Research Data Management: Information Security guidelines

"Data, including electronic data, must be recorded in a durable, secure and retrievable form… Appropriate data security should be applied based on a systematic assessment of security and risk"

Code of Practice for Research at the Open University, July 2013

Contents

1. Introduction

"Why is information security important?"

Information security enables you to control who has access to your research data and to determine, and keep track of, what others are authorised to do with your data. If you lose your data recovery could be slow, costly or even worse, it could be impossible. Furthermore, academic research often results in the creation of sensitive data which, if released, could be damaging to your reputation or that of your institution.

Adopting appropriate security measures will help protect your data from:

- Breaches of confidentiality, which could result in reputational damage, claims because of loss of intellectual property and damage to research subjects
- Failures of integrity (i.e. the accuracy and consistency of data), which can undermine research credibility
- Interruptions to the availability of data, which can impact on the research process
- Loss through accidental or malicious damage, modification or theft

"What is the University doing to maintain information security?"

The good news is that the University is constantly monitoring and re-evaluating the risks associated with Information Security and where necessary takes steps to ensure a continued safe and secure computing environment at the University. Some of these measures include:

- IT managed Antivirus Software on desktop computers
- IT managed vulnerability management program
- IT managed email filtering solution
- IT managed network protection technologies (e.g. Firewall)
- Secure Wireless Access Points
- Encryption solutions to protect sensitive University data

In addition to the security practices implemented behind the scenes the University has published a number of Information Security policies which mandate a number of good security practices to be adhered by all users working at the University which further help to prevent the University, or computer users from becoming a victim of cybercrime.

.

2. General security advice to complement your ways of working

"What can I do?"

This set of guidelines should be a good starting point for adopting appropriate security measures for your research data. Including any data security measures you will be taking in your Data Management Plan will help you to make sure you are protecting your data throughout your research project.

If you need further advice or support with any information security issues, contact the Information Security Team.

2.1. Information Classification

An essential starting point when determining the most appropriate security is understanding how important the information / data you wish to protect is. To help assess this, the University has published an Information Classification Policy which defines four levels of classification which must be referenced when classifying information at the start of any research project. Thereafter it is important to:

- Identify and manage any risks involved with storage of your data
- Highlight any needs for special equipment or resources
- Plan your data management strategy effectively

2.1.1 Examples of Research Data

You may find it helpful to consider the following examples of research data when classifying your own data; however your research project is likely to have its own particular security issues, so if you need help classifying your data then contact the Information Security Team.

Highly Confidential research data

- Details relating to identifiable individuals, the contents of which have the potential to cause damage or distress (NB. This could include contact details in a database).
- Data relating to an identifiable individual's sensitive personal details, i.e. health, disability, ethnicity, sex life, political or religious affiliations.
- Data concerning any identifiable vulnerable individuals.
- Large datasets of identifiable individuals (including data not of a sensitive nature, due to potential to cause the research project/university reputational damage).
- Data that could affect contracts with commercial or other partners.
- Information that could compromise patent applications.
- Any data that is the result of an un-repeatable study.

Proprietary research data

- Project documents and records that contain staffing, financial or contractual information.
- Small datasets of identifiable people's personal lives, where the data is not distressing or sensitive and where the individuals are not in a vulnerable group.

Internal use only research data

- Analysed data that would take significant time and effort to reconstruct.
- Internal project notes and documents

Public documents

- Research data, the loss or exposure of which poses no risk to the reputation or finance of the University.
- All published research data.

2.2 Storing data securely

2.2.1 During your project

The best place to store your data while you are working on it is on the University's centralised network file storage which is securely managed by the IT department.

Although the use of centralised University storage options are recommended you may have additional requirements and wish to store data on USB memory sticks, portable hard drives or optical media such as CD's or DVD's.

Information classified as Proprietary or Highly Confidential must be stored in an encrypted format when using portable storage media. To facilitate the requirement University computers will automatically prompt to encrypt portable storage media when such a device is connected to a University computer.

Where alternative 3rd party computer solutions (for example: 3rd party supplier, home computer) are utilised to for the storage of University data please refer to the encryption section for guidance.

2.2.2 Post-project

One of the aims of the University's current Research Data Management Project is to develop a solution to facilitate easy and secure long-term storage of the University's research data.

In the meantime, contact IT Services who may be able to offer storage for your data.

Alternatively, directories such as Databib, DataCite and re3data can help you find an external repository in which to store your data.

When choosing a storage solution for your data, you should ensure that the facilities provide:

- Adequate space for all the records which need to be retained
- Appropriate security measures to control access to the records
- Comply with the Data Encryption policy for data classified as Proprietary and Highly Confidential
- Comply with the Secure Cloud Computing Policy
- Appropriate environmental conditions for the record media used

2.3 Data Encryption

The University's Encryption Policy requires that information classified as Proprietary or Highly Confidential is encrypted when it is transmitted over the Internet or stored at a third party – this includes any storage medium used on a home PC.

If you are using a web browser to transfer information simply look for the padlock icon in the right hand corner the address bar. If visible this indicates encryption is enforced and the data may be transferred. If web solutions are not available to facilitate data transfers please ask the IT department for assistance.

For the storage of sensitive data outside of the University it is first necessary to ensure encryption is utilised. The University has an encryption solution for USB sticks when used on campus to copy data.

If you store sensitive information on your home computer consider using whole disk encryption solutions which automatically encrypt all data on the hard disk. Some versions of Windows 7 & 8 include Bitlocker which can facilitate this, or alternatively you may wish to consider using alternative software such as TrueCrypt which offers similar functionality.

2.4 Remote Access

The University provides secure remote access facilities which allow you to remotely access your work computer from a remote location. This way of working is preferred as you will continue to benefit from the inherent IT security employed at the University. For further information on Remote Access please consult IT's intranet pages on VPN Services.

When working remotely, these simple tips will help you to keep the device used for remote access secure.

- Use passwords to lock your device when not in use
- Ensure that the screen is not visible to others while you are working with sensitive data in a public place
- Ensure that your equipment is protected with anti-virus software
- Keep your device up to date with all recommended security updates when they are published by software vendors

- Keep your device physically secure, by locking it away to help protect from loss / theft.

For more information on accessing your data offsite please consult the Remote Access Policy.

2.5 Online cloud services (Dropbox, Skydrive, Livedrive, etc.)

While it's preferred that University storage solutions are utilised wherever possible it's recognised that in certain circumstances Cloud based solutions such as Dropbox and SkyDrive might be a preferred alternative solution.

University Information classified as Proprietary or Highly Confidential is not permitted to be stored in Cloud based solutions unless approved by IT. For all other information please consider the following before using such services:

- What guarantees does the service provider give that their service is secure? Is it certified to SSAE 16 or ISO 27001 standards which would provide assurance?
- What incident management process do they have in place in the event of a security breach? Would you be notified?
- Will your data be stored with other users' data, or is it kept separate?
- Do you know in what geographical location your data will be stored? Is there concern that foreign agencies may have access to the data?
- What would be the impact to you if the provider suddenly ceased operating and your data was unavailable?
- If you no longer wish to use the service how will you repatriate the data and ensure its secure destruction with the 3rd party?
- Is the third parties Service Level Agreement acceptable to the University?

2.6 Data transfer and collaboration

2.6.1 Within the OU

- The Open University's centralised network file storage enables sharing of documents between users.

Please note: More information on collaboration tools within the OU will become available throughout the course of the current Research Data Management project.

For advice on how to collaborate with colleagues within the OU, contact IT Service Delivery.

2.6.2 Outside the OU

Before you start…

- When collaborating with researchers outside of the OU it may be necessary to put into place a contract or agreement in order to determine the ownership, management and restrictions of use of shared information.

For more information on the legal aspects of research collaboration, consult RSQ's Legal Agreements factsheets.

How to collaborate…

One of the aims of the current Research Data Management Project is to develop a solution to facilitate easy, secure collaboration with external researchers.

In the meantime, IT can provide the following:

- Connectivity provisioned through approved Open University solutions (restricted to the IT resources required)
- Monitoring of third party connections for the detection and prevention of unauthorised access
- A central registry of all third party connections

2.7. Data retention and destruction

2.7.1 Data retention periods

For guidance on the retention periods of research data consult the OU's Guidelines for Selecting Research Data for Retention and Preservation and the Open University's Retention Schedule.

Remember, you should include information about data retention in your Data Management Plan.

2.7.2 Secure destruction of data

The following guidelines should help you to destroy your data securely:

- Destroy physical data with a shredder where appropriate
- Contact the IT Service Delivery team to dispose of any digital data classed proprietary or above

For more information on securely disposing of your data consult the Media Disposal Policy.

3. Information Security Incidents Policy

"What if something goes wrong?"

If you observe or suspect a security weakness in any Open University systems or you have any other concerns or problems contact the Information Security team.

4. Links

4.1 Links to related Open University resources

OU Principles of Research Data Management (2013)

Information Security Specific Policy Set (2013)

Information Security Charter (2012)

Code of Practice for Research at the Open University (2013)

Information and Records Management Policy (2010)

4.2 Links to other useful resources

JISC Information safety briefing paper (2005)

JISC Data Protection Code of Practice for the HE and FE sectors (2001)

MANTRA interactive training module on Storage and Security

RCUK Policy and Guidelines on Governance of Good Research Conduct (2011)

Isabel Chadwick
3rd February 2014

Appendix A: An overview of Information Security risks

Contents

1. Introduction

Information Security is an essential requirement in today's inter-connected and technology savvy world. A lapse in security good practice when using computer equipment may be exploited by cyber criminals, the results of which can have serious consequences for their victims.

This document outlines the motivation behind such attacks and explains the techniques most often used in an attempt to circumvent everyday security good practice.

2. Motivation

Attempting to circumvent security controls is by no means a new phenomenon in the world of computers – in fact, the first (experimental) computer virus was created way back in 1971; however it is the motivation which has changed significantly. Twenty years ago security compromises in computer systems were mainly the reserve of skilled individuals seeking fame or notoriety for their deeds. Contrast this with today where the rise and subsequent ubiquity of the Internet and the services it facilitates (e.g. social networking, internet shopping etc) has attracted the interest of many different types of cyber criminals and their activities often make headline news. Cyber criminals broadly breakdown into the following sub categories:

- **Hackers:** *Challenge, Ego, Rebellion, Notoriety.*
- **Organised Crime:** *Financial gain*
- **Script Kiddies:** *Fun, notoriety*
- **Hacktivist:** *Political agenda, revenge, exploitation, destruction*
- **Industrial Espionage:** *Competitive advantage, sabotage*
- **Governments:** *Surveillance, counter terrorism, espionage*

Of the groups given above it is Organised Crime and Hacktivist groups which tend to be the most prolific and therefore will be the main focus in this document.

3. Administrator level access / Malware

The ultimate goal of a cyber-criminal is to obtain administrator (sometimes known as Root) level privileges on the targeted computer. Once this is obtained the attacker has complete access and control over the computer and thereafter will often install malware (viruses) onto the computer which can be utilised in a variety of ways including:

- Silently and secretly gather information from the infected computer which is sent back to the malware creator (passwords, personal information and banking details are particularly valuable on the black market)
- Silently and secretly use the infected computer to participate in Denial of Service Attacks against a 3rd party of the malware creators choosing. (this may be to make a political statement or extort money from the targeted 3rd party)
- Use an infected computers resources to distribute bulk emails as part of spam and phishing campaigns.
- Silently and secretly take full control of the infected computer and thereafter use it to perpetrate attacks on other 3rd party computer systems.
- Used as a landing point within a network to attempt deeper network penetration utilising the "trusted" status of the compromised system.
- Redirect internet users of the infected computer to spoofed websites to illicitly gather information.
- Modify search results and redirect internet users of the infected computer to sponsored websites.
- Encrypt the infected computers data files (personal documents, music, videos etc.) so they are unavailable to the user; thereafter require payment to unlock them.
- Replicate and spread to other computers and attached USB media to infect other systems.
- Silently update themselves or receive new malware to continually evade anti malware solutions.

Computers that run Windows, Mac OS-X and Linux are all capable of being infected with malware, as are smart phone and tablet devices that run on Apple iOS or Google Android. However Windows based computers remains the predominant focus for malware creators simply because of the size of its user base compared to the other platforms (approximately 90%).

4. Security Vulnerabilities

For a cyber-criminal to leverage the benefits of malware on a computer they must first find ways to have the malware installed. Modern computer systems have in-built security mechanisms to help prevent the unauthorised installation of software (including malware), however a series of technological and social engineering attack methods are used to circumvent these mechanisms, the most common of which are listed below:

- Trojan Horse: A type of virus which masquerade or are hidden within something desired by a user. Examples include emails with “must check out this funny video clip” attachments or pirated software offered on popular file sharing sites.

- Software Vulnerabilities: Cyber criminals routinely seek out vulnerabilities in commonly used software applications (For example Adobe Reader, Microsoft Office) which can be exploited to silently take control of the computer and install malware. (This technique is often associated with hacking). Thereafter the malware itself can be used to seek out and infect similarly vulnerable computer systems.

- Website Vulnerabilities: Just like software applications, websites can also contain security vulnerabilities. Depending upon the type discovered they may be used to try and directly infect a computer with a virus when the website is visited; known as a drive-by infection. Alternatively they may replace legitimate website content with Trojan infected content (e.g. an instruction manual from a manufacturer website). If none of these more effective techniques are available they may be able modify the website to display seemingly legitimate content to redirect the user to a fake website if clicked.

- Phishing: Rather than wait for someone to visit hacked or fake websites cyber criminals may try and tempt a user with phishing emails. These unsolicited emails often purport to be sent by legitimate companies (for example: a bank, Amazon, Ebay, Facebook etc) and tempt to you to complete further action such as open the attachment or redirect you to a website – all of which serves to achieve the same result as mentioned above.

- Password Guessing: Computers are typically secured by login passwords which serve to protect the computer from unauthorised access from Malware as well as everyday users. However malware can attempt to guess the password by using commonly used passwords to get access.

5. Antivirus Software.

While it’s essential to have good antivirus software installed and working on computer systems they unfortunately cannot be considered a magic bullet. By their very nature antivirus solutions can only detect known viruses or new viruses that “look” very similar to previous versions. Consequently the Antivirus industry and cyber criminals are continually playing “cat and mouse” with antivirus firm Kaspersky announcing in 2012 that they were detecting 200,000 new viruses every day.

Another issue is that once malware has successfully infected a system they can “call home” for daily updates themselves or install completely new viruses. In this manner they can potentially remain undetected indefinitely with usually only the poor performance of the computer any indication that something is wrong.

Consequently good up to date antivirus software is just one of the measures that need to be taken to protect computer systems and the users using them.