Research Data Security

*P**aul Kennedy***

IT Services

Is information security important to RDM?

- *"EPSRC recognises that there are legal, ethical and commercial constraints on release of research data. To ensure that the research process (including the collaborative research process) is not damaged by inappropriate release of data, research organisation policies and practices should ensure that these constraints are considered at all stages in the research process."*
  - *EPSRC, Policy Framework on Research Data Management, Principle ii*

- *"Research organisations will ensure that effective data curation is provided throughout the full data lifecycle … the full range of responsibilities associated with data curation over the data lifecycle will be clearly allocated within the research organisation, and where research data is subject to restricted access the research organisation will implement and manage appropriate security controls;"*
  - *EPSRC, Policy Framework on Research Data Management, Expectation viii*

Is information security important to RDM?

- *"All new research proposals must include research data management plans or protocols that explicitly address data capture, management, information security (specifically integrity and confidentiality), retention, preservation, sharing and publication."*
  - *UoN, Research Data Management Policy, Clause 1.3*

- *However, the level of information security required will depend on:*
  - *The risk level associated with the data*
  - *The complexity of the equipment and IT resources required to process and analyze it*
  - *The needs of the school or research group*

What risks are there for research data?

- *Attacks are no longer undertaken primarily to show technical skill and to gain kudos with fellow hackers*
- *We can be a target just because of who we are or what we say.*
    - *UEA Climate Research Unit Attack*
    - *GhostShell attack against World's top 100 Universities*
- *There's money to be made in e-Crime*
- *Global companies and nation states want your intellectual property*

What risks are there for research data?

- *"Cyber security is one of the biggest challenges facing our organisations and the economy today, and the threat is directly relevant for universities. This relates particularly to the theft of intellectual property, the undermining of the UK's research base, and the jeopardising of the economy. Universities need to be aware of the risks surrounding cyber security, and to put in place a few simple measures which can increase their resilience and reduce the vulnerability of information assets being compromised."*

  – *Cyber Security, Protecting Universities from the Cyber Threat, Universities UK Policy Briefing,* 23 July 2012

Advanced Persistent Threat

- "***Advanced persistent threat*** *(**APT**) usually refers to a group, such as a foreign government, with both the capability and the intent to persistently and effectively target a specific entity. The term is commonly used to refer to cyber threats, in particular that of Internet-enabled espionage using a variety of intelligence gathering techniques to access sensitive information, but applies equally to other threats such as that of traditional espionage or attack. Other recognized attack vectors include infected media, supply chain compromise, and social engineering."*

  – *Wikipedia (Sorry!)*

Advanced Persistent Threat

What are we doing?

- *Nationally, the Russell Universities IT directors (RUGIT) and IT security managers (RUGIT IT Security group) are working with UUK and the Centre for Protection of National Infrastructure (CPNI) on a set of information security controls for HEIs.*
- *CPNI already has a "Top 20 critical security controls" for its primary constituents (Energy, Transport, Communications, Emergency Services, Health, Finance etc).*
- *However, these may work best in corporate organisations, so the RUGIT IT security group (chaired by Nottingham) is working with CPNI to define a version of the top 20 controls suitable for HEIs.*

What are we doing?

- *Locally, a research data security working group between RKTB and IS has developed:*
  - *The research data management policy*
  - *A data classification schema to help classify confidential research data*
  - *A data breach reporting policy*
  - *Security guidance for researchers*
- *These have been approved by Management Board along with recommendations that:*
  - *"Schools and departments create an inventory of confidential or highly confidential data which they create, process or store as part of their research activities and review the data security measures in place to protect these from inappropriate access, data loss or data breach."*
  - *"All research staff and postgraduate research students undertake periodic data protection awareness training to understand their responsibilities when handling confidential or highly confidential data."*

Security Support Already Provided!

- **Network Security**
  - Enterprise-class perimeter firewalls
  - Enterprise-class internal firewalls (for specific systems)
  - Enterprise-class anomaly detection network monitoring solution
  - Off-campus managed email filtering service
  - Enterprise-class secure web proxy
  - Encrypted wireless local area network service
  - Virtual Private Networks
  - Network access control solution (student network only)
  - Network access monitoring solution (main campus network only)
  - Network bandwidth management service (student network only)
- **Operational Security**
  - Centrally-managed anti-virus client
  - Centrally-managed patching service for Windows computers
  - Central logging service
  - Centrally-managed digital certificate service
- **Access Control**
  - Identity and Access Management system provides “cradle to grave” user account management. Account creation and deletion controlled by sources of authority
  - University username and password authentication required for access to centrally provided IT services
- **Physical Security**
  - Server hosting & Data Centre access controls (keypad and/or card access system)

New Security Support for 2013-14

- *Centrally supported encryption service*
- *Guidance on doing a high risk data inventory and the data classification schema*
  - *Trial of the DCC Data Asset Framework (DAF) with CHS*
- *Online data protection awareness training through Moodle*
  - *General course for everyone in the organisation*
  - *Additional module specifically for research data*

Longer Term

- *Adoption of ISO 27001 the international standard for Information Security Management Systems*
  - *This standard contains 133 separate information security controls so will take 2-3 years to fully deploy*
  - *NHS, government and industrial partners usually reference this standard in their security questionnaires*
  - *Not yet mandatory and only a handful of Universities have adopted it so far*
  - *However, we now have one teaching contract with the Department of Education for which it is mandatory*
  - *Likely to be become mandatory for research sometime in the future*
  - *Early adoption may give us a competitive advantage when bidding for (some) research funds*

Questions?

For more information contact:

is-security-support@nottingham.ac.uk

or

Paul Kennedy

Ext 67648