Data Storage, Security & Compliance

Kieren Lovell
University Information Services
University of Cambridge
To inform people of good data security practices, threats to your data, why all data is important

......& how we can help.
Objectives

1. Introduction
2. Data Storage (Cloud vs Local)
3. Security
4. Compliance
5. Threats
6. Email
7. Local Machine
8. Physical Security
>>Introduction (IM)

Michelle Finnegan  
Deputy Director IM

Stephen Geraghty  
System Security Officer

Maddy Taylor  
IM Compliance Officer

Kieren Lovell  
IM Manager & Instructor
Introduction

Joined Royal Navy in 2002

Communications Specialist in Mine Warfare Warships

Joined MARBATSTAFF on HMS INVINCIBLE as a Communications Security Specialist.

Awarded Herbert Lott Award for Services to Information Security

Headhunted to Norway as the SME

Civilian Instructor for the Royal Norwegian Navy in Warfare, Communications & IM

Joined Nuclear Weapon, HMS Vengeance in 2003
Introduction
>>Data Storage (Local vs Cloud)

1. Not a simple binary
2. Local problems
3. Cloud issues
Data Storage (Local vs Cloud)

Whatever you select, answer the following:
1. What are the requirements of your funder?
2. How easy is it to use?
3. Do you have a secure backup?
4. Is your research sensitive? Who would be the likely TA's?
5. Damage on release?
6. Security is about C.I.A.
7. Does not conflict with Open Data
1. Let's take Cambridge
2. Since May 2015
   - All successful hacks have been human error
     - Unpatched servers
     - Failures in processes
     - Bad password management
     - Phishing
     - Open source intelligence
1. "But my data / research isn't important/classified?"
2. Attack vectors:
   - Crypto Locker
   - IP Theft
   - Data Destruction
   - Bank fraud
   - Journal Access
   - Wider Reputational Damage
   - Banking fraud
>>Compliance

1. Home Office, Defence, Medical, NDA.....
Cheatcodes

1. Need a compliance check? Contact me!
2. For Research Data Abroad? I conduct research security and workshop courses for "At Risk" students
3. Think "Passphrase", not "Password"
4. Do not do three monthly changing
Email Security

1. As secure as a postcard
2. PGP is an option, but complicated (but we can help)
3. Any research data, share through cloud providers (Dropbox for business though UIS, OneDrive, or other authorised Cloud solutions) rather than email
1. Public Wifi is not secure
2. We offer a VPN service. www.uis.cam.ac.uk and search VPN
3. If using ipad or iphone, do not use this service.

PureVPN / Tunnelbear
1. Encryption (Hard Drive)
2. PGP/GPG for sensitive research (As well)
3. Private/Public Keys - Keep a backup!
4. Backup's
5. Firewall
6. Software Updates
7. Anti Virus*
8. Jailbreak
9. Physical Security
10. Find my iphone / Android / Windows Phone
1. Introduction
2. Data Storage (Cloud vs Local)
3. Security
4. Compliance
5. Email Security
6. Wifi
5. Local Machine/Device Security
Discussion

Lock in: How to avoid
- Filetypes
- Open source (Positives and Negatives - e.g. OwnCloud)
- Open Standards
- Size of data
- Backups