Information Security

Essential components of data security, privacy and risk management for your school

Introduction:

- 20 years in education
- Experience in VET, HE and K-12
- Former Head of IT - Europe for Navitas
- Former IT Director for TKAT (UK)
  - Implemented GDPR standards across 3500 employees and 22,000 students
  - Designed and implemented cyber security program, reducing risk and winning accolades from Department for Education

Topics and aims for today

- Privacy
  - What is privacy and why is it important?
  - What is personal information?
  - Awareness of relevant laws and penalties
  - What is GDPR and how does it affect Australian/NZ schools?
- Privacy risk areas
  - The risk profile
  - Privacy Impact Assessments
  - Handling a data breach
- Security
  - Common security breaches in education
  - What should you focus on?
  - What does a good security program look like?
  - Risk Management
- Predictions and tips

What are we doing? High level overview

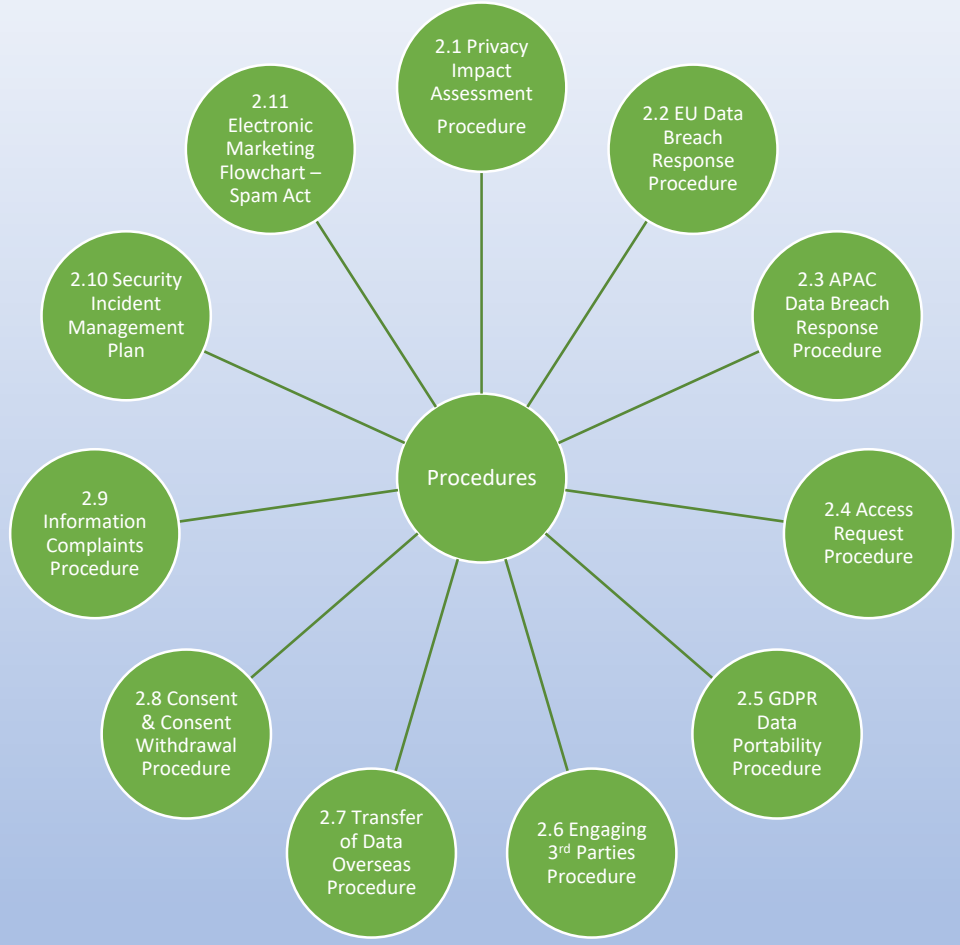
- New Information Governance Framework developed

- Privacy
  - GDPR is our benchmark regulation
  - Privacy and awareness training for all staff
  - Process mapping by department to find issues and mitigate risks
  - New policies developed (inc data protection policy)

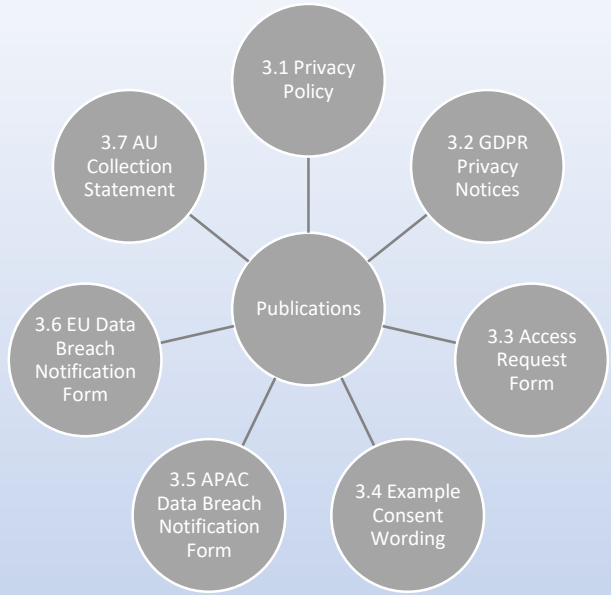
- Security
  - Risk assessments of each subsidiary
  - Security training being released to all staff members through myEdOnline
  - Security policies and procedures all drafted including Security Incident Management Plan

EHG Information Governance Framework

1. Clarify accountability



2. Guide actions



3. Ensure transparency

4. Ensure compliance

EHG employs a collection of policies, procedures, publications and tools to help protect information

5. Embed security

What is privacy?

- Our right to have our personal information protected
- Protecting who we are, what we think, what we do and what we believe
- Privacy awareness is increasing amongst the general population and *digital natives*

Why is privacy important?

- Ensures protection of an individual's identity
- Maintains confidence in the education system
- Retain parent and student confidence
- Reduce risk of penalties

- *International privacy laws are getting tougher. Examples are:*
  - *EU GDPR (2018)*
  - *Brazilian General Data Protection Law (2018)*
  - *Vietnam Cybersecurity Law (2019)*
  - *Thailand Personal Data Protection Act (2019)*
  - *California Consumer Privacy Act (2020)*
  - *Indian Personal Data Protection Bill (drafted)*
  - *China Data Privacy Act (in draft)*
  - *Kenya Data Privacy Act (in draft)*

Important: Australian Privacy Act changes announced 24th March

- *More powers to the OAIC*
- *Up to $10m fine OR 3 times the amount benefited by misuse of information OR 10% of a company's annual domestic turnover… whichever is greater*
- *Specific rules to protect the personal information of children and other vulnerable groups*

What is personal information?

'Information or an opinion about an identified individual, or an individual who is reasonably identifiable

Personal information can be:

- *True or false;*
- *Verbal, written or photographic*

- A person's name, signature, home address, email address, telephone number, date of birth, bank account details, TFN and credit information
- A person's employment details, such as work address and contact details, salary, job title and work practices
- An opinion about an individual's attributes can be personal information. For example, if you form an opinion about someone based on what you know of their gender or ethnic origin.

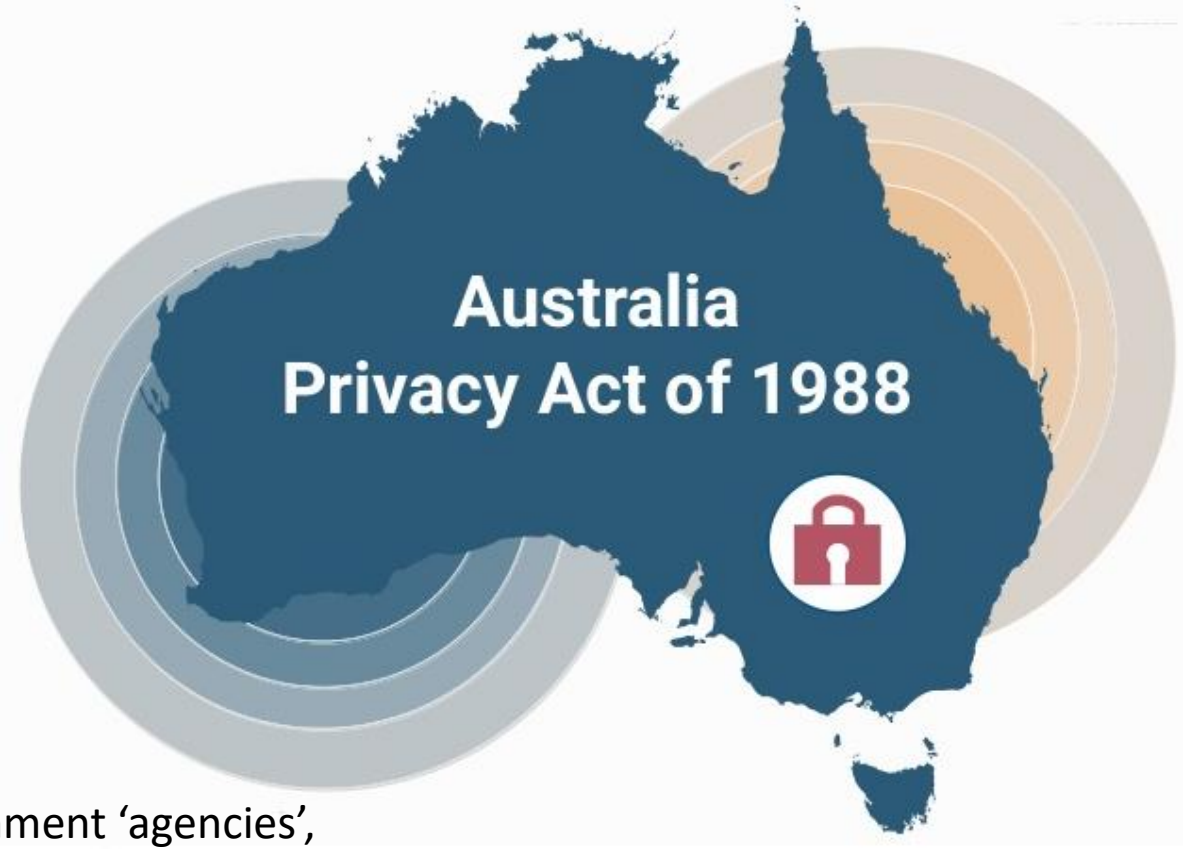
- **Sensitive information**: Health, race, ethnic origin, political opinions, membership of a political association, professional or trade association or trade union, Religious beliefs or affiliations, philosophical beliefs, sexual orientation or practices, criminal record, biometric information

It's important to know the difference in case a data breach occurs.

The Law

Privacy Act 1988 policed by the Office of the Australian Information Commissioner (OAIC)

- Latest revision 2018 incorporated ‘Notifiable Breach Scheme’
- Consists of thirteen privacy principles referred to as the ‘APPs’
- The APPs set out the rights and obligations for the *collection*, *use* and *disclosure* of personal information



Other relevant laws:

- Spam Act 2003
- State privacy laws – aimed at government ‘agencies’, including education

<u>In general, private/non-government schools are covered by the Privacy Act and public schools are subject to state or territory laws</u>

GDPR and Australian Schools - Myth busting

Some perspective..

A monumental effort, heavy fines

"GDPR is still being worked out" Not true. The GDPR text was agreed in 2016 and went into law in 2018

"GDPR only concerns European citizens" Not true. "*This Regulation applies to the processing of personal data of data subjects who are in the Union*" Article 3(2)

"If you teach a European child in Australia, they are protected by GDPR" Not true. See above.

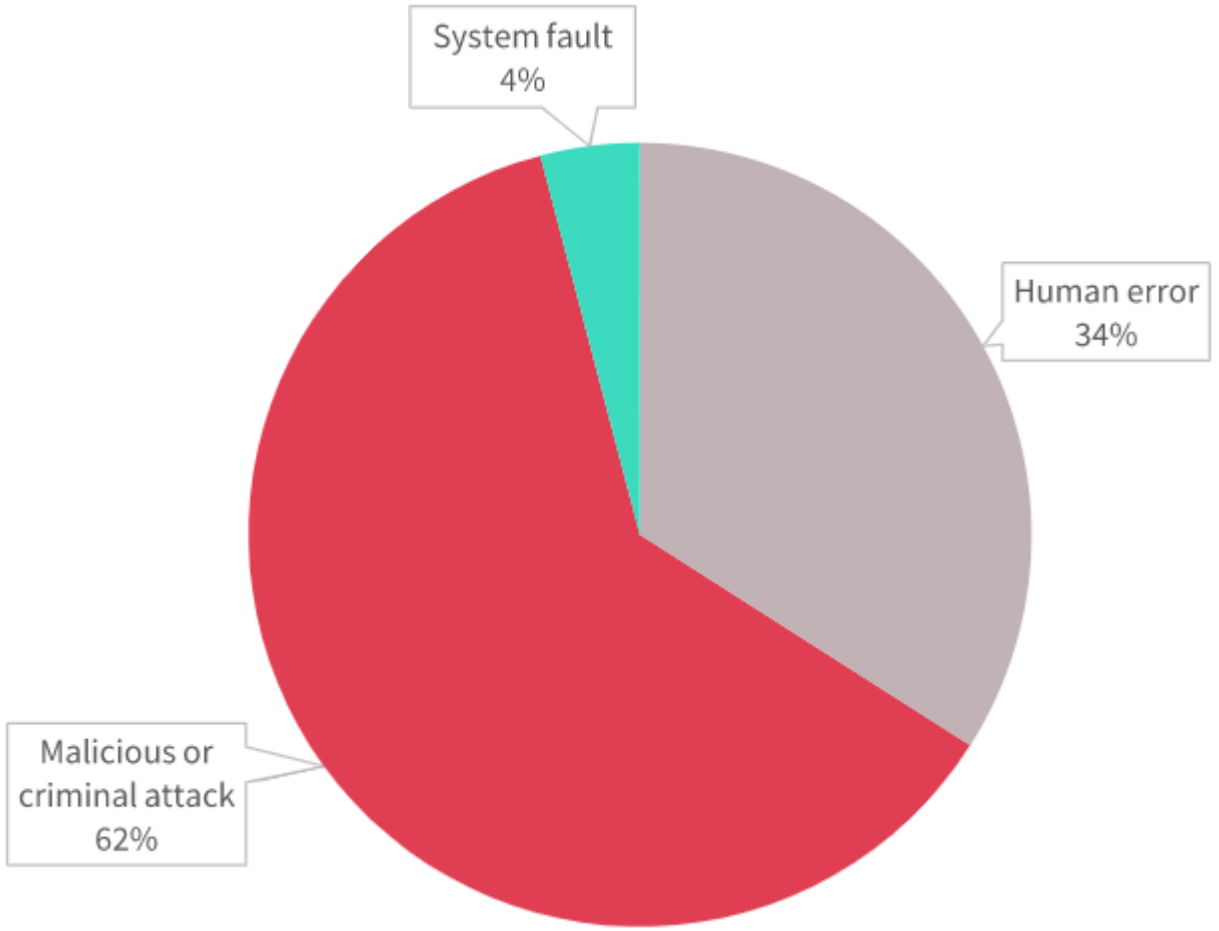
"Australian and NZ schools are not in scope" True, unless processing EU resident's data (e.g. parents are in Europe)

General advice:

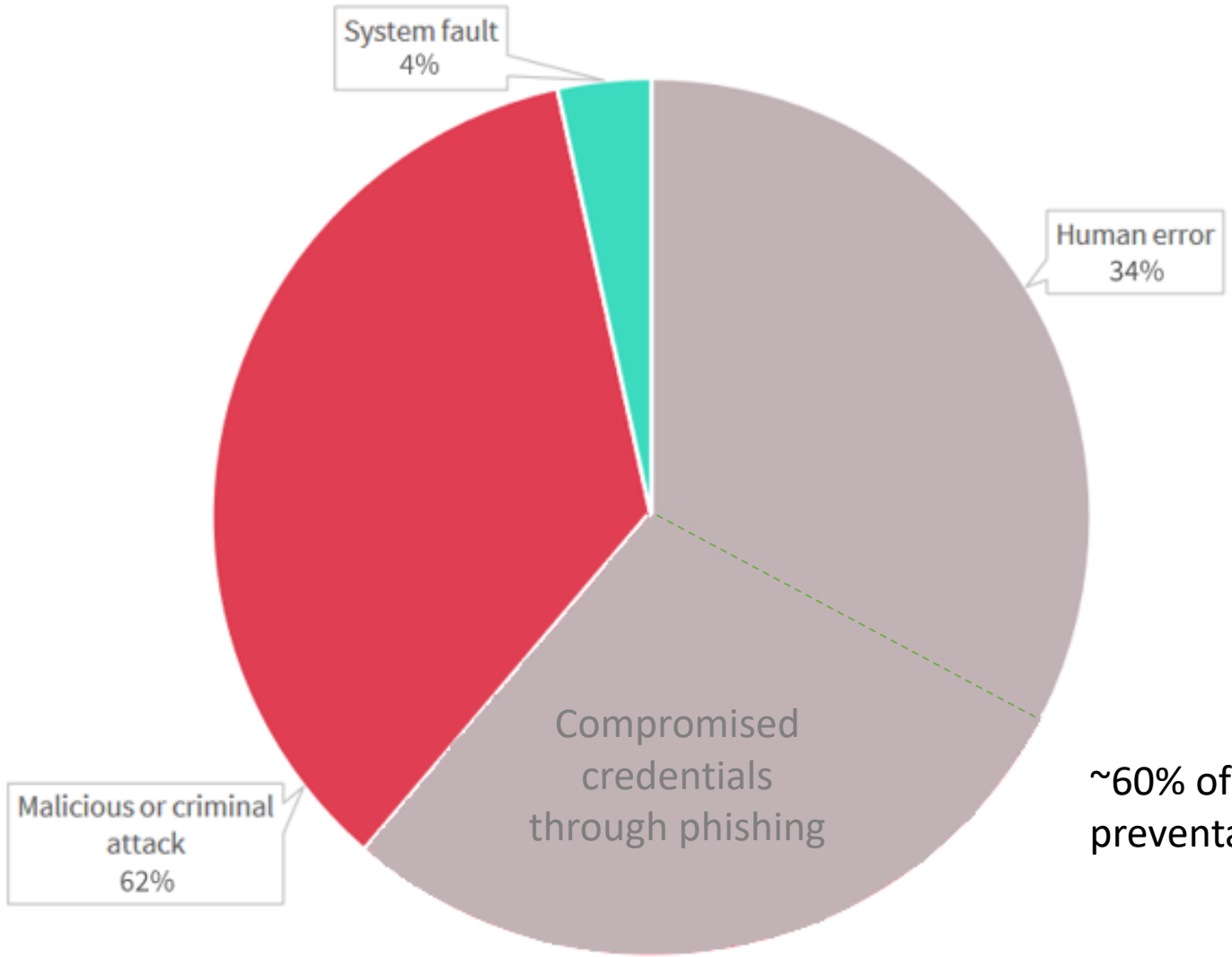
- ✓ Do not panic
- ✓ Providing your privacy practices are sound then you are low risk
- ✓ If they are not mature, consider starting a privacy program (gap analysis, process mapping, policy review etc)
- ✓ Follow advice on following pages….

Privacy risk areas for schools

Privacy Risk Profile

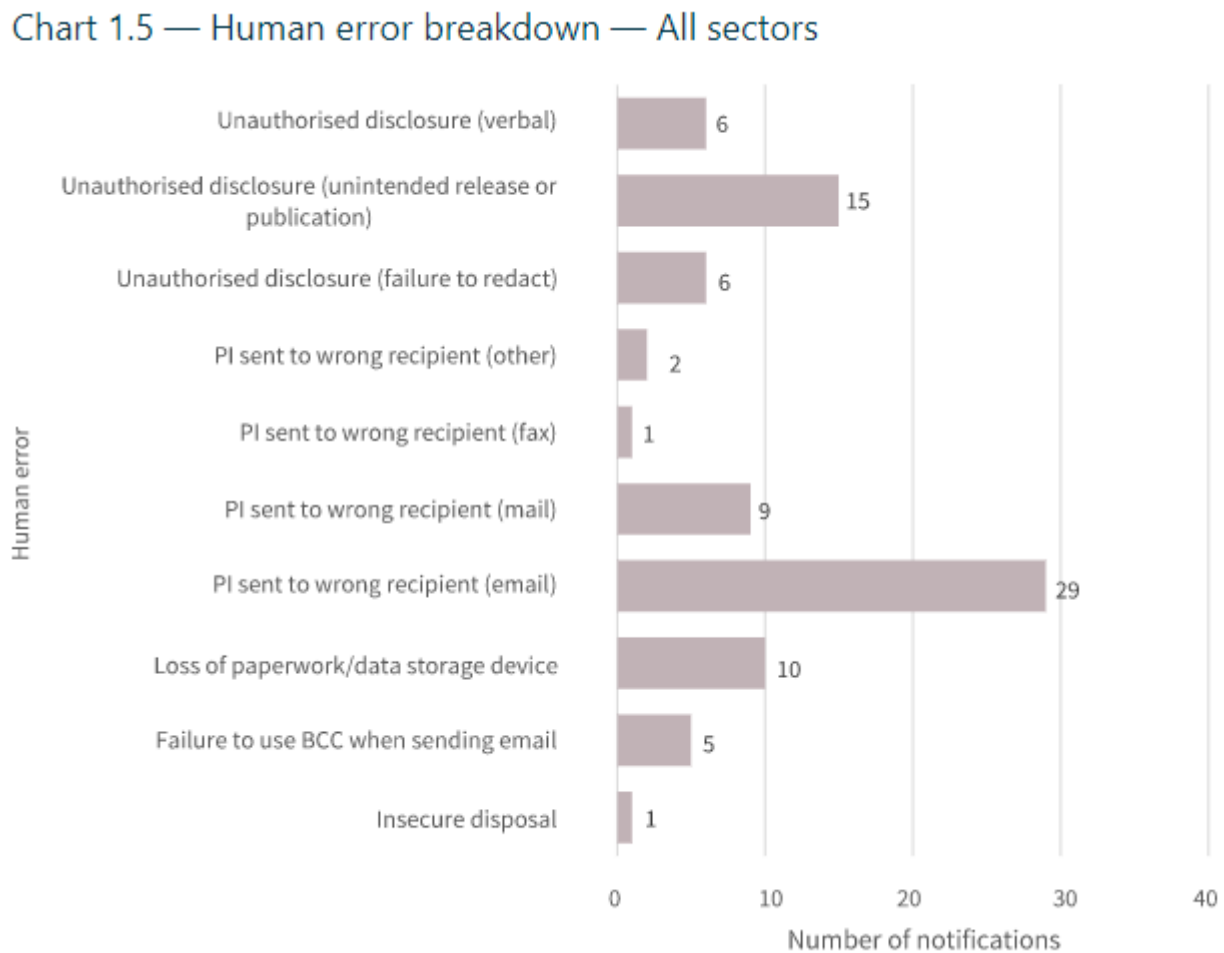


OAIC Quarterly Report August ’19 – Sources of data breach



~60% of data breaches highly preventable

Phishing accounted for 43% of all malicious or criminal attacks in Q2 2019



245 Breaches notified relating to over 10,000,000 individuals

Future scenario for your schools?

BBC Sign in | News | Sport | Weather | Shop | Reel | Travel | More | Search

NEWS

Home | Video | World | Asia | UK | Business | Tech | Science | Stories | Entertainment & Arts | Health | World News TV | More

England | Local News | Regions | Kent

Rochester Grammar School USB stick loss exposes pupil data

5 June 2018 Share

A USB stick was lost from Rochester Grammar School

The data of more than 1,000 pupils at a Kent school was exposed when an unencrypted memory stick was lost.

The stick held information on every pupil at Rochester Grammar School.

It included the names, years, school house, date of birth, email address and special

LIVE **BBC Live: South East**

19 March 2019

Scheme to help the poor has funding cut

Top Stories

Father and son in first NZ mosque funeral

The two Syrians had come to New Zealand as refugees and leave behind a wife and younger brother.

47 minutes ago

'This isn't us... or is it?' asks NZ comic

3 hours ago

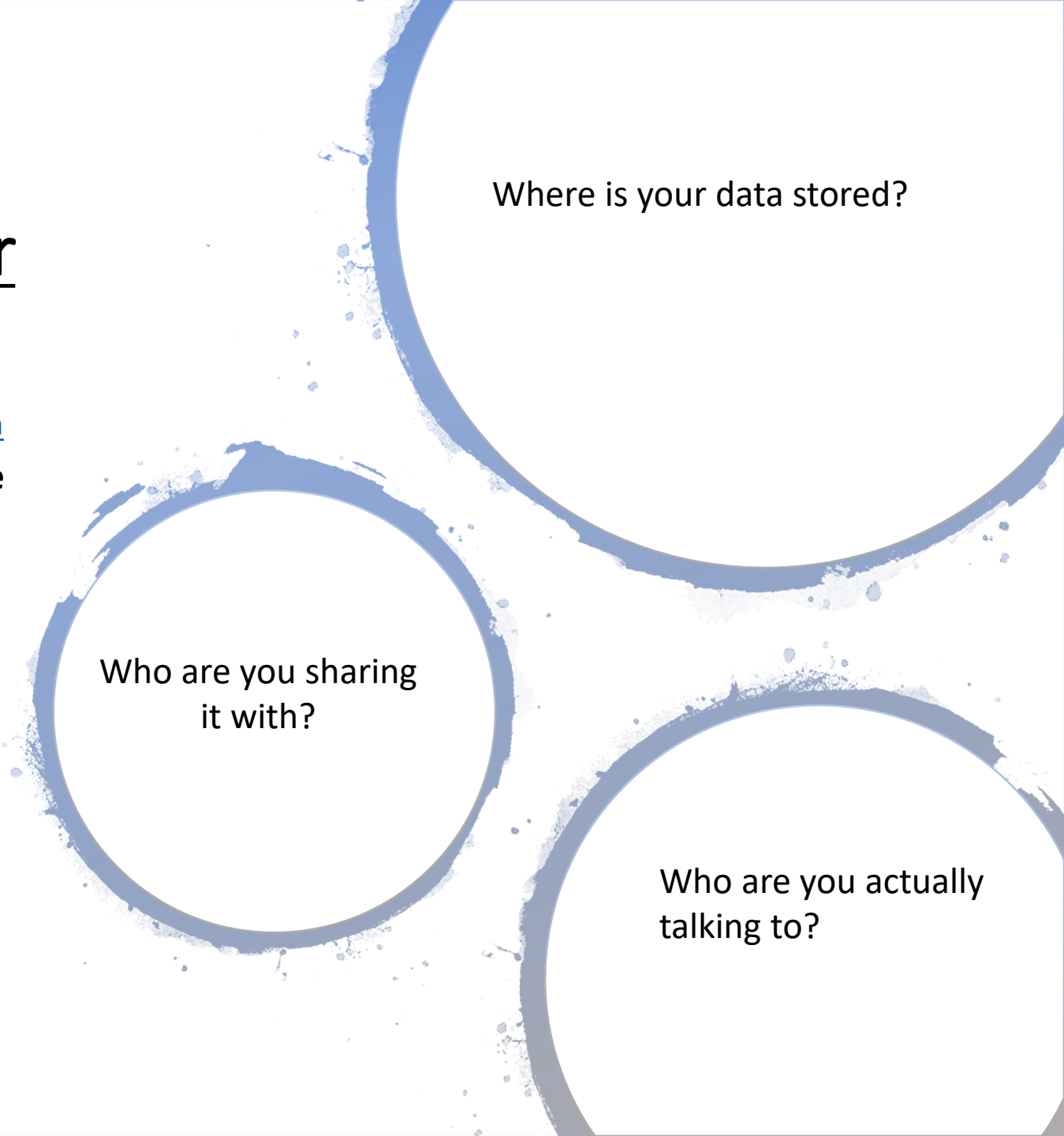
UK cabinet row over PM's Brexit delay bid

1 hour ago

Features

Other risk areas to consider

- **International data transfers** – *consider cloud providers and where they store data*. https://www.acsc.gov.au/infosec/irap/certified_clouds.htm
- **Do you have an appropriate lawful basis to share all of the data you are sharing**? *Are you sharing more than you need to?*
- **Do you have processes for dealing with 3rd parties?** *Are caller identities validated before information is released?*
- **Do you have privacy training in place for ALL staff?**



Privacy Impact Assessments

- A measure recommended by Information Commissioners to help ensure compliance
- Used for:
  - New or amended programs, activities, systems or databases
  - New methods or procedures for service delivery or information handling
  - Changes to how information is stored.

https://bit.ly/2ophegq

Conducting PIAs is a globally recognised method managing for any risky activity

Handling a data breach

- Understand: Data breaches will happen.
- It's important to try to reduce the number of them through training and awareness, but have a plan in place for when they happen

Steps:

1. Appoint a Privacy Officer
2. Understand which Privacy Law(s) apply to you
3. Have your Privacy Officer design or adopt a data breach process:
    1. *Contain the breach – conduct an initial assessment*
    2. *Evaluate the risks associated with the breach*
    3. *Mitigate against further harm*
    4. *Remediate where possible*
    5. *Notify individuals and/or authorities as appropriate*
    6. *Review the cause of the breach and implement improvements/learn lessons*

Security

Common security breaches in education

- Not password protecting or encrypting email attachments
- Using unencrypted USB storage devices to store and transfer personal and sensitive information
- Disclosure of information over the telephone to an unauthorised recipient
- Poor access control on file servers
- Poor password management – *such as changing a highly confidential password and sending it to our Service Desk or staff account takeovers by pupils*
- Holes in perimeter networks – e.g. RDP ports left open to the internet
- Backup failures (configuration errors, lack of ‘air-gap’ or not being tested)

What should you focus on?

1. Training and awareness – reduce breaches that result from human behaviour

- **Cybersecurity Basics** – users need to be able to spot attacks such as phishing, spear-phishing etc
- **Privacy Basics** – including sharing of data securely in any form

2. Harden your defences

- **Access Control** – least privilege, role-based access, processes for onboarding, offboarding and crossboarding
- **Firewall security** – minimise open ports and ensure good change control. Pen testing
- **Protect internally as well as externally** – VLANs with strict ACLs
- **Password management** – long passphrases, no expiry, no complexity, check passwords against breached password list
- **Multi-factor Authentication** – reduces successful phishing attacks dramatically (there are ways to may this less frustrating)
- **Preventative maintenance** – patching and update of operating systems and applications
- **Ensure a good quality antivirus**

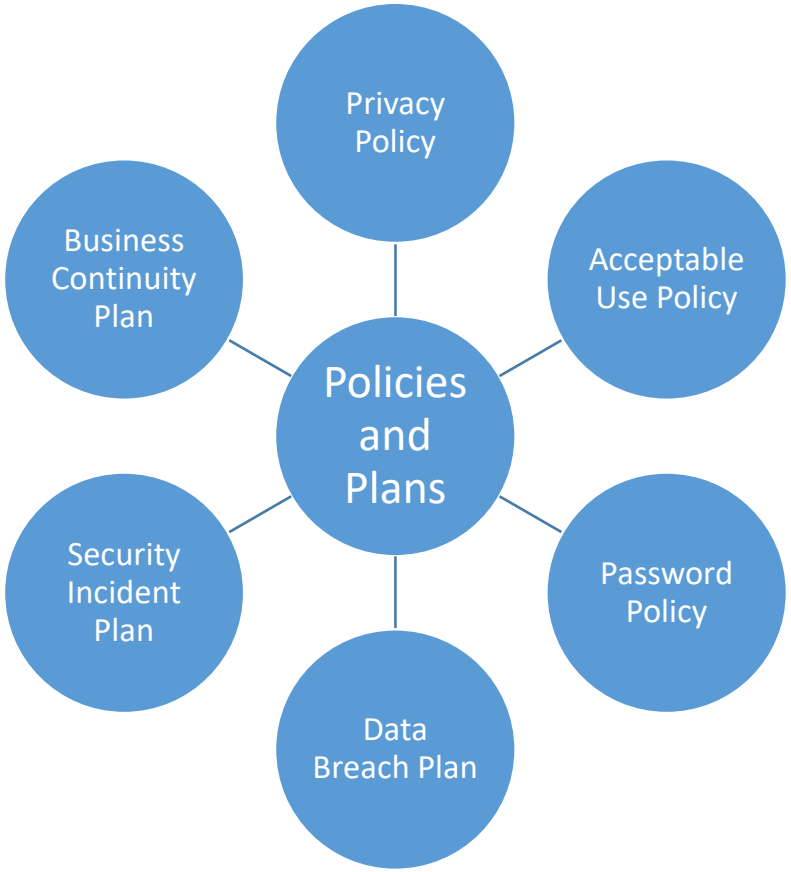
3. Review your backup strategy

- **Frequency** – should be daily and monitored to ensure they are successful
- **Airgap** – ensure your backups are kept separate from your main network (e.g. offline copy)
- **Planning** - Backup plan + disaster recovery plan (subset of BCP) are up-to-date and meet business expectations

4. Be prepared

- **Incidents** - Security Incident Plan should be drafted and tested
- **Risk register** – track where you believe you have risks

Small School Essential Policies



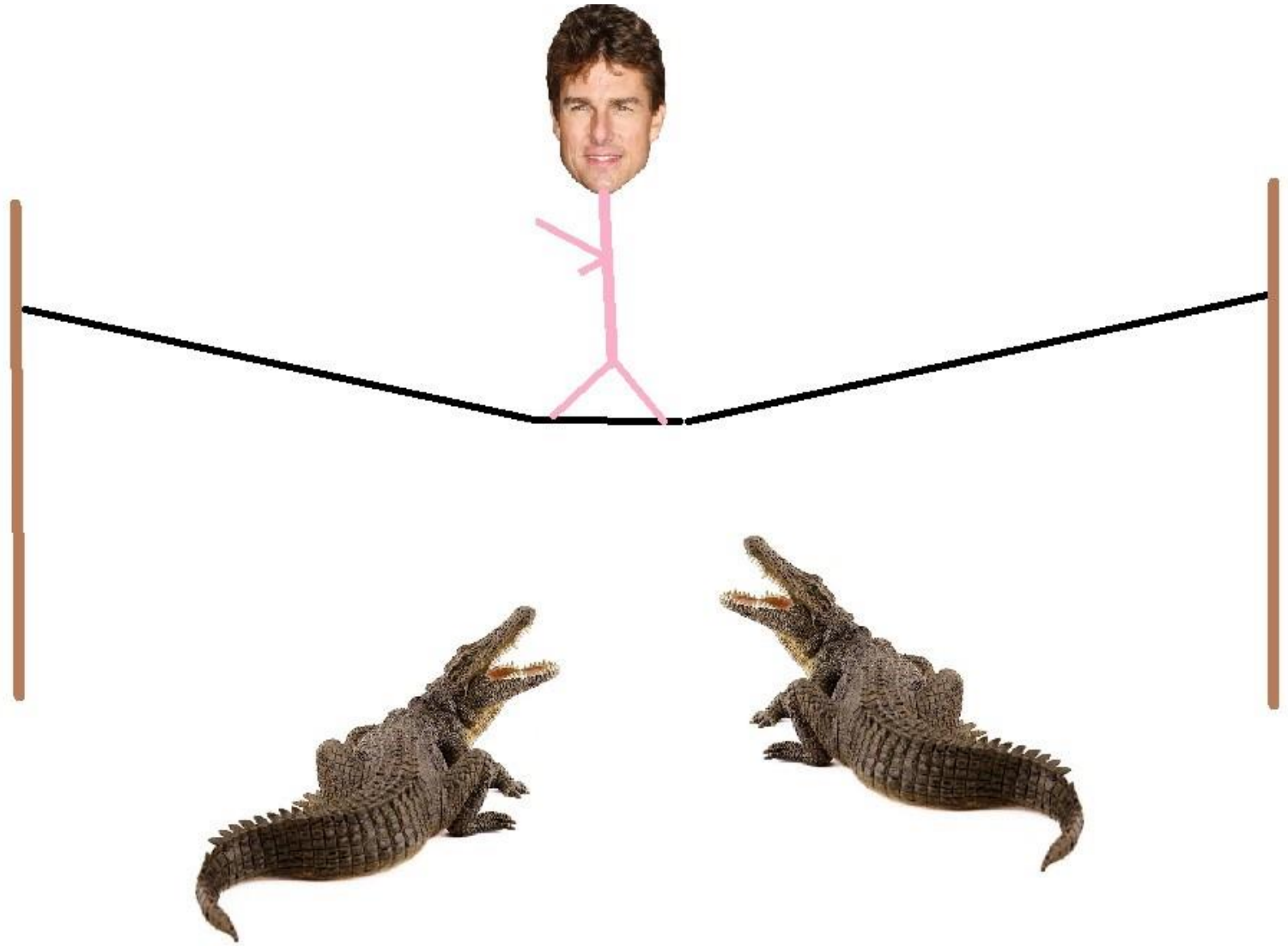
- Internet use
- Security of personal information (staff, students and parents)
- Using personal devices for work
- Remote working procedures

What does a good security program contain

1. Training and awareness – All staff
2. Policy & Procedures – Ensure they are understood
   - Accountability at all levels Intern to Principal
     - IT Security Policy
     - Password Policy – *Passphrases not passwords*
     - Acceptable Use Policy
     - Disaster Recovery Policy etc
3. Risk assessment – Continuous cycle
4. Adoption of the ACSC Essential Eight
5. Tracking at board/senior leadership level (example RAG status) – this is not an IT responsibility, it's a school responsibility. IT should be held to account for security, but need adequate support to succeed

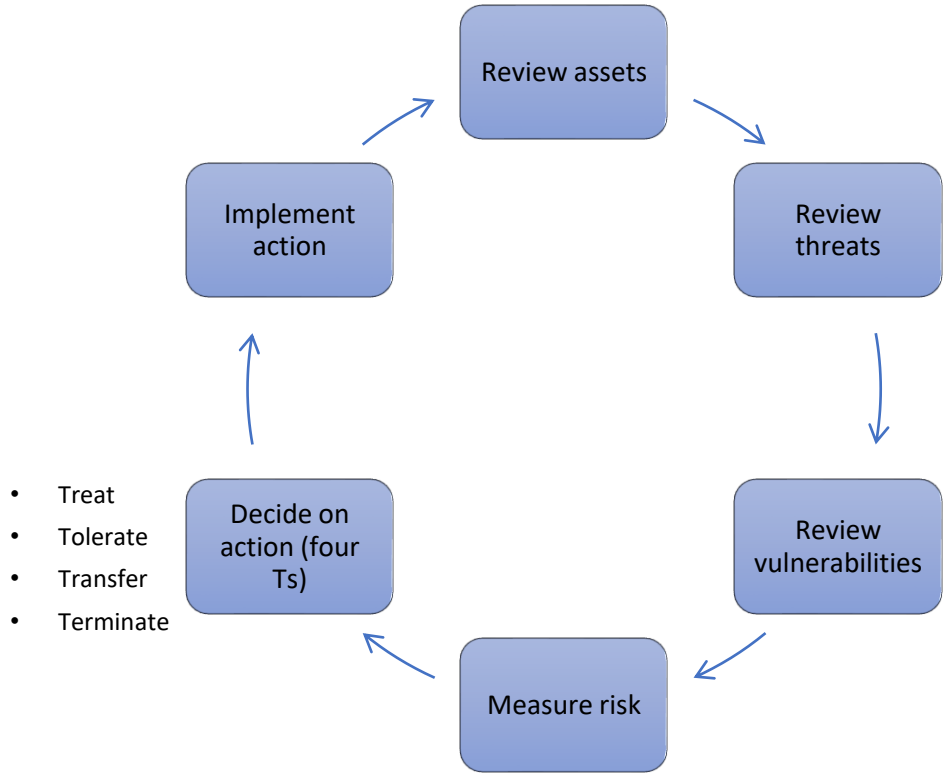
IT Security	R	The school is at imminent risk of multiple attack vectors and/or is not benchmarking regularly (every 6 months).
	A	School has gone some way to mitigate against identified IT security risks and common attack vectors, but some areas for improvement remain, may not benchmark every 6 months.
	G	School has reviewed IT security risks and has mitigated against all identified risk areas and attack vectors, benchmarks every 6 months. Has adopted the 'ACSC Essential Eight'.

How to manage IT Security? *Risk Management*



ASSET: Tom Cruise, THREAT: being eaten by crocodiles, VULNERABILITY: insufficient safeguards to prevent him falling off

Risk Assessment



Asset	Threats	Vulnerabilities	Impact	Likelihood	Risk Rating	Treatment	Residual impact	Residual Likelihood	Residual Risk	Risk Owner	Due by
Servers	Loss of data	Lack of disaster recovery plan	HIGH	HIGH	HIGH	Implement disaster recovery plan	HIGH	VERY LOW	LOW	Joe Bloggs	14/7/2019
Laptops	Theft of data	Lack of encryption	HIGH	MEDIUM	MEDIUM	Encrypt laptops with Bitlocker	HIGH	VERY LOW	LOW	Ivor Plan	15/6/2019

Predictions and Tips

- Australian and New Zealand privacy regime to get tougher over time
- Other nations to continue adopting GDPR-style privacy laws
- Greater emphasis on security in the education sector
- Student and particularly parents' awareness of privacy and their digital rights to increase

- ✓ Train your staff in privacy and cyber security
- ✓ Harden your school defences
- ✓ Manage your passwords properly and use ***MFA*** wherever possible
- ✓ Review your backup strategy
- ✓ Be prepared with a data breach and security incident plan
- ✓ Appoint a Privacy Officer and give them time and support
- ✓ Be aware of the privacy laws that your organisation is bound by and make use of the free materials available to you
- ✓ Conduct PIAs when appropriate, especially when bringing on new services
- ✓ Make your security program proportionate to your size and your activities

Thank you