Information Security and Best Practices

Stephen Gough
Assistant Director of IT Services

10 November 2008
IT Supporters seminar – 4/2/08

- Information Security Policy
- Mike Roch
- https://www.reading.ac.uk/nmsruntime/saveasdialog.asp?lID=21223&sID=63947
Information Policy

- Autumn 2006
- “All information recorded within the scope of University activity is deemed a University record. Therefore staff have a duty to ensure appropriate keeping and/or disposal of all information they create and handle.”
- Information Strategy Cttee responsible for policy devt
- University management structures responsible for implementation (cf Health and Safety policies)
  - internal & external auditors to provide monitoring

Sub-policies

- Agreed Autumn 2007
  - Systems Planning Policy
  - Systems Management Policy
  - Systems Operation Policy
  - Software Management Policy
  - Communications Networks Management Policy
Information Security

• **CIA**

• **Confidentiality**
  – Can only the appropriate people read it?

• **Integrity**
  – Is the data all present and correct?
  – Could it be altered inappropriately?

• **Availability**
  – Can the appropriate people get to it when required?
Risk assessments

<table>
<thead>
<tr>
<th>PROBABILITY of security breach</th>
<th>IMPACT of security breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>× Lab PC</td>
<td>× Staff PC</td>
</tr>
<tr>
<td>High</td>
<td></td>
</tr>
<tr>
<td>× Student PC</td>
<td>× Dept Web Server</td>
</tr>
</tbody>
</table>

× FOCUS
Research data – audit

• What is being stored in your school?
  – Data audit to identify data assets & owners
  – Data Audit Framework
    • http://www.data-audit.eu/
    • Online tool coming
      – Can be used at inst/school/dept/research team levels

• What’s the value of the data?

• What are requirements of funding body?
  – Will probably need data kept available for years after end of project
Research data – risk analysis

• Risk
  – Of loss
    • Due to fire/theft/hardware failure/negligence

• Impact
  – Loss of funding
    • Possibly for whole University
  – Damage to reputation

• Decisions & actions
  – No single copies of data
  – Keep on properly managed & backed up server
  – Physically secure
School servers

• CIA – Confidentiality, Availability, Integrity

• Availability low for most school file servers
  – What if server had to be replaced?
    • How long without access to data?

• Availability high for central file servers
Central storage

• Quotas
  – UGs & taught PGs  200MB
  – Research PGs  2GB
  – Staff  3GB
  – Quota increase form

• Collaborative shares
  – [http://www.reading.ac.uk/closed/its/docs/facilities/Collaborative Fileshare.asp](http://www.reading.ac.uk/closed/its/docs/facilities/Collaborative Fileshare.asp)
  – CIFS only
  – Share per school, top-level folder per research group etc
  – Quota set on 5GB per top-level folder
    • Can ask for more
Central storage

- ITS Looking for some guinea pig depts/schools
  - Reasonably big data requirements (1-2TB)
  - No charge initially
  - Help determine storage regime
    - fast vs slow disk
    - backup
    - archiving
MoD admits another laptop stolen

The Ministry of Defence has confirmed another laptop containing "sensitive information" was stolen while an official checked out of a hotel.

An MoD spokesman said the theft from the Britannia Adelphi Hotel in Liverpool on Thursday brought the total number of laptops stolen to 659.

Probe into data left in car park

An inquiry has been launched after a memory stick with user names and passwords for a key government computer system was found in a pub car park.

Subcontractor Atos Origin, which lost the stick, said there had been a "direct breach" of its procedures.

It said the matter was being taken "extremely seriously" but the integrity of the website, which was closed for a short time, had not been compromised.

Prime Minister Gordon Brown said the company would have "to explain itself".

NHS memory stick found in street

An NHS trust has apologised after a computer memory stick, containing the confidential files of 200 patients, was found in a street.

Tees, Esk and Wear Valleys Trust said the stick was found by a member of the public in Barnard Castle, Co Durham.

It stored a summary of medical histories and patients' national insurance numbers and addresses.

The trust confirmed the stick was lost by a computer technician upgrading computers in Teesdale and Weardale.

Trust chief executive Martin Barkley said an investigation was under way into the "isolated incident".

But a spokeswoman for the Department of Work and Pensions said the device contained user names and passwords for testing an old version of the system, and all the information was encrypted.
Portable devices – advice at UCL

- Only store sensitive data on portable devices or media when absolutely necessary
  - In nearly all cases it is not necessary and not advisable for UCL staff to store sensitive data on portable devices or media. If there is a need to work with sensitive data away from UCL premises, the preferred method is to use a secure remote connection to UCL, which allows access to the data via an encrypted stream of traffic; this avoids storing a copy on the client machine. All UCL users have access to WTS, which provides such a connection. Where available, Virtual Private Networks (VPNs) can also provide a secure remote working environment.

http://www.ucl.ac.uk/cert/GuidanceStorageSensitiveData.html
Portable devices

• But, they will be used, so…
  – Physical security
    • Keep laptops locked to desks in offices
    • Keep laptops in car boots and not in view
  – Think about what’s stored on the device
    • Should the data be removed from the University at all?
    • Is it confidential/sensitive?
  – Encryption if necessary
    • Last line of defence
    • SafeStick secure memory sticks
      – http://www.blockmaster.se/
    • Verbatim - Store'n'Go USB Drives
    • Carry it Easy Plus (from CoCoSys)
Portable devices & media policy

- Add to other sub-policies
- What are the issues?
  - assess risk
  - value of data
  - what should be stored centrally
  - what types of data should not normally be stored on portable devices
  - encryption
  - recommendations of easy to use devices
Portable devices & media policy

- Guidelines and good practice for using mobile devices
  - from UCISA Information Security Toolkit, 3rd Edition
  - Personal computers should not be used at home for business activities if virus controls are not in place.
  - When travelling, equipment (and media) should not be left unattended in public places. Portable computers should be carried as hand luggage when travelling.
  - Time-out protection should be applied.
  - Portable computers are vulnerable to theft, loss or unauthorised access when travelling. They must be provided with an appropriate form of access protection (e.g. passwords or encryption) to prevent unauthorised access to their contents.
Portable devices & media policy

- Passwords or other access tokens for access to the organisation’s systems should never be stored on mobile devices where they may be stolen and give the thief unauthorised access to information assets.
- Manufacturer’s instructions regarding the protection of equipment should be observed at all times, e.g. to protect against exposure to strong electromagnetic fields.
- Security risks (e.g. of damage, theft) may vary considerably between locations and this should be taken into account when determining the most appropriate security measures.
References

- UCISA Information Toolkit, Edition 3.0
  - [http://www.ucisa.ac.uk/publications/ist.aspx](http://www.ucisa.ac.uk/publications/ist.aspx)

- University of Essex – Best Practice In Electronic Information Security, Guidance For Desktop Users
  - [http://www2.essex.ac.uk/iss/policies/security_guidance.htm](http://www2.essex.ac.uk/iss/policies/security_guidance.htm)

- Imperial College – Information Systems Security Policy - Code of Practice 11: Security of Small Portable Devices and the Data Stored Therein