



University of Salford
A Greater Manchester University

Data Security For Education Institutions: A View From The Sharp End



John Kelly – Network & Telecom Operations Manager



The University Of Salford

Facts & Figures

- 40 Buildings
- 3500 Staff
- 22,000 fte students
- 9,000 active host devices on the network
- Approx 3000 telephone extensions



Data Security Issues?

Taxman loses sensitive personal data on 25m people

(The Times, November 20th 2007)

Government warned over data-transfer security

(ZDNet.co.uk, 30th July 2007)

NHS patient data sold on eBay (ZDNet.co.uk, Sept 17th 2007)

Nationwide fined £1m for laptop theft (ZDNet.co.uk, Feb 14th 2007)

County council hit by laptop theft (ZDNet.co.uk, Feb 28th 2007)

TJX Companies breach - 45.7 million customer accounts compromised.

Salesforce.com breach – Employee gave away corporate login details to phishers, who then stole a customer contact list.



Data Security: Why Worry?

- The Data Protection Act 1998
 - Any organisation that processes personal information must comply with eight principles, which make sure that personal information is:
 - Fairly and lawfully processed
 - Processed for limited purposes
 - Adequate, relevant and not excessive
 - Accurate and up to date
 - Not kept for longer than is necessary
 - Processed in line with your rights
 - Secure
 - Not transferred to other countries without adequate protection
 - A data controller who persistently breaches the Act and has been served with an enforcement notice can be prosecuted for failing to comply with a notice. This offence carries a maximum penalty of an **unlimited** fine in the Crown Court.



Data Security: Why Worry?

- JANET Acceptable Use Policy (AUP)
 - Section 9.7: Unacceptable Use includes:
 - corrupting or destroying other users' data;
 - violating the privacy of other users;
 - disrupting the work of other users;
 - using JANET in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
 - other misuse of JANET or networked resources, such as the introduction of "viruses".



Who & What Do You Trust?

- Threats are everywhere!
- Technology:
 - External access (Internet Based)
 - Wireless networks
 - USB drives & removable media
 - Mis-configured/un-patched servers
- Human:
 - Untrained staff
 - Bored students
 - Malicious attackers
- Don't trust anything or anyone.....



It Starts At The Top

- Essential that the Senior Management Team of the organisation “buy-in” and support security measures
- Acceptable Use Policy
 - Everyone agrees (even if they don’t read it!)
 - Review it – every year at a minimum.
 - Clear statement of sanctions (and follow through with them)
- Data Management Procedures
 - Who should be accessing what
 - How information is stored and referenced
 - How information transfers should be handled
 - How old information is disposed of
- Security Team
 - Full time Security Officer
 - Perform investigations and implement solutions
 - Needs to be trusted and empowered



What Do You Need To Secure?

- Do you know what services are out there?
- Service Registration process
 - Find out what is out there and who it belongs to
 - Who needs to access each service and where from?
 - Who is responsible for the data on the server?
- Client Audit
 - What sort of clients are connecting?
 - How are they connecting?
 - What are they doing with the data?



How Do You Secure It All?

- Assume all clients are insecure
 - Treat clients inside your network the same as Internet based ones
 - Ring fence your critical services with firewalls
 - Defence in depth
- Monitor what is happening
 - Check log files for unusual activity
 - Consider penetration testing of secure systems
- Procedures
 - Document every process



Physical Security

- Who has physical access to the hardware? Who should?
- Portable devices – ensure data stored on laptops is protected by more than a password
- 3rd parties – who is responsible for contractor access?



Maintaining Security

- Making Changes
 - Consider a Request For Change (RFC) system
 - All changes affecting security are assessed by peers
 - Changes authorised by Heads of Service
- New Projects
 - Ensure that security is designed in from the start
 - Involve suppliers
 - Learn to say no!
- Monitoring & Testing
 - Perform regular security testing
 - Patch management



Finally.....

“You cannot trust any agency with people's personal data.”

- Frank Abagnale, quoted in the Daily Telegraph.