



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



Information Security: What NDORMS needs to know

Wulf Forrester-Barker
NDORMS Information Governance Manager
Summer 2017



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



Information Security: What might be interesting...



BOTNAR
RESEARCH CENTRE | NDORMS



KENNEDY
INSTITUTE OF RHEUMATOLOGY | NDORMS



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



Information Security:

~~What might be interesting...~~



BOTNAR
RESEARCH CENTRE | NDORMS



KENNEDY
INSTITUTE OF RHEUMATOLOGY | NDORMS



NDORMS

NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



Information Security: What NDORMS needs to know



NDORMS

NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



BOTNAR

RESEARCH CENTRE | NDORMS



KENNEDY

INSTITUTE OF RHEUMATOLOGY | NDORMS

Why are you here?



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



- I was told I had to be
- It is a subject I am interested in
- I am confused about what I ought to be doing to stay safe
- I think I might have done something in error...

What do we do?



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



- World-leading translational research in musculoskeletal health, from bench to bedside.
- 600+ staff and students, including over 60 PIs
- Close collaboration with NHS
- Diverse research interests on local, national and global stage
- Wide range of supporting infrastructure
- Still growing!



BOTNAR
RESEARCH CENTRE | NDORMS



KENNEDY
INSTITUTE OF RHEUMATOLOGY | NDORMS

What data do we have?



NDORMS

NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



- Scientific data, including high volume sources
- Imaging – some groups now collect more than a terabyte per year
- Clinical trials, including participant data
- National level data sets (eg. HES, CPRD)
- Research and systems for all of the above
- Administrative information, including personnel and financial records



BOTNAR

RESEARCH CENTRE | NDORMS



KENNEDY

INSTITUTE OF RHEUMATOLOGY | NDORMS

What about you?



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



- What types of data are you responsible for?
 - If you were unable to access them, how would that affect you?
 - Are they public information or do they need to be kept private?
- How would it affect your colleagues if you had a problem?
 - Reputation, data, funding, jobs...

Who are we responsible to?



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



- Each other (especially those who work under our leadership)
- Those we collect data from
- The University of Oxford
- External data providers
- Information Commissioner's Office
- National law – eg. Data Protection Act 1998 (General Data Protection Regulation from May 2018)

You Aren't an Island



NDORMS

NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



BOTNAR

RESEARCH CENTRE | NDORMS



KENNEDY

INSTITUTE OF RHEUMATOLOGY | NDORMS

What are the risks?



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



Information Security Risk Matrix	Deliberate	Accidental
External	Eg. 'Attack': malware encrypts your files and demands a ransom payment.	Eg. Force majeure: storm damage to electricity supply causes a major power surge
Internal	Eg. Deliberate leak: employee finds a place that will pay for personal data and imagines they won't get caught!	Eg. Equipment Failure: one morning your computer doesn't wake up and your backup drive is months out of date

What are the risks?



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



Information Security Risk Matrix	Deliberate	Accidental
External	Eg. 'Attack': malware encrypts your files and demands a ransom payment.	Eg. Force majeure: storm damage to electricity supply causes a major power surge
Internal	Eg. Deliberate leak: employee finds a place that will pay for personal data and imagines they won't get caught!	Eg. Equipment Failure: one morning your computer doesn't wake up and your backup drive is months out of date



BOTNAR
RESEARCH CENTRE | NDORMS

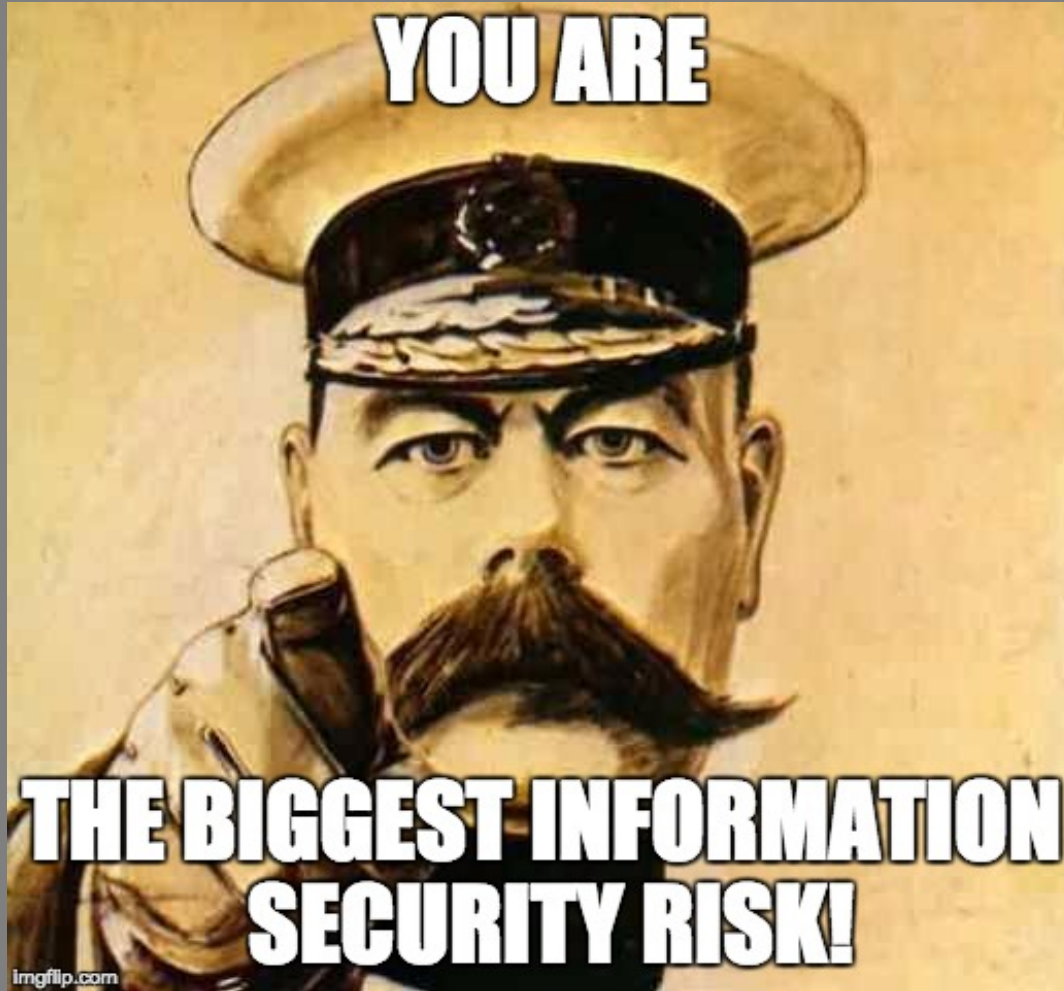


KENNEDY
INSTITUTE OF RHEUMATOLOGY | NDORMS

So, it's down to you!



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



The Part of Threes



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



- Three externally originated threats to guard against
- Three local risks to be aware of
- Three key messages to take home

External threats



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



BOTNAR
RESEARCH CENTRE | NDORMS



KENNEDY
INSTITUTE OF RHEUMATOLOGY | NDORMS



Malware

- Software that was written to do you harm and which tricked you into installing it
- Antivirus software gives some protection but malware is constantly evolving and uses tricks to avoid detection
- A recent example is WannaCrypt – didn't affect NDORMS but we have had other ransomware in the past.

Threat 1 – Malware



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



- How do you stay safe?
 - Keep software up to date
 - Be careful what you click on – emails and websites
 - Ensure your data is properly backed up
- What should you do if affected?
 - Disconnect from the network but don't turn off
 - Get IT support immediately – they promise to be supportive
 - IT support will look after required onward reporting

Threat 2 – Phishing



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



Phishing

- Attempts to trick you into giving away login names, passwords and other details
- Normally via email but can be found elsewhere online
- Details get collected, collated and sold by criminals
- Increasingly well disguised

Phishing Poll



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



How many phishing messages have you had in the past six months?

How many of those appeared to come from University of Oxford sources?

Threat 2 – Phishing



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



- How do you stay safe?
 - Be alert to the fact that phishing is a real, ongoing problem although perhaps not a flood
 - Be cautious about anything that wants you to click on it. If in doubt, get a second opinion
 - Don't reuse the same password in lots of places or with only minor changes
 - Renew passwords annually and after any scares
- If Oxford-branded, report to phishing@it.ox.ac.uk, attaching the message, with a copy to local IT support

Phishing Example



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



From: EMAIL-IT ADMIN

Sent: 30 May 2017 11:05

To: <your.name>

Subject: DEAR STAFF EMAIL USER OF : <your.name>@ndorms.ox.ac.uk

COMPULSORY STAFF EMAIL VERIFICATION ON 30 May, 2017 FOR OUTLOOK WEB APP!

Dear <your.name>@ndorms.ox.ac.uk ,

We are doing a mandatory staff eMail accounts clean up and upgrade to Microsoft office 365 complete email suite.
You need to respond today or your email will stop working.

Please Click [HERE](#) to Confirm your Email Account Active

After circulating this migration notice, any email account not processed as directed above will be deactivated without any further notice permanently as only the Migrated/verified from this mail will be able to use email via the new office 365 email suite.

Regards,

Email Administrator,
Microsoft Outlook Utilities

Malware AND phishing



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



- Targeted emails can combine both of these tactics
 - Personalisation to get past your guard
 - File or link to install malware on your machine
- Don't be too trusting of the 'from' and 'to' fields – these can be crafted to deceive
- Most common current example – attached 'invoice'

Threat 3 – Physical Loss



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



Physical loss of equipment

- Theft from the building, including any computer small enough to pick up and carry out.
- Laptop mislaid or stolen while out and about
- Could apply to other IT equipment, such as USB sticks, external hard drives or even your phone (how many accounts does it automatically log onto?)
- Nothing reported recently – don't be complacent

Threat 3 – Physical Loss



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



- How do you stay safe?
 - Physical security – keep things locked down or locked up
 - Challenge strangers and tailgaters
 - Whole disk encryption – easy, free and safe
 - Have backups that aren't stored with the machine
- What should you do if affected?
 - Report to IG Manager and Institute administrator
 - Remotely wipe / disable if possible
 - Change login details

Internal risks



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



BOTNAR
RESEARCH CENTRE | NDORMS



KENNEDY
INSTITUTE OF RHEUMATOLOGY | NDORMS

Risk 1 – Equipment Failure



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



Dead machine

- One day you might try to start your computer and find nothing happens...
- Or perhaps you are middle of working on a task and it suddenly goes off...
- Computers are complex systems, full of component parts that can wear out or degrade over time
- The right word is not “if” but “when”!

Question – Equipment Failure



NDORMS

NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



Have you ever experienced an IT system either dying completely or becoming too unreliable to use?

Did the experience make you change your habits... and did that last long enough to make a difference the next time?



BOTNAR
RESEARCH CENTRE | NDORMS



KENNEDY
INSTITUTE OF RHEUMATOLOGY | NDORMS

Risk 1 – Equipment Failure



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



- How do you stay safe?
 - You can't be entirely safe but you can minimise the inconvenience
 - If you start to experience problems, get IT support sooner than later; early action can make repairing or replacing a machine a less painful experience
 - Backups are your main defence – ideally, test them before you need them and review them from time to time
- What should you do if your machine does break?
 - Work with IT support
 - If you have a unique set up, make sure you know how to reinstall and configure it on a new system

Risk 2 – Unreadable Data



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



Unreadable data

- Just because you saved a file, doesn't mean you can still open it
- Parts of the file can be damaged, corrupting data and possibly making it unreadable
- Old drives and disks might not work – or we might not have a device they can work with
- You might no longer have software that can make use of the data.

Risk 2 – Unreadable Data



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



- How do you stay safe?
 - Backup to a maintained system, not a single device. Network drives are ideal.
 - Curate your collection: keep notes about what you did, how you stored it and copies of the programs required (periodically check they still run)
 - Where possible, use file formats that can be opened by many programs (eg. CSV, PDF-A), if necessary converting during the closing stages of the project
 - Retention policy – what should you not keep
- What should you do if you discover a problem?
 - Get help from IT support, who can link into the range of expertise (and old kit) across the University

Cloud Backups?



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



- Dropbox, iCloud and other third party services
 - Data stored on unknown computers at unknown locations – unsuitable for confidential data
 - Acceptable for uses like personal music files, reference manager library
- For University data, use University systems
 - Network drives, OxFile, Filr, Nexus365 (pending), etc

Risk 3 – Passwords



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



Problems with passwords

- Have you got too many passwords to remember?
- Do you take shortcuts, like using the same password in many places or writing them down in your notebook?
- Are your passwords easy to guess?
 - Widely used, like '123456' or 'password'
 - Short
 - Common pattern, like word + number

Risk 3 – Passwords



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



- How do you stay safe?
 - Make sure your password isn't one of the low-hanging fruit (long, hard to guess :-)
 - Use a password management system (eg. Lastpass, OnePass, Keychain, Keepass, etc – or even a manual approach)
 - Update regularly (yearly is enough unless working under more specific rules), and immediately if you have any reason to be concerned
 - Two factor authentication (2FA)

Three Things to Take Away



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



1. You are responsible for valuable information
2. Most of what you need to do is regular, mundane and easy:
 - Backup your data (network storage is ideal)
 - Be cautious about what you click on (emails and websites)
 - Keep your software updated
3. Review your information regularly and, if some of it has stricter rules, follow them.

What now?



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



- Be familiar with and **follow** our Information Governance policies
- Get problems sorted out rather than sitting on them – know how to get IT support in your building
- Information Governance Manager available to advise on all information security questions
- From the autumn, we will require everyone to use the University's online Information Security module annually rather than just at induction
- Be proactive – discuss, plan, write it down and act
- Remember to sign the register!

Follow the links on the handout to access the information you need

Any Questions?



NDORMS
NUFFIELD DEPARTMENT OF ORTHOPAEDICS,
RHEUMATOLOGY AND MUSCULOSKELETAL SCIENCES



BOTNAR
RESEARCH CENTRE | NDORMS



KENNEDY
INSTITUTE OF RHEUMATOLOGY | NDORMS



- ICO Enforcement actions:
<https://ico.org.uk/action-weve-taken/enforcement/>
- Island: <https://static.pexels.com/photos/121506/pexels-photo-121506.jpeg>
- 'You are the biggest information security risk'
generated at <https://imgflip.com/i/1qxyur>
- Clouds: <https://www.flickr.com/photos/wulf/631394534/>
- Images are either licenced for free re-use or belong to NDORMS