Joint Universities Computer Centre Limited (“JUCC”)

Information Security Awareness Training - Session Three

End User Security, IS Control Evaluation & Self- Assessment

Portable Storage Media and Internet Storage Handling

Agenda

- Portable and Internet Storage
- Vulnerabilities
  - Loss of Portable Storage Media
  - Security Breach of Internet Storage
  - Consequences
- Best Practices
  - Data Encryption
  - Access Control
  - Proper Data/ Media Disposal
  - Portable and Internet Storage Management

Examples of portable and Internet Storage

- USB flash drives
- Portable hard drives
- Smart phone
- Tablet
- Data disc (e.g. CD, DVD)
- Web-based file hosting service
- FTP file servers
- Email server

How vulnerable?

Data loss statistics

- Portable media theft/ loss is the 2nd major reason causing incidents of data loss

By cause of data loss: number of records/people affected since 2007 (to June 2010)

Incident Type	Number of people affected
Improper disposal	77,769,077
Hard copy theft/loss	1,361,008
Portable media theft/loss	114,192,269
PC loss	598,577
PC theft	13,852,948
Hacking	249,351,765
Malicious insider	23,521,995
Malware	67,815
Web/network exposure	23,356,796
Human/system error	8,297,740
Unknown	1,352,334

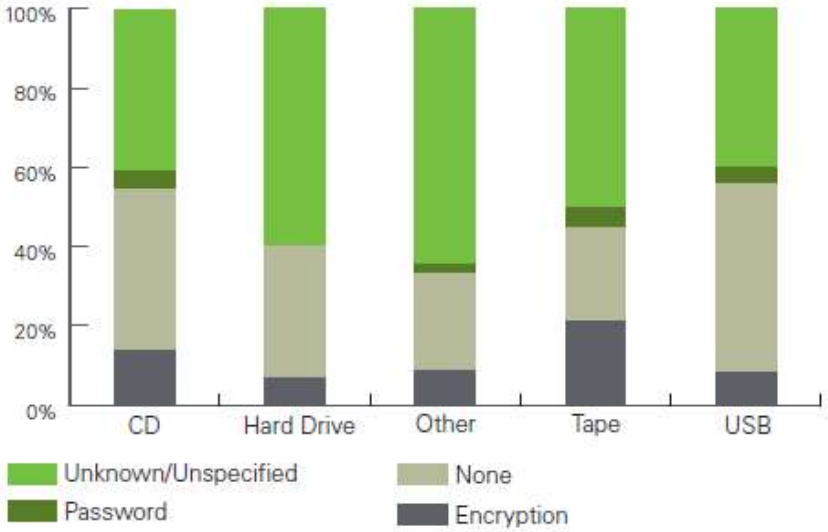
Source: KPMG International, October 2010

How vulnerable?

Data loss statistics

- Among all incidents, for 20-40% of the time, portable media are not securely protected

Portable media v Security protection: number of incidents related to portable media as % of total since 2007 (to June 2010)



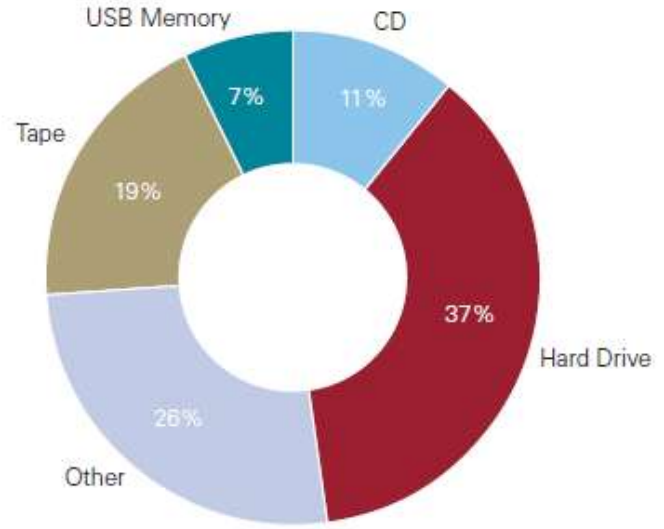
Source: KPMG International, October 2010

How vulnerable?

Data loss statistics

- Over a third of reported data lost through portable media has involved hard drives

By portable media: number of portable media incidents as % of total for 2010 (January-June)



Source: KPMG International, October 2010

University of Arizona Losses Drive Containing Personal Information on Thousands

Issue

- The University of Arizona lost a hard drive containing the personal information of former students

Consequences

- Enrolment information such as Social Security numbers of over 8,000 former students were lost

Vulnerabilities

- Human error
- Lack of encryption
- Inadequate user IT awareness and security measures

Dropbox security breach: accounts of 25m users unlocked for 4 hours

Issue

- Dropbox, a leading file-hosting service, turned off its password security system for 4 hours caused by a programmer’s error and users could log-in using any password

Consequences

- Accounts of 25 million users of the service were accessible to visitors of the site
- Users’ job-related and private files, images and videos in Dropbox were openly accessible

Vulnerabilities

- Human error
- A software bug that rendered the service's authentication mechanism non-functional

Security Breach of Internet Storage

Do you know the Terms of Service?

Limitation of Liability

TO THE FULLEST EXTENT PERMITTED BY LAW, **IN NO EVENT WILL DROPBOX**, ITS AFFILIATES, OFFICERS, EMPLOYEES, AGENTS, SUPPLIERS OR LICENSORS **BE LIABLE FOR** (A) ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, EXEMPLARY OR CONSEQUENTIAL (**INCLUDING LOSS OF USE, DATA**, BUSINESS, OR PROFITS) DAMAGES, REGARDLESS OF LEGAL, THEORY, WHETHER OR NOT DROPBOX HAS BEEN WARNED OF THE POSSIBILITY OF SUCH DAMAGES, AND EVEN IF A REMEDY FAILS OF ITS ESSENTIAL PURPOSE; (B) AGGREGATE LIABILITY FOR ALL CLAIMS RELATING TO THE SERVICES MORE THAN THE GREATER OF $20 OR THE AMOUNTS PAID BY YOU TO DROPBOX FOR THE PAST THREE MONTHS OF THE SERVICES IN QUESTION. Some states do not allow the types of limitations in this paragraph, so they may not apply to you.

(www.dropbox.com)

Consequences

- Acquisition costs of recovery facilities
- Loss of customers
- Destruction of brand reputation
- Litigation

“A company’s data is one of its most important assets, so even a SINGLE INSTANCE of data loss is significant”

Best Practices – Encryption

What is encryption?

Encryption is a process of **translating** a message, called the **plain text,** into an encoded message, a **cipher text** which **is non-readable to unauthorised parties**.

Best Practices

- **Centralise/ Approved** encryption key infrastructure/ services
- Use **standard/ approved cryptographic algorithms** and utilities
- **Back up keys** on a regular interval **to a separate protected, dedicated hardware device**

Data encryption management process

1. Identify data to be encrypted

- External requirement
- Internal procedures
- System and network environment
- Support limitation

2. Design a solution

- Cryptography
- Authentication
- Solution Architecture
- Policies and Procedures
- Deployment Plan
- Users' comments

Data encryption management process

3. Test a prototype

- Addressing requirements
- Testing of authentication
- Performance and compatibility test
- Recoverability
- Implementation of vulnerability assessment
- Collecting users' feedback

4. Solution deployment and monitoring

- Deployment
- Testing and applying patches
- Regular vulnerability assessment

Best Practices – Access Control

Protecting your own internet and portable media

Internet Storage

- Set user profiling and access rights
- Avoid storing organisation's information on public file-hosting websites

Portable storage

- Encrypt on both files and portable device with password authentication
- Do not leave storage devices unattended

Mobile device

- Apply screen lock and encryption
- Avoid using unauthorised applications

Common disposal methods for different types of data

Physical data

- **Cross-cut shredding** of media into small regular pieces
- **Disintegration** of media into small electronic units
- **Incineration** of media by burning
- **Pulverisation** of media into powder form

Common disposal methods for different types of data

Electronic data (reuse of media)

- **Sanitise** when it is no longer necessary for business use (Overwriting all previously stored data with a predetermined pattern of meaningless information, such as a binary pattern and an additional third pattern)
- **Degaussing** of magnetic media
- **Erasing/ overwriting** of media with secure deletion software

More on Sanitisation

•Apply different levels of sanitisation to different categories of data (with reference to university's own data classification and handling guidelines)

•For media that contains more than one classification of data, the sanitisation method selected should be **consistent with the most restrictive classification**

Data Classification	Disposal	Clearing and Sanitisation	Destroying
Public	✓	✓	✓
Private		✓	✓
Restricted		✓	✓

"Simple deletion and formatting is not sufficient"

Best Practices – Portable and Internet Storage Management

- **Records** - Keep records of information transferred to portable/ Internet storage
- **Assessment** - Assess whether information should be transferred to the portable/ Internet storage
- **Classification** - Implement appropriate controls and handling procedures according to the value, importance, sensitivity and protection requirements of data

Best Practices – Portable and Internet Storage Management

- **Guidelines** - Follow the guidelines provided by IT department for different data handling processes throughout the information lifecycle:

- **Creation and identification** (e.g.: define the HR record creation procedure and information asset inventory management procedures)
- **Access** (e.g.: define file access rights for each user profile groups in USB and shared file servers)
- **Use, transmission and storage** (e.g.: define how information saved on Internet storage is transmitted and used safely)
- **Transportation** (e.g.: establish procedures for transferral of backup tapes to off-site location)
- **Destruction** (e.g.: define how tapes, unused CDs and hardcopies of sensitive information are disposed of)
- **Breach disclosure** (e.g.: define the procedures and period for data breach disclosure)

Q&A

?

Copyright Statement