ICA Africa Programme
Programme pour l'Afrique

ICA Training Programme
Programme de Formation

Digital Records Curation Programme

Week 6:
Information Security

Digital Preservation Class Recap

What did you learn?

Learning outcomes:

At the end of this class you will be able to:

- understand that information security has physical and digital components
- identify the techniques that can be used to secure digital information
- encrypt and decrypt digital records

Physical information security

"… the common ground between physical security and information security" (Wikipedia)

Guards against theft, damage, unauthorised access to and/or removal of information

"Physical security protects people, data, equipment, systems, facilities and company assets [through] site design and layout, environmental components, emergency response readiness, training, access control, intrusion detection, and power and fire protection" (Harris, 2013).

Physical information security threats

Include:

- Malicious (theft, arson)
- Accidental (lost, damaged property)
- Natural (fire, flooding)

Risks

- Theft/loss of equipment, supplies
- Infiltrating flash drives or electronic devices into organisation
- Unauthorized access
- Equipment burnt or fire/water damaged
- Loss of power or connectivity (and therefore access to computer equipment)
- Inability to access premises

Physical information security measures

- Prevention (good security, good housekeeping, regular review and testing of procedures)
- Detection (fire and flood detectors, access sensors, systems and alarms)
- Mitigation (Personnel, procedures & equipment to stop and address damage – fire extinguishers, water pumps)

Business continuity and disaster recovery plans are an important defence and all aspects of physical information security require specialised knowledge and skills

Group Work – Classroom Audit

Work in groups to conduct an audit of the classroom to identify how its physical information security could be improved.

Digital aspects of information security

- “The protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide” (Wikipedia)
- Refers to non-physical security of computer systems and content or data

Attacks/vulnerabilities

- Digital information is at risk from vulnerabilities of humans and within computer programmes and systems as well as attacks on them
- Includes:
  - Malware (software that causes harm to programs and data)
  - Trojans (conceal malicious code within ostensible useful application)
  - Phishing (deceiving users into supplying sensitive information)
  - Spoofing (masquerading as valid entity using false data such as username)
  - Direct-access attack (unauthorized user gaining physical access)
  - Denial of service (system unavailable to intended users)
  - Backdoor (secret by-pass of cyber security)
  - Human gullibility and carelessness

Defence and protection

- Defence in depth (layers of security measures, physical and electronic)
- Security by design (security is a priority in system development)
- Security architecture (security controls documented and maintained as part of system architecture)
- Firewalls (to monitor and control network's incoming and outgoing traffic)
- Encryption (conversion of data into code to prevent unauthorised access)
- Usernames linked to permissions (to control access)
- Passwords (to control access to systems and documents)
- Two-factor authentication (two secure pieces of information)
- End user security training
- Policies and procedures

UK National Cyber Security Centre's 10 steps to cyber security

1. Defining (and communicate) the organisation's Information Risk Management Regime
2. Secure configuration of technology systems
3. Security policy and procedures for mobile working or remote access to systems – for users and service providers
4. Security incident management policy and procedures
5. Malware prevention
6. Managing user privileges
7. Monitoring attempted attacks on systems
8. Network security (including Wi-Fi access)
9. Removable media controls
10. User education and awareness

Collaboration

- Cyber-security is a very specialised and rapidly-changing field of expertise
- Work with your IT colleagues
- Key recordkeeping tasks:
  - Deletion of records when they reach their retention limit
  - Identification of records with sensitive information so as to protect them appropriately

Working in Pairs – Passwords and Encryption

- Use ‘John the Ripper’ software to assess the ease of cracking some sample passwords.

- Work in pairs to encrypt, exchange and decrypt digital records using BitLocker or similar free encryption software.

Conclusion

- Information security requires physical protection measures
- It requires risk assessment and management
- Cyber-security is a specialised and changing field of expertise
- Recordkeeping professionals need to work with IT colleagues

Any questions?