The University Information Security Policy & InfoSec one year on…

Tom Anstey

Weatherall Institute of Molecular Medicine & InfoSec

infosec@it.ox.ac.uk

http://www.it.ox.ac.uk/infosec/infosecproject/

July 17, 2013

The need for a Policy!

OxCERT led a Information Security Self-Assessment in 2007-2009

									compliant	partially compliant	not compliant	not applicable	blank		
(Section 1 asked for the addess details of the unit)	Unit A	Unit B	Unit C	Unit D	Unit E	Unit F	Unit G	Unit H	c	pc	nc	na	blank	**total**	Percentage of units not compliant with this recommendation
11. There are procedures in place for the management of removable media.	nc	nc	nc	pc	pc	nc	nc	nc	0	2	6	0	0	**8**	75%
12. There are procedures in place for the secure and safe disposal of media when it is no longer required.	pc	pc	c	pc	pc	pc	c	c	3	5	0	0	0	**8**	0%
13. Procedures for the handling and storage of information have been established to protect it from unauthorised disclosure or misuse.	nc	nc	nc	c	nc	pc	nc	c	2	1	5	0	0	**8**	63%
14. There are procedures in place to ensure that media containing information is protected against unauthorised access, misuse or corruption during transportation beyond the unit's/University's physical boundaries.	pc	nc	nc	c	nc	na	nc	nc	1	1	5	1	0	**8**	63%
15. Controls are implemented to ensure that electronic messaging is appropriately protected.	nc	c	nc	c	pc	c	nc	nc	3	1	4	0	0	**8**	50%
16. A policy on the use of cryptographic controls for the protection of information has been developed and implemented.	pc	na	nc	pc	nc	nc	na	nc	0	2	4	2	0	**8**	50%
17. Wherever possible non-public data are only kept in encrypted form. Any printed records of passwords, etc. are also protected from unauthorised access.	pc	na	nc	c	pc	nc	c	nc	2	2	3	1	0	**8**	38%
18. Key management procedures are in place to support the unit's use of cryptographic techniques.	nc	na	nc	c	pc	nc	nc	na	1	1	4	2	0	**8**	50%
19. Where a network connection is not possible, procedures exist to ensure that data in transit are encrypted, with the encryption key sent separately.	nc	na	nc	c	pc	na	nc	na	1	1	3	3	0	**8**	38%

Information Security Best Practice 2009-2011

WE WILL BE ADOPTING THE BEST PRACTICES IN OUR INDUSTRY, JUST LIKE EVERYONE ELSE.
BEST PRACTICES
www.dilbert.com scottadams@aol.com
IF EVERYONE IS DOING IT, BEST PRACTICES IS THE SAME THING AS MEDIOCRE.
9-3-08 ©2008 Scott Adams, Inc./Dist. by UFS, Inc.
STOP MAKING MEDIOCRITY SOUND BAD!
SORRY.

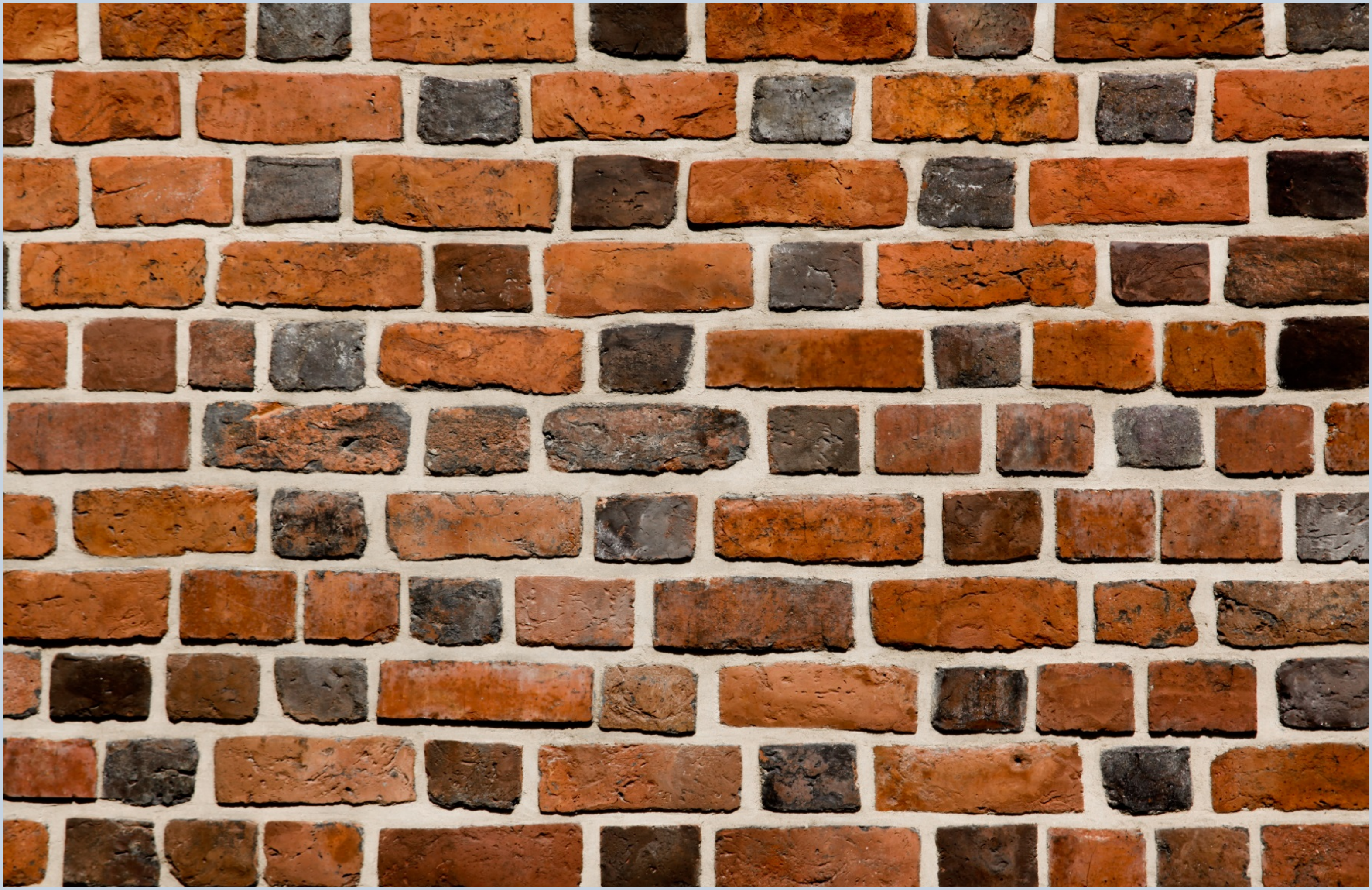
Cookie legislation
May 2012

DELETE COOKIES?!
gegen-den-strich.com
FERNANDEZ
DUMBFOUNDED
The cookie monster was dumbfounded that you could actually delete cookies on the computer.
FreePosterMaker.com

iT services

UNIVERSITY OF OXFORD

Creating a University Policy (1)



Creating a University Policy (2)

+

ICTF staff + Council Secretariat

Creating a University Policy (3)

I AM NOT RESISTANT TO CHANGE!!! NOW LET ME GET BACK TO MY COMMODORE 64!
cloud

Governance: Central -vs- Local

- The University Policy tells you *what* to do - a local policy gives more on *how* you do it in your unit

- The responsibility is devolved downwards, but if the correct local policies and risk assessments are in place and carried out, the responsibility for risk goes upwards

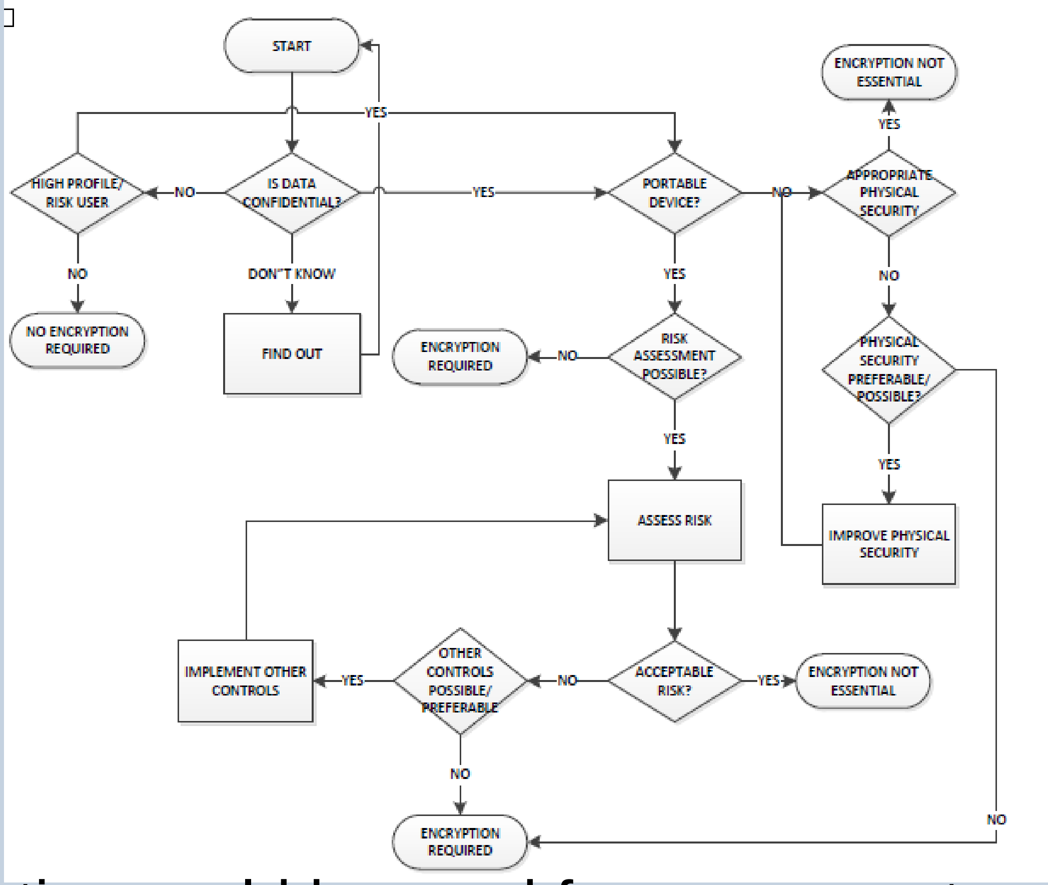
- Creation of Information Security Advisory Group (ISAG) chaired by Emma Rampton in Council Secretariat; includes University Security Service, Conference of Colleges, ICTF, Academics & InfoSec

Identify the problems – Risk Assessments

Non-IT Security

Includes liaison with:

University Marshal
Bio-Medical services
Legal services
Hospital trusts
Personnel services



Not just an IT issue

Flowchart for data encryption could be used for paper waste destruction protocol.

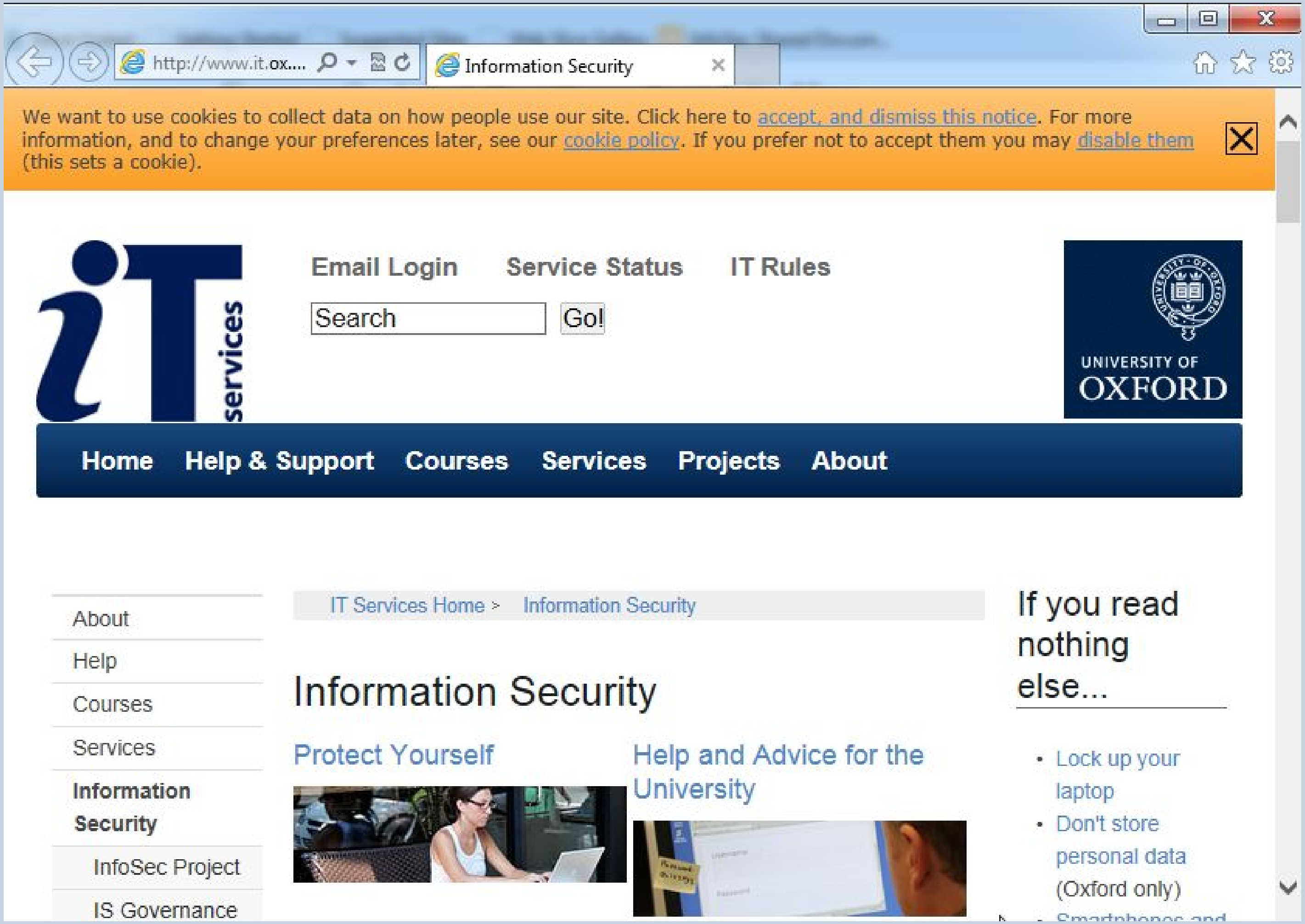
Whole Disk Encryption

Finding a balance between security and usability.

Lunchtime seminars

- Each term
- 5 speakers
- 8 sessions

InfoSec website and SharePoint



We want to use cookies to collect data on how people use our site. Click here to accept, and dismiss this notice. For more information, and to change your preferences later, see our cookie policy. If you prefer not to accept them you may disable them (this sets a cookie).

IT Services Home > Information Security

Information Security

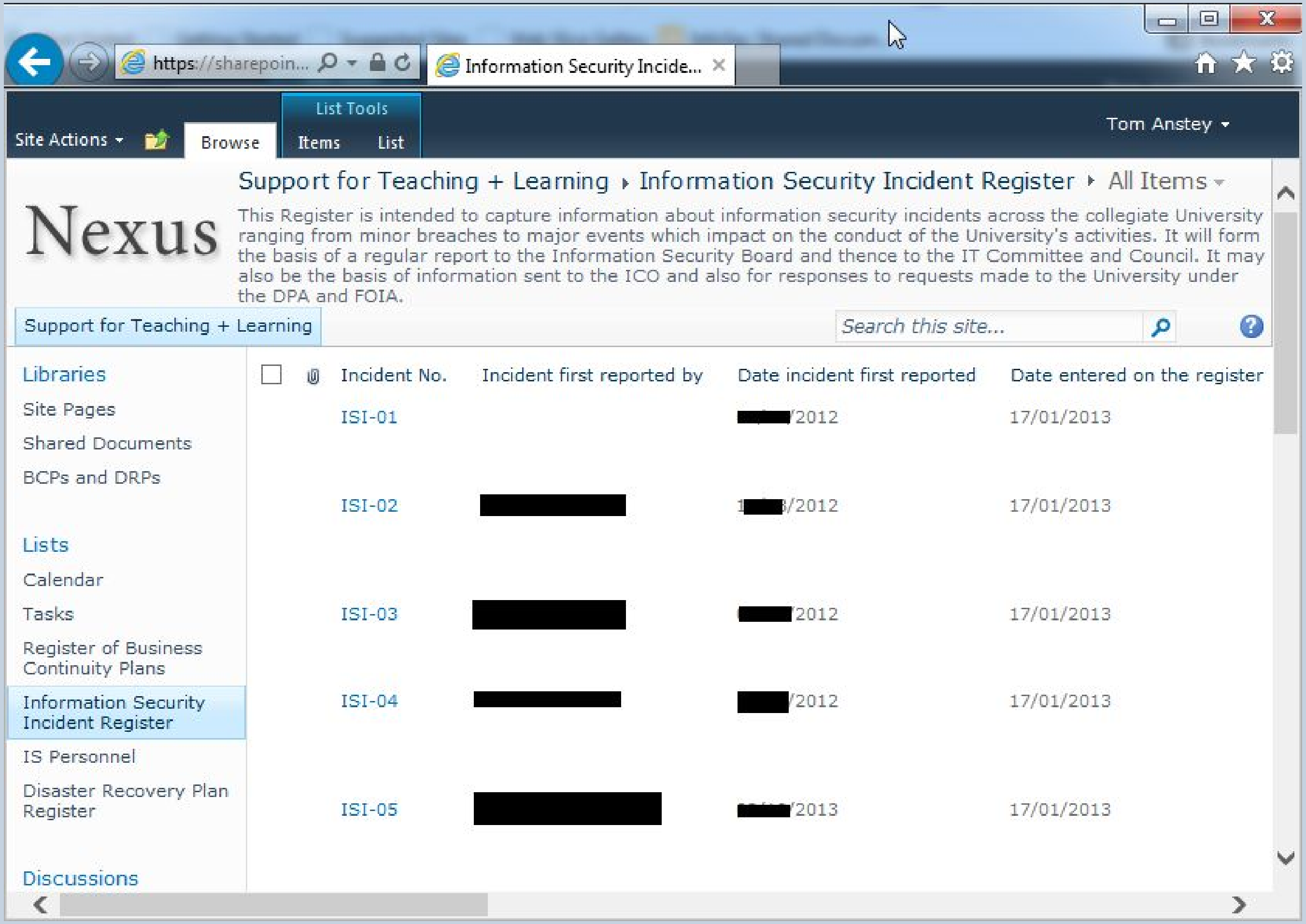
Protect Yourself

Help and Advice for the University

If you read nothing else...

- Lock up your laptop
- Don't store personal data (Oxford only)
- Smartphones and

Incident register



Support for Teaching + Learning ▸ Information Security Incident Register ▸ All Items

Nexus

This Register is intended to capture information about information security incidents across the collegiate University ranging from minor breaches to major events which impact on the conduct of the University's activities. It will form the basis of a regular report to the Information Security Board and thence to the IT Committee and Council. It may also be the basis of information sent to the ICO and also for responses to requests made to the University under the DPA and FOIA.

Support for Teaching + Learning
Search this site...
Libraries
Site Pages
Shared Documents
BCPs and DRPs
Lists
Calendar
Tasks
Register of Business Continuity Plans
Information Security Incident Register
IS Personnel
Disaster Recovery Plan Register
Discussions

□	Incident No.	Incident first reported by	Date incident first reported	Date entered on the register
	ISI-01		[redacted]/2012	17/01/2013
	ISI-02	[redacted]	[redacted]/2012	17/01/2013
	ISI-03	[redacted]	[redacted]/2012	17/01/2013
	ISI-04	[redacted]	[redacted]/2012	17/01/2013
	ISI-05	[redacted]	[redacted]/2013	17/01/2013

Is guidance to IT Staff enough?

- IT Staff don’t own the sensitive data
- They don’t know what is stored, nor the associated risk
- What about paper copies? Is it really IT’s problem?

Divisional briefings to administrators

This is where the power really is!

They’re now on board and understand the need for improved practices, and a local policy.

Improved understanding of a unit’s responsibility and liability.

It’s in the Toolkit!

Examples
Explanations
Encryption
… easy to read!

On-going work in progress
Aims to meet ISO2007:2005

http://www.it.ox.ac.uk/infosec/istoolkit/

Centre for the Protection of National Infrastructure

CPNI
Centre for the Protection
of National Infrastructure

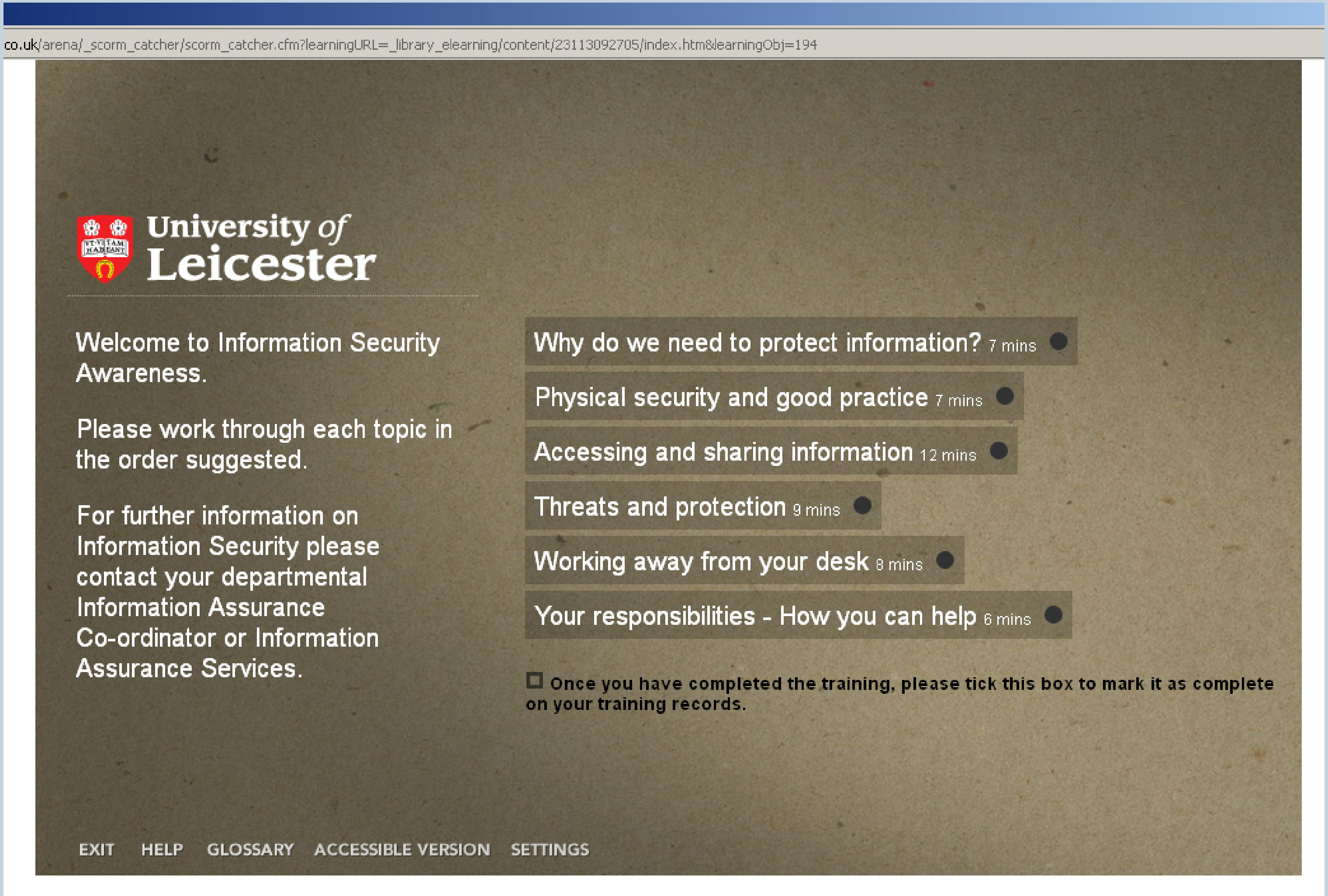
Government cyber-security initiative

Fits in with other ox.ac.uk academic work

e.g. Andrew Martin, Sadie Creese et al.

Don’t get your reputation torn to
SHREDS
Dispose of our data carefully.
Lock it...shred it...
just don’t leave it.

EPIC on-line training



co.uk/arena/_scorm_catcher/scorm_catcher.cfm?learningURL=_library_elearning/content/23113092705/index.htm&learningObj=194

Welcome to Information Security Awareness.

Please work through each topic in the order suggested.

For further information on Information Security please contact your departmental Information Assurance Co-ordinator or Information Assurance Services.

- Why do we need to protect information? 7 mins ●
- Physical security and good practice 7 mins ●
- Accessing and sharing information 12 mins ●
- Threats and protection 9 mins ●
- Working away from your desk 8 mins ●
- Your responsibilities - How you can help 6 mins ●

□ Once you have completed the training, please tick this box to mark it as complete on your training records.

Post mortem discussions

Summary

- Provide proper management backing to get a unit policy into place
- Increase user awareness and provide training to all users
- Create information asset & risk registers and develop a business continuity plan for disaster recovery. Start on high impact areas.
- Manage mobile devices, and encrypt laptop hard disks and devices containing sensitive data, or provide secure remote access
- Purchase and issue encrypted devices that allow managed password recovery to those needing to remove sensitive data
- Act on your risk assessments. Give a reasonable timescale for implementation; it is a culture change