Cybersecurity

As presented by the IT Department

Cybersecurity is the protection of computer systems from the theft and damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide.

What	How
• Theft • Damage • Disruption • Misdirection	• Targeted attacks • Deception – phishing! • Viruses/Worms • Botnets

Often more than one intention and method …

Rate of new 'specimens' (unique samples – not attacks) increasing exponentially …
2007 0.13 M - 2016 6.83M - 2017 est to be in excess of 7.5M and approx. 50% are Viruses

Risks & Vulnerabilities

- >80% of attacks are via weak or stolen passwords
- 1 in 131 emails contains malware
- Corporate email 6x more likely to be targeted than personal for phishing
- Most phishing occurs mid-week (when targets are at work)

Why does Cybersecurity matter?

- Threat volume rapidly increasing
    - Any kid can buy a malware kit for under $50 and stands to make thousands…
- Threat sophistication increasing
    - Intentional targeting of cyber defences (backups, etc)
- State actors are weaponizing cyber warfare and well funded
    - Trickle-down to non-state actors is easily observable
- Increasing governance expectations
    - No C-level or director should be ignorant or complacent
- Required by law
    - Privacy Act 1988 (Commonwealth)
    - Health Records Act 2001 (Vic)
    - Privacy and Data Protection Act 2014 (Vic)
- Becoming required by governments and funding agencies
    - E.g. CIMS in Victoria
- Cost

Mandatory Data Breach Notification

Personal information is lost or subject to unauthorised access or disclosure

- A database is hacked
- A device is stolen
- Information is provided to the wrong person

New legislation in force since February 22, 2018: https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

How to Cope

The Australian Signals Directorate (ASD) has developed strategies to mitigate cyber threats – the Essential Eight are the most effective – each has 5 maturity levels.

"As a baseline, organisations should aim to reach a maturity level of three for all of the Essential Eight mitigation strategies."

To prevent malware running

Application whitelisting TOP 4 A whitelist only allows selected software applications to run on computers. **Why?** All other software applications are stopped, including malware.	***Patch applications*** TOP 4 A patch fixes security vulnerabilities in software applications. **Why?** Adversaries will use known security vulnerabilities to target computers.
Disable untrusted Microsoft Office macros Microsoft Office applications can use software known as 'macros' to automate routine tasks. **Why?** Macros are increasingly being used to enable the download of malware. Adversaries can then access sensitive information, so macros should be secured or disabled.	***User application hardening*** Block web browser access to Adobe Flash Player (uninstall if possible), web ads and untrusted Java code on the Internet. **Why?** Flash, Java and web ads have long been popular ways to deliver malware to infect computers.

To limit the extent of incidents and recover data

Restrict administrative privileges TOP 4 Only use administrator privileges for managing systems, installing legitimate software and applying software patches. These should be restricted to only those that need them. **Why?** Admin accounts are the 'keys to the kingdom', adversaries use these accounts for full access to information and systems.	***Patch operating systems*** TOP 4 A patch fixes security vulnerabilities in operating systems. **Why?** Adversaries will use known security vulnerabilities to target computers.
Multi-factor authentication This is when a user is only granted access after successfully presenting multiple, separate pieces of evidence. Typically something you know, like a passphrase; something you have, like a physical token; and/or something you are, like biometric data. **Why?** Having multiple levels of authentication makes it a lot harder for adversaries to access your information.	***Daily backup of important data*** Regularly back up all data and store it securely offline. **Why?** That way your organisation can access data again if it suffers a cyber security incident.

https://asd.gov.au/publications/protect/Essential_Eight_Explained.pdf

The 6 Pillars of Cyberdefence

1. User education
   - The earliest and best form of defense
   - And, the least commonly used

2. Perimeter defenses
   - Generally effective, but relies mostly on having seen the malware before
   - Thus, vulnerable to 'zero day' exploits
   - Device that sits between private and public networks, also on email eg Mailguard

3. End user defenses
   - The most common but least effective
   - Most malware tricks the user into bypassing these defenses
   - For example, antivirus software

4. Heuristic* defenses
   - Effective, provided the heuristic is as predicted
   - Example, software that watches for patterns or situations that vary from the norm

5. Policies
   - A trade-off between safety and restricted freedoms
   - Personnel and machine setups

6. Second line of defense
   - Backup and disaster recovery.

*A heuristic technique, often called simply a heuristic, is any approach to problem solving, learning, or discovery that employs a practical method not guaranteed to be optimal or perfect, but sufficient for the immediate goals

What should you do?

- Get a cybersecurity audit & find out your vulnerabilities
- Address highest risks
- Train and engage staff - Create a security culture, Training, Induction**
- Ensure business continuity – backup & data recovery
- Report cybercrime

**** Identifying Fraudulent Emails**

- Check sender address
- Look for poor spelling or grammar
- You didn't initiate action or don't have an account
- Request sign in to a website or provides a link
- Request for personal information or payment
- Generic salutation or uses email name

Key Learnings

- Get a cybersecurity audit
- Policies & procedures (what to do if …)
- Staff training
- Upgrades – backups, software, protection software …
- Eliminate shadow IT
  - Hard drive storage v server or Cloud
  - Poor Dropbox use
  - Mobile devices – phones
  - Thumb drives

Useful Links

Office of the Australian Information Commissioner: https://www.oaic.gov.au
Strategies to Mitigate Cybersecurity Incidents: https://asd.gov.au/infosec/mitigationstrategies.htm
The IT Department: http://itdepartment.com.au

QORF
OUTDOOR PROJECTS