Security Concepts

Definitions

Information Security

Practices to keep data secure, defined in properties data should have

CIA per data

ICT Security

Monitor and control access to information

Safeguard transmission

Secure storage and data disposal

Cyber security?

The same computer?

A blend

Magic?

https://csrc.nist.gov/glossary/term/information_security
https://statisticaldataintegration.abs.gov.au/topics/secure-data-management/information-and-communication-technology-security

Confidentiality, Integrity, Availability (CIA)

CIA comes from the information systems industry

Confidentiality

Only those entitled to access the information can see it

Authorise, encrypt, access control, authenticate, restrict physical access

Integrity

Information cannot be altered and changes are immediately detectable.

Backup, checksum, hash, correction code

CIA...

Availability

Information is available (to read, write) to those who need it without interruption or onerous access restrictions.

Redundant systems, data recovery, disaster planning, UPS, backup power systems, redundant network connections.

e.g. “Fail open” authentication systems have been DDOSed (loss at availability) to allow attackers to bypass access restrictions (break confidentiality)

Repudiation

Authenticity

Enforcing commitments, contracts, agreements.

The internet has no fundamental way of managing this.

Not designed for commerce, access control (paywalls) or even uploads.

Information Security Measures

Policy

What data needs to be protected and in what way

Password

Roles and responsibilities

Access controls

Measures

Technical (hardware or software – e.g. encryption/firewall)

Organisation (staff, team responsibilities)

Human (training)

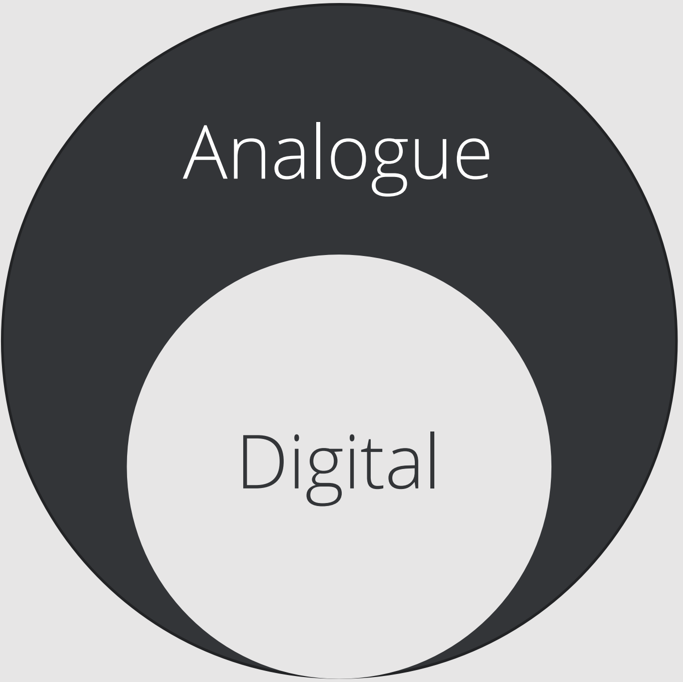
Physical (Access control)

Information Security

Information Security

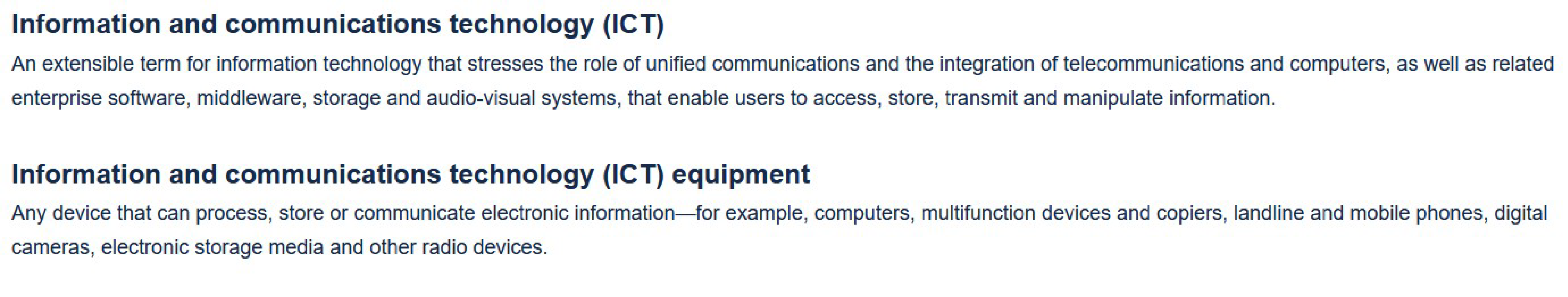
Practices to keep data secure, defined in properties data should have CIA

"The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability."



Information and Communications Technology

From our government definition and a little extra

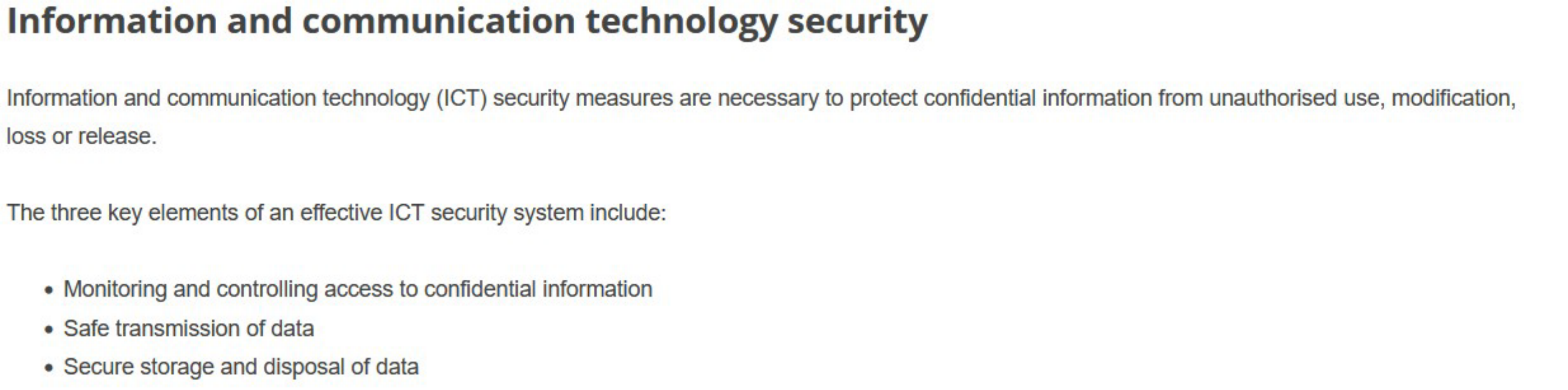


Information and communications technology (ICT)

An extensible term for information technology that stresses the role of unified communications and the integration of telecommunications and computers, as well as related enterprise software, middleware, storage and audio-visual systems, that enable users to access, store, transmit and manipulate information.

Information and communications technology (ICT) equipment

Any device that can process, store or communicate electronic information—for example, computers, multifunction devices and copiers, landline and mobile phones, digital cameras, electronic storage media and other radio devices.



Information and communication technology security

Information and communication technology (ICT) security measures are necessary to protect confidential information from unauthorised use, modification, loss or release.

The three key elements of an effective ICT security system include:

- Monitoring and controlling access to confidential information
- Safe transmission of data
- Secure storage and disposal of data

https://www.cyber.gov.au/acsc/view-all-content/glossary
https://statisticaldataintegration.abs.gov.au/topics/secure-data-management/information-and-communication-technology-security

What’s Vulnerable

Through the use of ICT

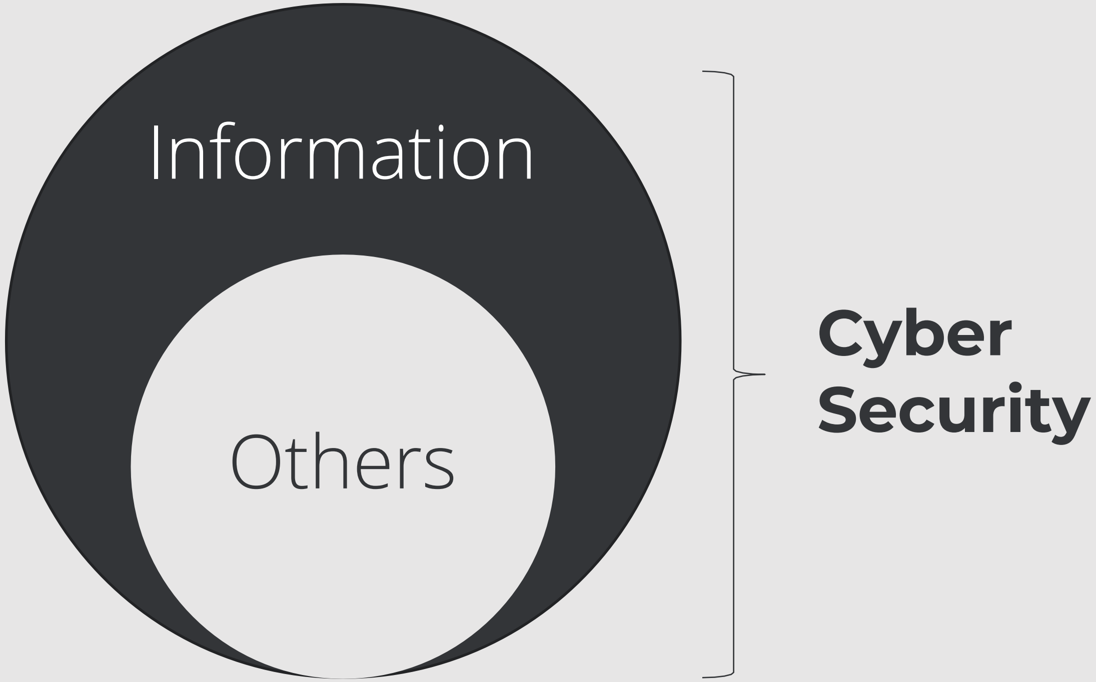
Information assets

Non-Information based assets

Remember ICT is processes, storage or communication of electronic information which can be edited, manipulated, displayed

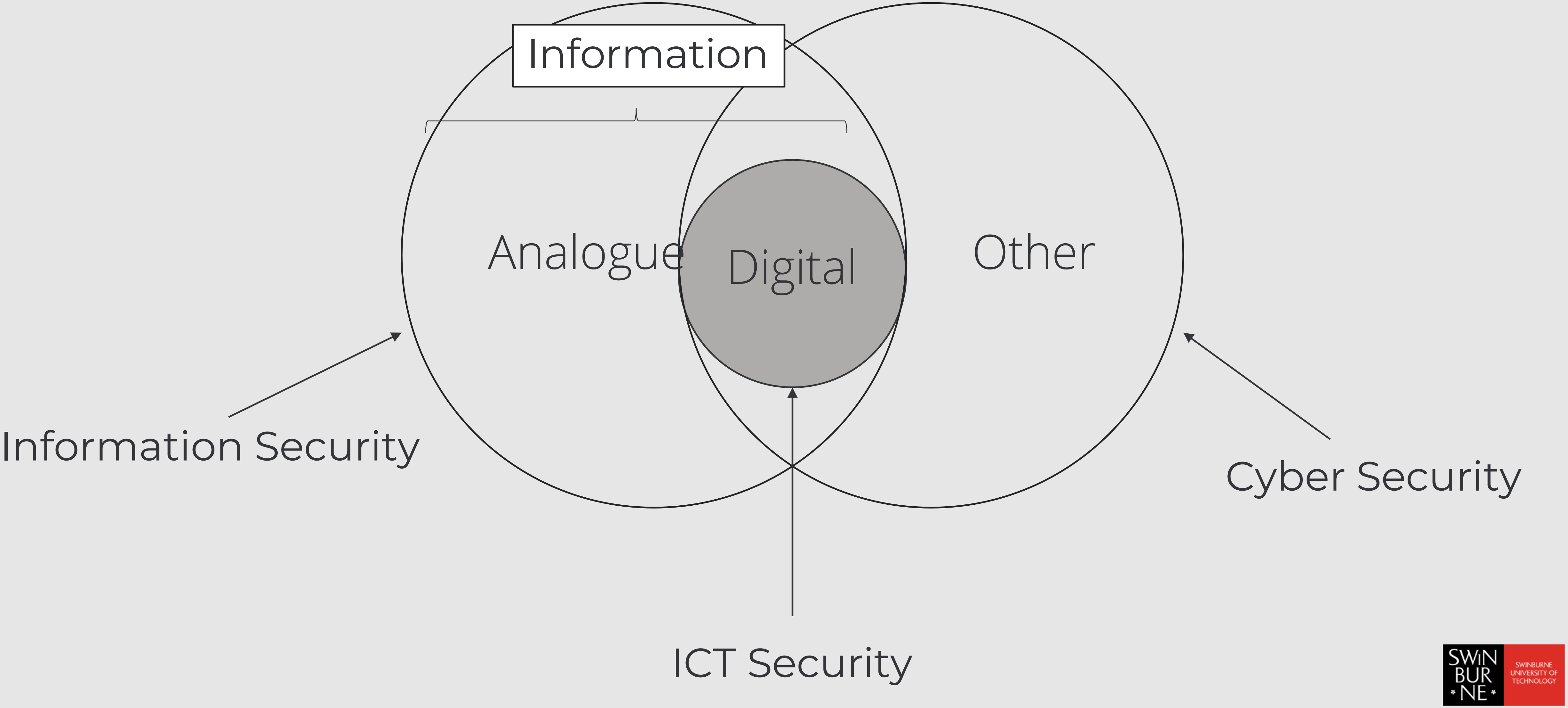
What could others mean here?

- Inspecting webpages for a phishing attempt
- Malware detection
- Inspecting traffic for known indicators
- …



https://www.cyber.gov.au/acsc/view-all-content/glossary
https://www.itgovernance.co.uk/what-is-cybersecurity

All Together



* Security

Information Security

Information assets (stored or transmitted) ≠ using ICT

Computer Security / ICT Security

Monitor and control access to information

Safeguard transmission

Secure storage and data disposal

Cyber security?

Non-Information based assets = using ICT [vulnerable]

Information based assets

Definitions

Cyber security?

Information Security, ICT Security?

A blend?

Magic?

Aus Gov Glossary

Measures used to protect the confidentiality, integrity and availability of systems, devices and the information residing on them.

Industry

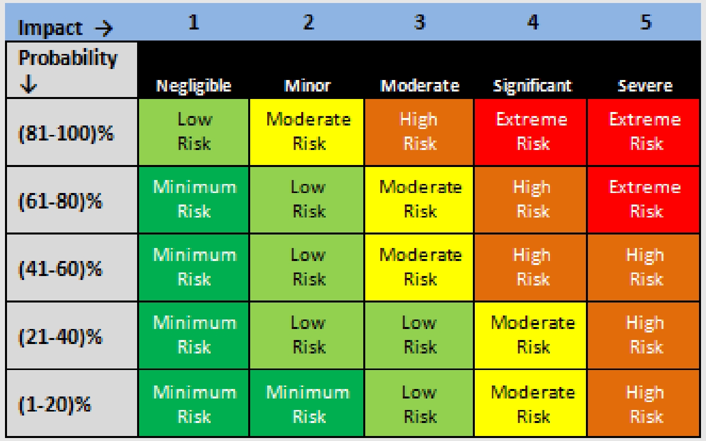
Cyber security is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks.

It aims to reduce the risk of cyber attacks and protect against the unauthorised exploitation of systems, networks and technologies.

https://www.cyber.gov.au/acsc/view-all-content/glossary
https://www.itgovernance.co.uk/what-is-cybersecurity

Security paradigms

- **Probabilistic Risk Analysis**
  - Assess the probability and severity of known* attacks against targets.
  - Risk factor = pr(Risk) * pr(Severity) for each target.
  - Allocate protection budget to highest risk factor target.
- **Doesn't work because:**
  - Criminals change the risk probabilities by studying the protection schemes and attack (many of) the least protected/probable targets.



Impact →	1	2	3	4	5
Probability ↓	Negligible	Minor	Moderate	Significant	Severe
(81-100)%	Low Risk	Moderate Risk	High Risk	Extreme Risk	Extreme Risk
(61-80)%	Minimum Risk	Low Risk	Moderate Risk	High Risk	Extreme Risk
(41-60)%	Minimum Risk	Low Risk	Moderate Risk	High Risk	High Risk
(21-40)%	Minimum Risk	Low Risk	Low Risk	Moderate Risk	High Risk
(1-20)%	Minimum Risk	Minimum Risk	Low Risk	Moderate Risk	High Risk

Security paradigms

- **Perimeter security**
  - Encase the LAN with firewall / IDS / IPS to prevent any nasty stuff from getting in.
  - Referred to as "M&M security”
  - Hard outer shell, soft middle.

- **Doesn't work because:**
  - If malware gets past perimeter, all computers become compromised. e.g. US drones
  - phishing attacks, social engineering, insiders, XSS, VPNs
  - managers who are “too important” to follow procedure/policy.

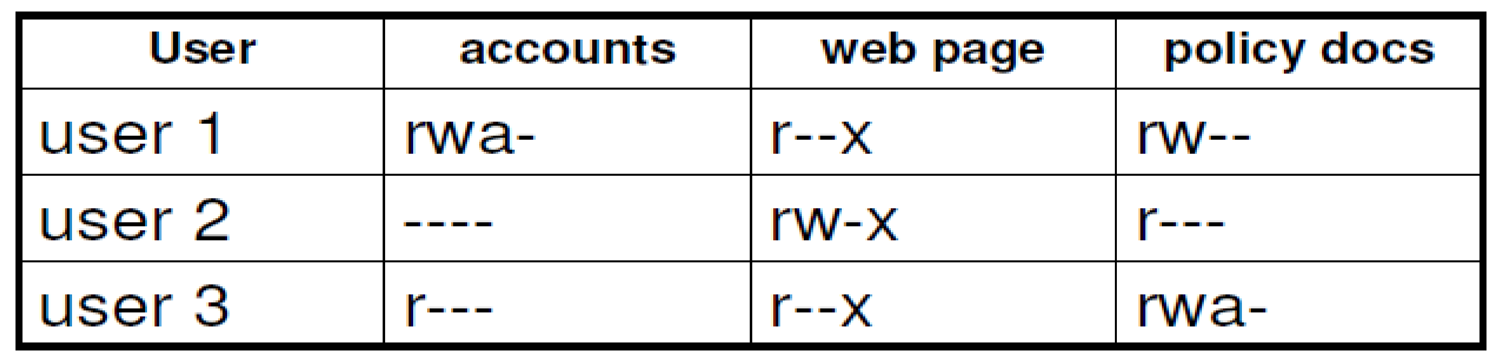
Security paradigms

- **Security policy**
  - Accidental damage or vulnerabilities may be introduced by insiders, management, visitors.
  - To reduce the chances of your network users compromising the network, tell them what they are allowed to do!
  - Make sure that they understand what they are not allowed to do.

  - https://www.swinburne.edu.au/about/leadership-governance/policies-regulations/procedures-guidelines/acceptable-use-guidelines/

Security paradigms

- **Access control / User Rights Management (ACLs)**
  - ➢ Both Windows and Linux support this complicated method of enforcing security.
  - ➢ Individual files / directories are tagged to allow/disallow file execution, reading, writing for different user groups.
  - ➢ Users are groups according to their roles / normal activities and privileges.



User	accounts	web page	policy docs
user 1	rwa-	r--x	rw--
user 2	----	rw-x	r---
user 3	r---	r--x	rwa-

Security paradigms

- **Reactive security / Black listing**

default allow

- ➢Used for default installations of Windows (including Vista) and Linux assume there is only one user who is the system administrator.
- ➢All activities (and types of network traffic) are allowed.
- ➢Rules are added / ports are closed when a problem / incursion occurs.
- ➢Black-listing of known threats

- **Doesn't work because:**

➢ 0-day attacks are not known; not on black list.

Security paradigms

- **Proactive security / White listing**

  default deny

  - All unknown activities / ports / software are blocked until an administrator allows them.
  - Allowed activities / ports / software are white-listed

- **Hard to implement:**

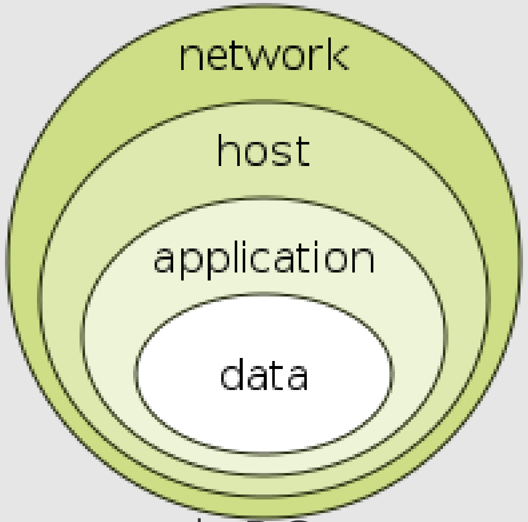
  - push-back from users, managers, CEO.
  - Requires open-minded, responsive and agile ISOs

Security paradigms

- **In Practice…**
  - Some blacklisted things
  - Some whitelisted things
  - Unknown threats slip through undetected.
  - Different policies for different resources (segmentation)
  - High-value targets are default deny, ACL;
  - Low value targets are default allow, daily re-image of SOE to minimise threat from 0-day attacks.
    - Persistent malware can defeat this
  - Need Defence in Depth because no single control is effective.

Security paradigms

- **Defence in Depth – can be based on ISO/OSI layers**
  - ➢ Sanitise input data, filter output data
  - ➢ ACLs, restricted rights to prevent unauthorised insiders / intruders.
  - ➢ AV / AntiMalware on all boxes
  - ➢ IPS, DMZ, network firewall, subnet firewalls, software firewalls on each PC.
  - ➢ Physical security + screening of employees


network
host
application
data