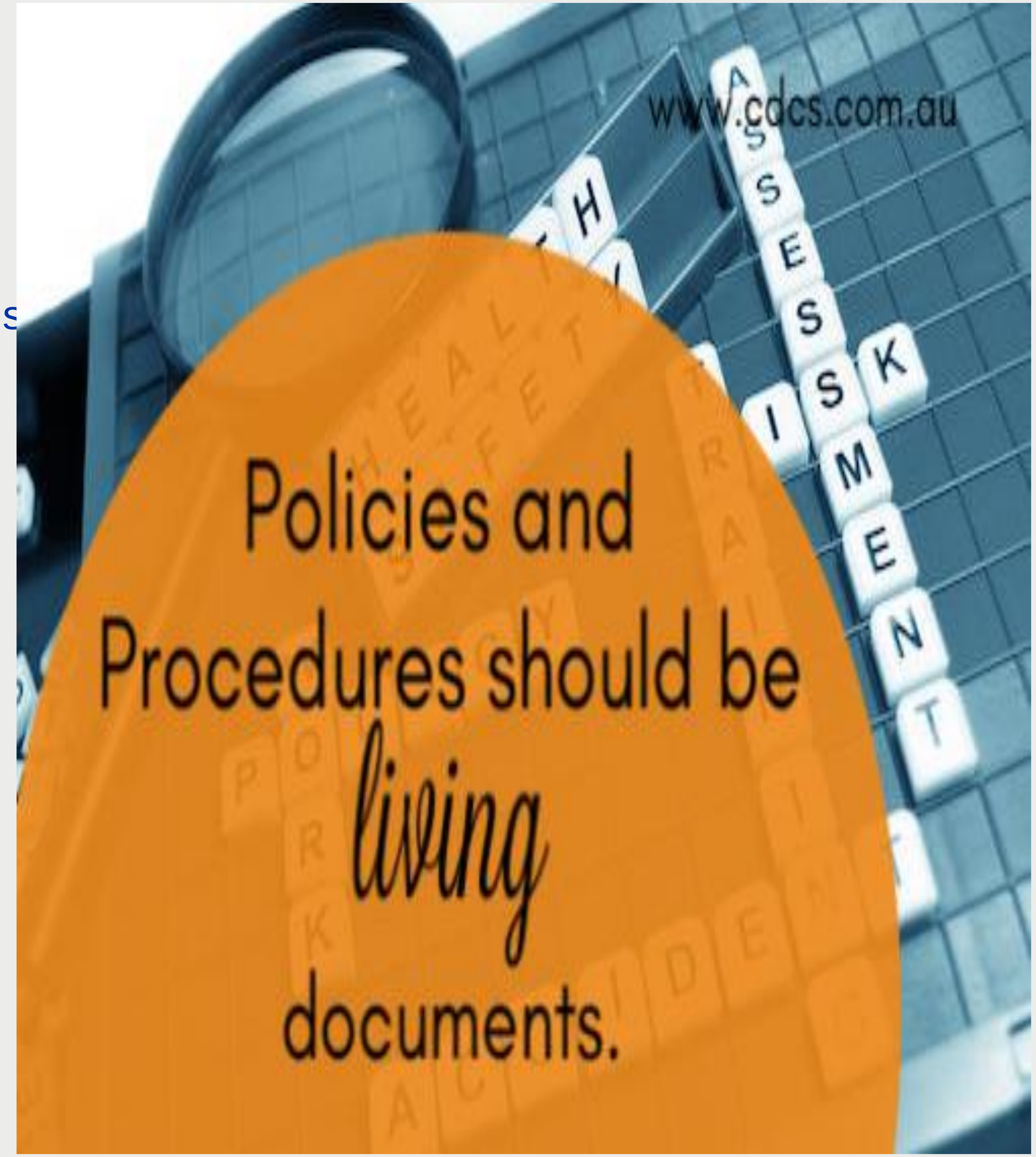


Image Source:cdcs.com.au

CYBERSECURITY & DATA SECURITY

Scenario 1:

Break in and theft of IT hardware (server &/or hardware) - On premise server and clinical management system

- Purpose of theft (Data theft/ransom/fraud)
- Prevention - Practice Security and IT storage (alarm system/monitored alarm system/key access/server storage (locked room with deadlock or under a desk).
- Password access – 40% of respondents in the GP HTDCS stored passwords on paper, in notebooks or a word document.
- SLA's with ITMSP – replacement IT hardware and/or operating environment time/data recovery time/what is backed up/where is the backup stored (is it password protected and/or encrypted)? Can ITMSP do what they say they can do? Has it been tested?
- What is the likely downtime and what would be the impact of that downtime? Business Interruption Insurance coverage?
- Who to advise Police/ITMSP/PHN/Insurance/Staff/OAIC.

Image Source: serverguys.com.au

CYBERSECURITY & DATA SECURITY

Scenario 2:

Break in and theft of IT hardware – Cloud based server and clinical management system

- Actual theft of IT equipment – Hardware
- Purpose of theft (Data theft/ransom/fraud)
- Prevention - Practice Security and IT storage (alarm system/monitored alarm system/key access)
- Password access – 40% of respondents in the GP HTDCS stored passwords on paper, in books or a word document
- SLA's with ITMSP – Replacement IT hardware time/data recovery time/what is backed up/where is the backup stored (is it password protected and/or encrypted). Can ITMSP do what they say they can do? Has it been tested?
- What is the likely downtime and what would be the impact of an that downtime? Business Interruption Insurance coverage?
- Who to advise Police/ITMSP/PHN/Insurance/Staff/OAIC.

Image source: Adobe Stock

PRIVACY

Data Breaches

What are Notifiable breaches?

- A data breach happens when personal information is accessed or disclosed without authorisation or is lost. If the Privacy Act 1988 covers your organisation or agency, you must notify affected individuals and the OAIC when a data breach involving personal information is likely to result in serious harm.

What is the process to follow after a data breach

- https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response

Australian Government

Office of the Australian Information Commissioner

Data breach preparation and response

A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)

oaic.gov.au

RESOURCES

Australian Digital Health Agency

- https://www.digitalhealth.gov.au/healthcare-providers
- https://www.digitalhealth.gov.au/healthcare-providers/training-and-support/cyber-security-training-and-support
- https://training.digitalhealth.gov.au/login/index.php
- Backups - Prepare for an emergency (digitalhealth.gov.au)

Australian Cyber Security Information Commissioner

- https://www.cyber.gov.au/

RACGP

- https://www.racgp.org.au/

Office of the Australian Information Commissioner

- https://www.oaic.gov.au/

You can check if your email or phone has been in a data breach here:

https://haveibeenpwned.com/

The PHN

- Developing an online training platform that will build on the ADHA Training and cover cybersecurity and data security.

Image Source: Adobe Stock