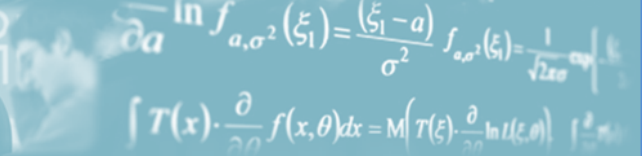
UNIVERSITY OF BIRMINGHAM

Tightening Information Security

Dr. Sean Duffy, Director of IT Services

ICTF 2013 Conference



Poacher

?

Gamekeeper

Poacher

Poacher

?

Gamekeeper

Gamekeeper

Agenda

- Why Information Security is an issue
- External agencies
- Information Classification
- Enhanced security tools
- Changing behaviours

Data Security – a growing problem

- What kind of data?
- Who is responsible?
- How secure?
- What happens when something goes wrong?

What kind of Data?

- Personal data (e.g. name + address – dinner attendees, external research collaborators).
- Sensitive personal data (e.g. medical info, patient records, sexuality, criminal record, political/religious beliefs, ethnic origin).
- University's commercial data (e.g. IP, admission / conversion rates, TRAC data, research income per department).
- 3rd party commercial data – research data, IP, supplier lists.

Who is responsible?

- The University, individual students, and members of staff
  - Under the Data Protection Act
  - Under the Human Rights Act - right to privacy
  - Under research contracts which may impose similar security as the 3rd party's – e.g. private sector, NHS, Ministry of Justice
  - Under our University policies on DPA and Research

Data Protection Act 1998

- Personal data must be processed in accordance with the 8 Data Protection Principles.
- It is a CRIMINAL offence to
  - Obtain or disclose personal data to / from a third party (without consent).
  - Procure disclosure of personal information to another.
- There are some exemptions i.e. necessary to prevent/detect a crime or justified in the public interest.

Eight Data Protection Principles

- Data must be:
  - fairly and lawfully processed;
  - processed for limited purposes;
  - adequate, relevant and not excessive;
  - accurate;
  - not kept longer than necessary;
  - processed in accordance with the data subject's rights;
  - KEPT SECURE;
  - not transferred to countries without adequate protection.

‘Fairly and lawfully processed’ means…….

- The individual has given consent or it’s a contractual duty, or its required by law

  AND

- The individual is told why we want it, how long we will keep, and who will have access to it.

- Finally, would an independent outsider consider the processing was fair?

How Secure?- Uni/3rd party IP

- CPNI have advised that certain countries are hacking universities to trawl for their IP and other research partners. There is even evidence of hacking legal firms to see what IP patents are about to be filed. CPNI keep a list of topics of interest to certain countries in on their website.

DPA sanctions

- As well as potentially a criminal prosecution, ICO can now fine up to £500k, and require an undertaking, e.g. to train every member of the organisation in DPA (that could include all students). They can also audit and issue enforcement notices.

Possible civil actions

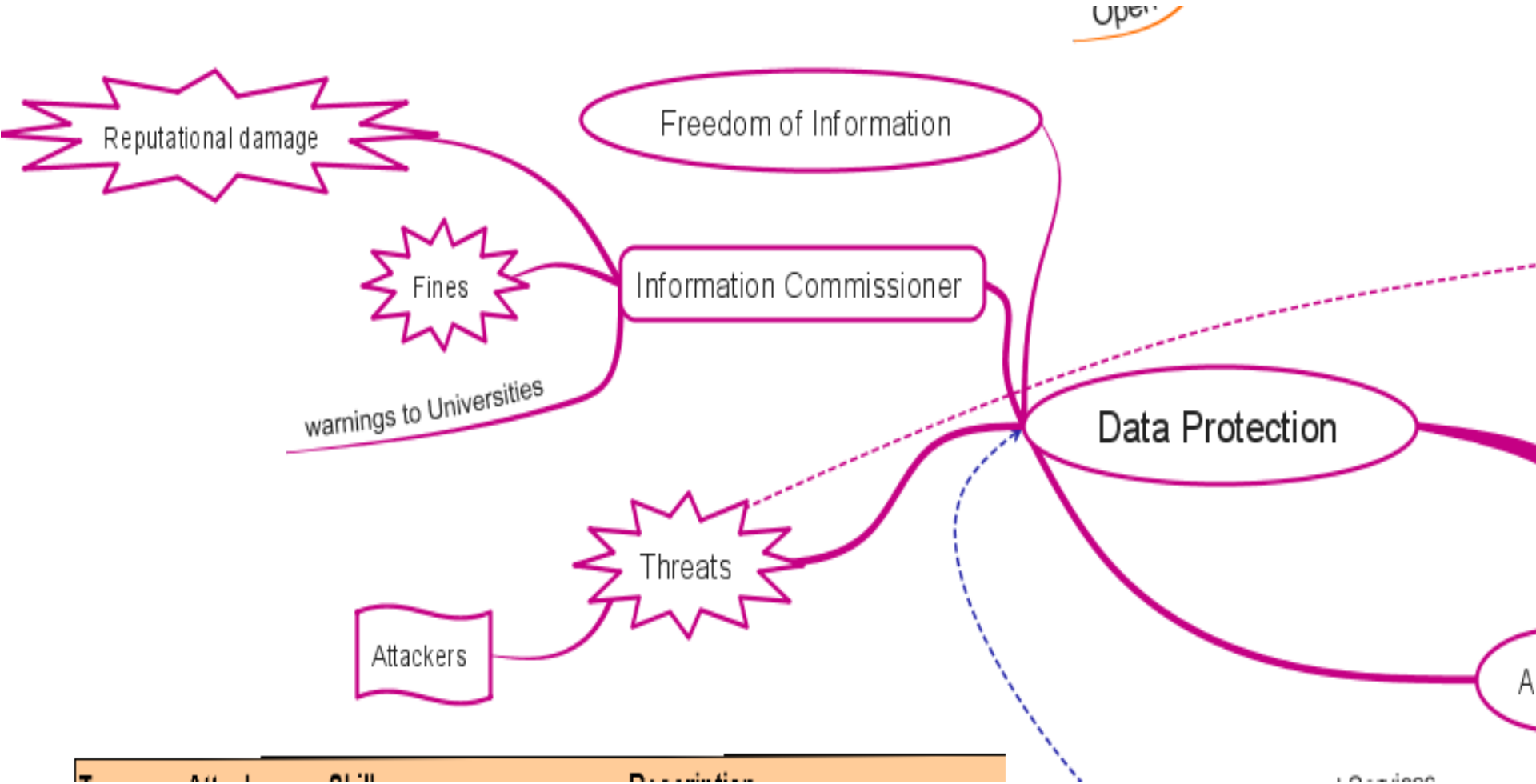
- The University can be sued for compensation if personal data is lost, destroyed or disclosed without the authority of the individual (they will probably also add a claim for breach of privacy under the Human Rights Act)

- A court will consider whether the University had taken reasonable precautions.

Commercial consequences

- Action for breach of confidentiality – for some industrial partners, this is their prime concern. They will injunct and/or sue UoB for breach. They will terminate all contracts. Depending on the loss/leak, the damages could be large, and then there is the reputational damage.

Legislative environment



Agenda

Why Information Security is an issue

External agencies

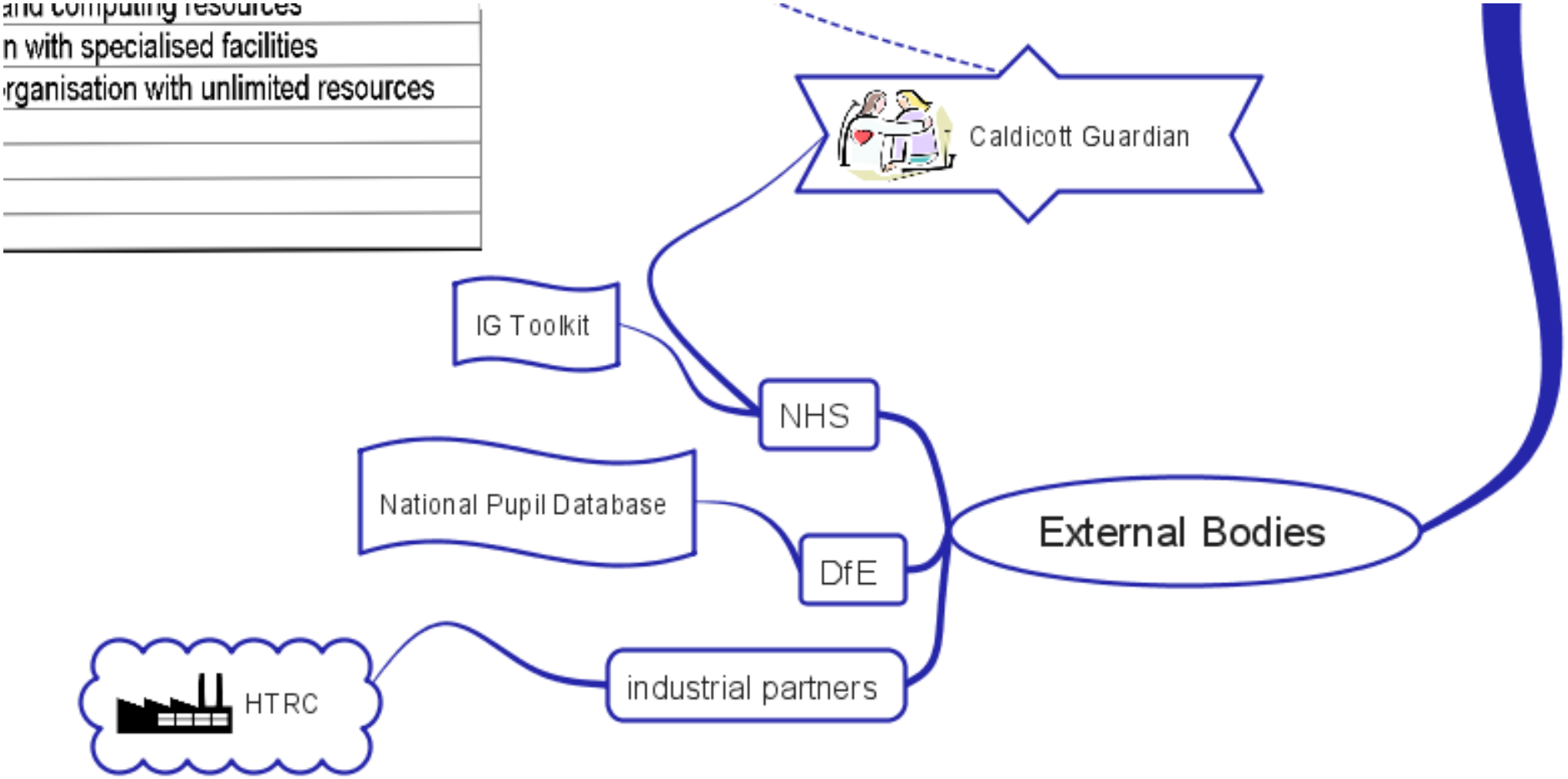
Information Classification

Enhanced security tools

Changing behaviours

External agencies requiring greater security

and computing resources
n with specialised facilities
rganisation with unlimited resources



Agenda

Why Information Security is an issue

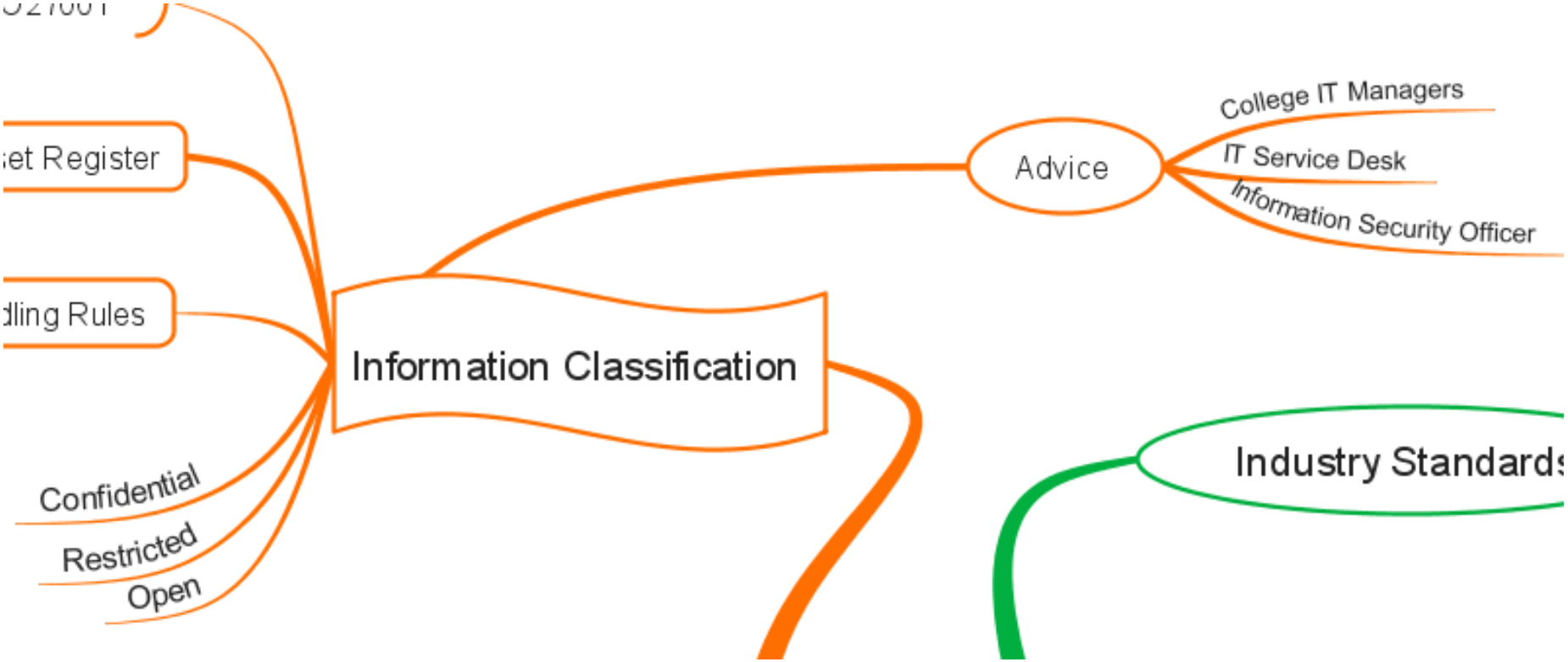
External agencies

Information Classification

Enhanced security tools

Changing behaviours

Information Classification



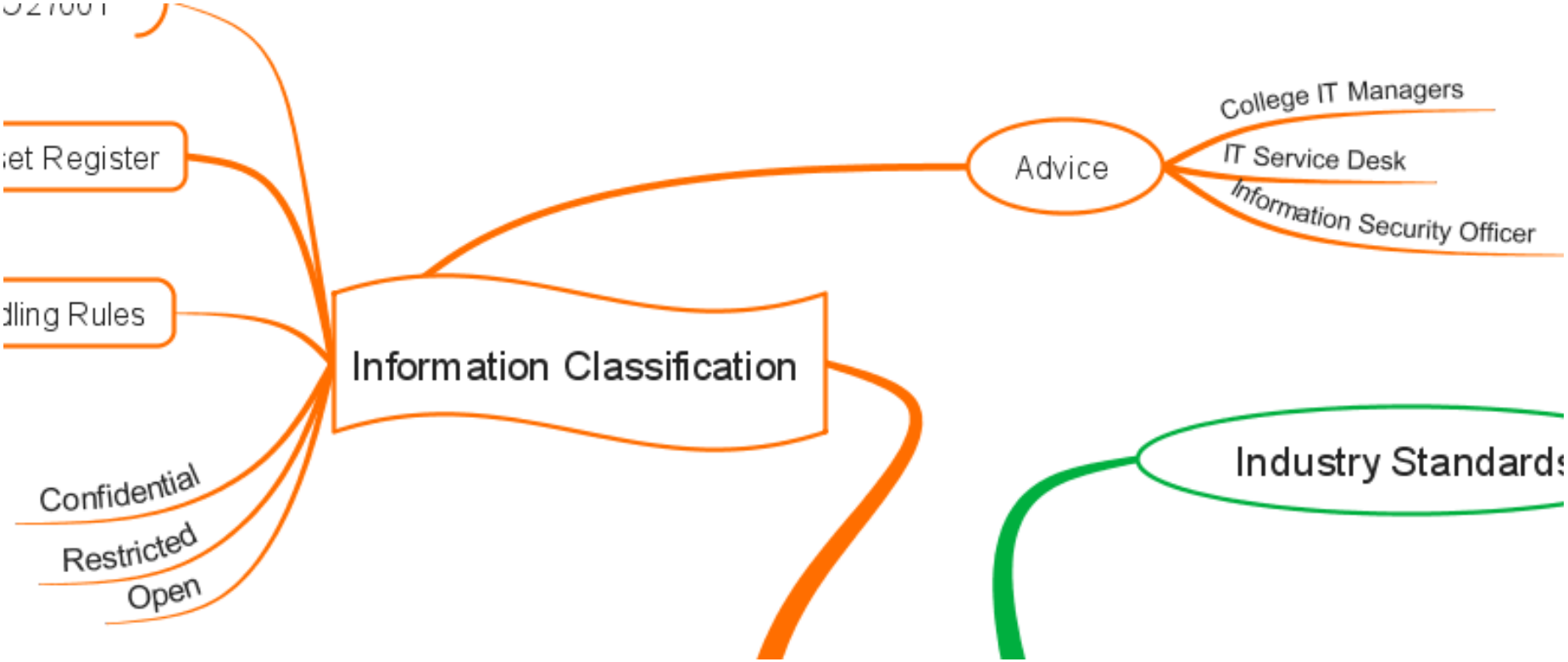
Information Classifications

Category	*Summary*	*Examples*
Open	Information intended for the public domain or that carries no appreciable confidentiality risk.	All information is assumed to be open unless specifically designated otherwise.
Restricted	Information intended for a defined audience but not particularly sensitive.	• Committee minutes (except Council and Senate). • Draft discussion papers - restricted • Intranet web sites • Most internal documents
Confidential	Information likely to cause significant harm to the University's reputation, assets or ability to meet its legal and contractual obligations if revealed outside of the intended audience. Obligation to treat as Confidential by law or contract. Information that carries a high confidentiality risk.	• Student recruitment information • Admissions information • Legally privileged documents • Senior Management and Strategic discussion papers • Live examination papers • Contracts, commercial data • Unpublished research • University budget / TRAC data • Personal details (DPA) • Salary and Payroll data • Patient identifiable data • Credit / payment card details

Handling Guidelines

Email	• Encrypt **Confidential** email and attachments • Sign email to protect against tampering (but no need to sign encrypted email)
Storage	• Encrypt **Confidential** data except when stored in a protected network zone • Do not encrypt **Restricted** so that it can be scanned for viruses and other malware • Avoid storing **Confidential** data on laptops, desktops, mobile devices and removable media else ensure it is encrypted
Cloud Storage	• Encrypt **Confidential** files • Ensure physical storage within UK or EEA
Fax	• Do not fax **Confidential** information unless a trusted person is standing by at the other end to receive it
Paper Documents	• If **Confidential**, mark on every page. • If **Restricted**, mark prominently on first page or cover at least • Store **Confidential** papers in a locked cabinet with known key holders
Destruction	• Shred **Confidential** paper copies or use secure disposal service • Delete **Confidential** files and overwrite removable media using utility
Mobile Devices	• Encrypt **Confidential** files using approved app. • Use ‘Good for Enterprise’ or Outlook Web Access (OWA) only

Assistance and advice



Agenda

Why Information Security is an issue

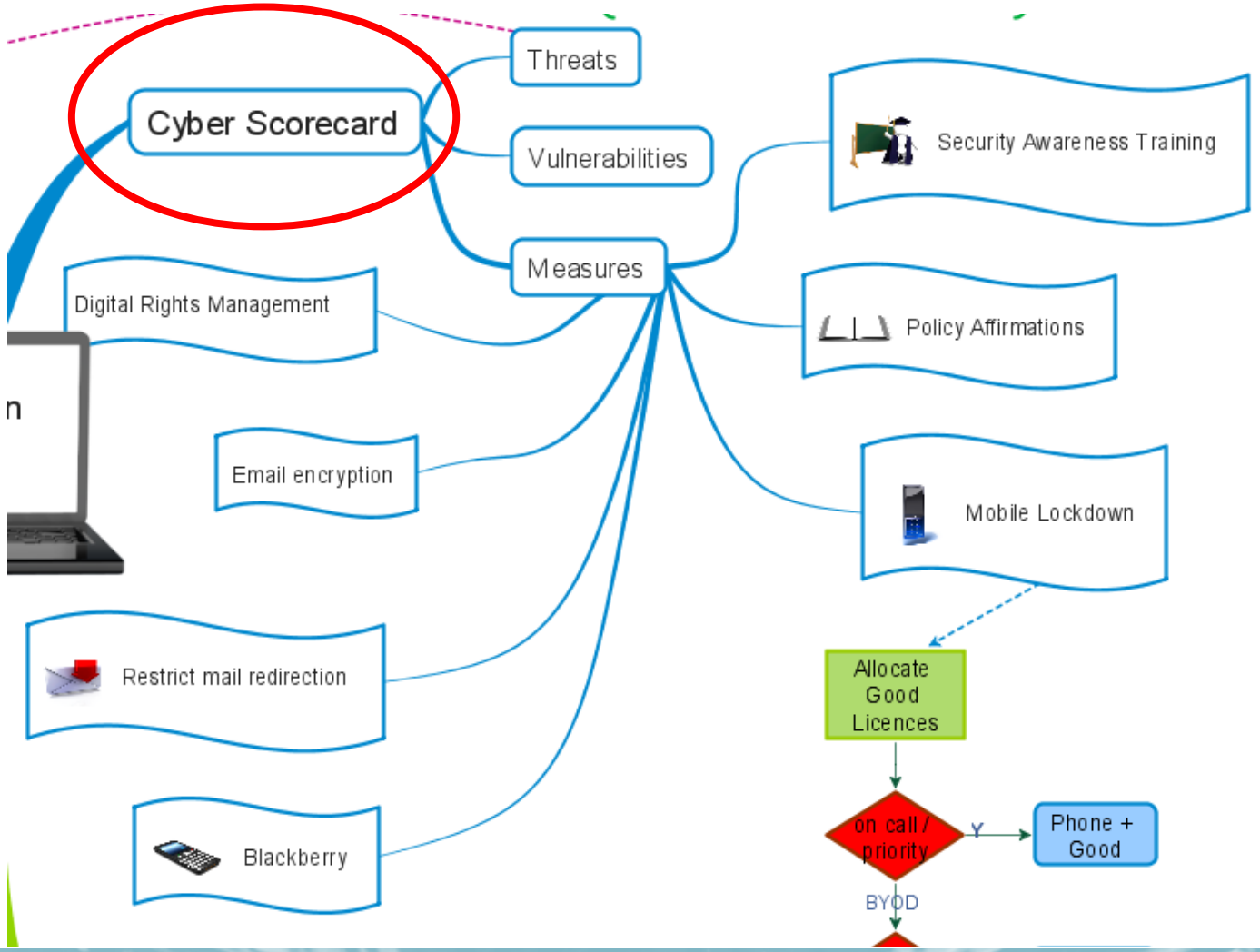
External agencies

Information Classification

Enhanced security tools

Changing behaviours

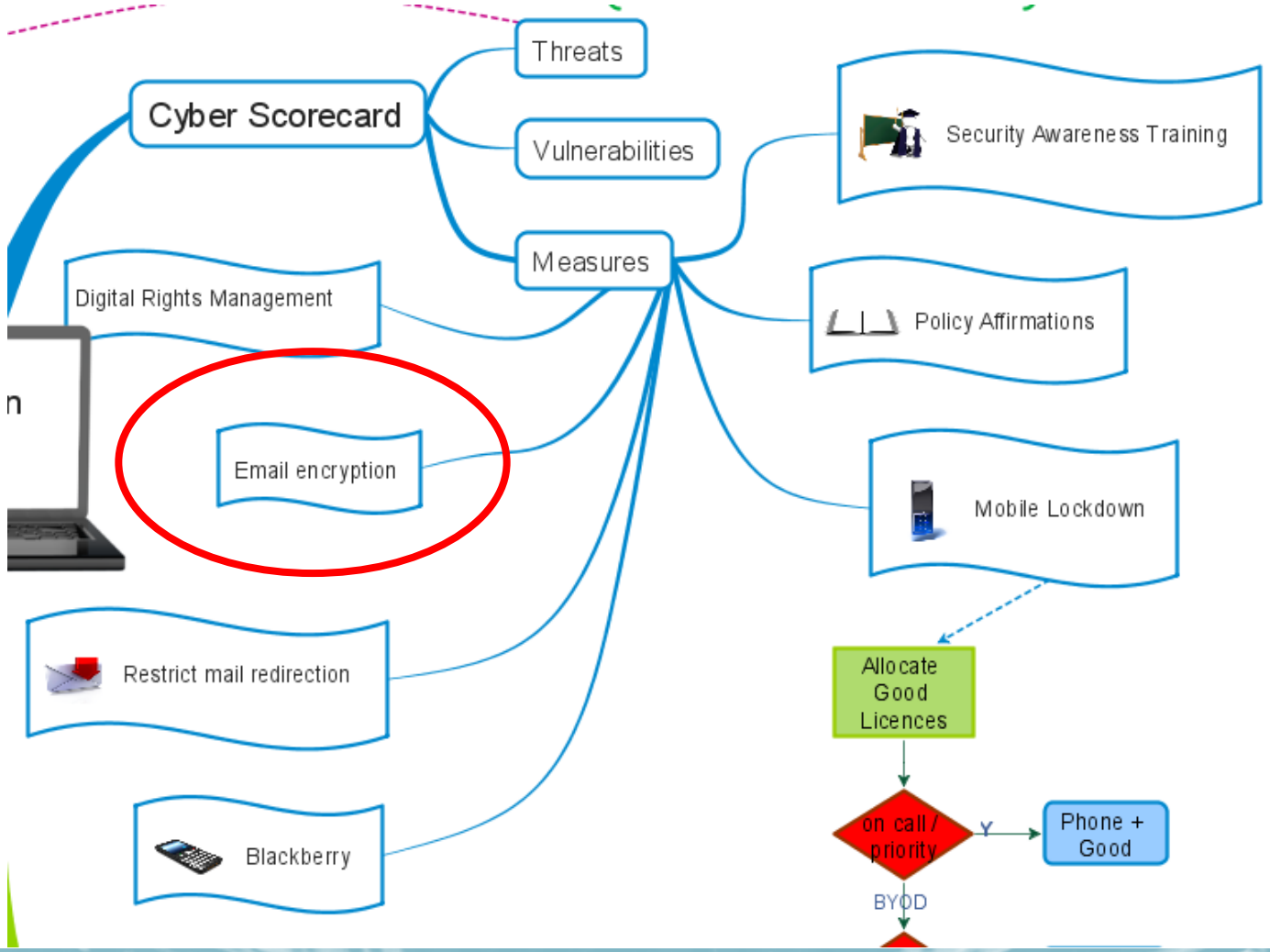
Security measures and initiatives



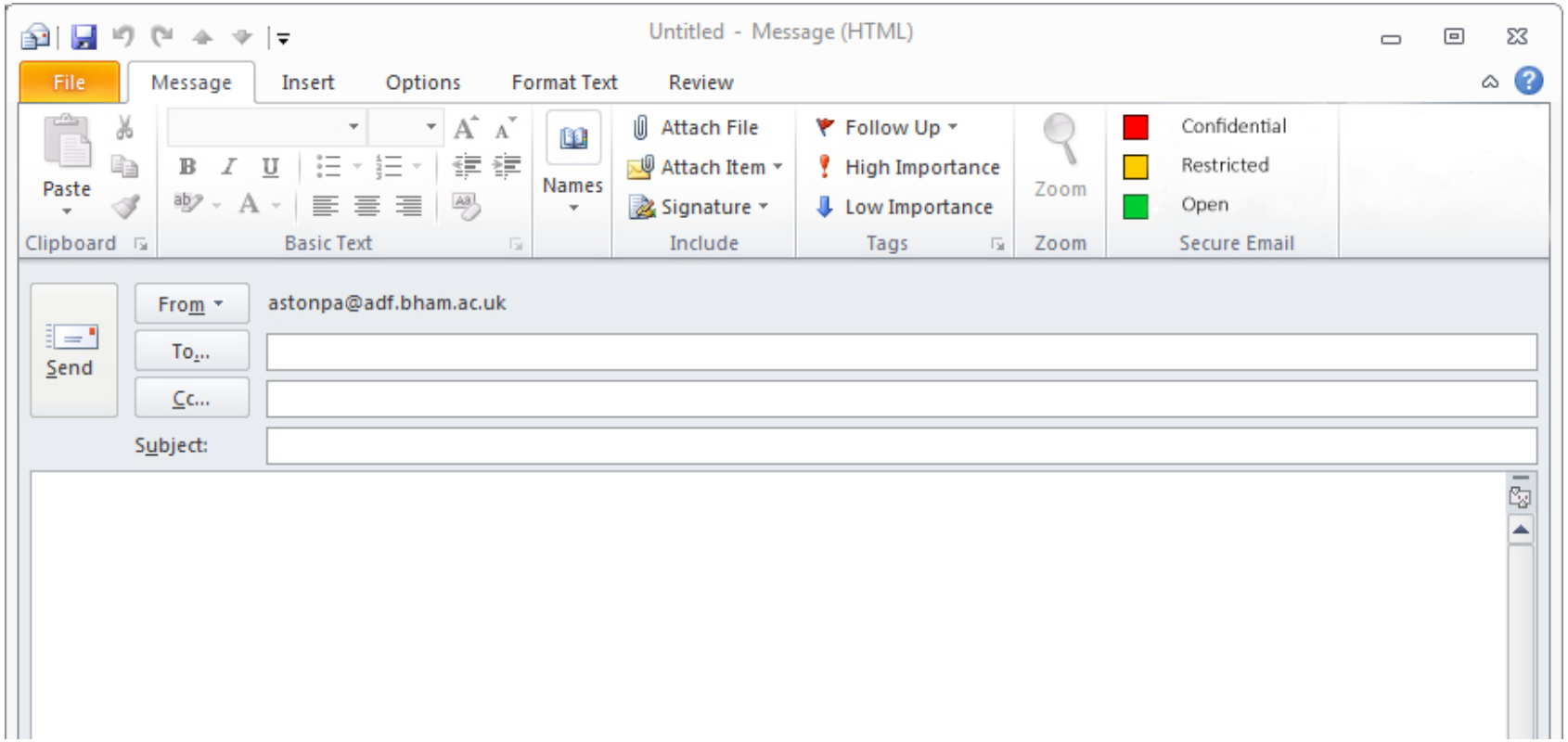
Cyber Security Scorecard

ID	Threats	Assets	Vulnerabilities		Controls	Adopted	Status	Timing	
1	Loss or theft of mobile device	Mobile devices	Email stored in mobile devices	8	Mobile Device Management (MDM)	L	Production	Q2 2013	!
2	Loss or theft of mobile device	Mobile devices	Email stored in mobile devices	9	Mobile email lockdown	L	Development	Q2 2013	!
3	Targeted theft of mobile device	Mobile devices	Email stored in mobile devices	8	Mobile Device Management (MDM)	L	Production	Q2 2013	!
4	Targeted theft of mobile device	Mobile devices	Email stored in mobile devices	9	Mobile email lockdown	L	Development	Q2 2013	!
5	Social engineering	Staff	Untrained staff	18	Security Awareness Training	L	Feasibility	Q2 2013	!
6	Hacking	Core business applications	Remote access	4	VPN with strong authentication	H	In Use		
7	Hacking	Critical applications	Remote access	4	VPN with strong authentication	H	In Use		
8	Hacking	Network accessible storage (NAS)	Poor or incorrect configuration	43	Server configuration standards	H	In Use		
9	Hacking	Network accessible storage (NAS)	Generic accounts	13	Remove or disable generic accounts	M	In Use		
10	Hacking	Network accessible storage (NAS)	Remote access	4	VPN with strong authentication	H	In Use		
11	Hacking	Application servers	Security Misconfiguration	43	Server configuration standards	H	In Use		
12	Hacking	Application servers	Poor or incorrect configuration	43	Server configuration standards	H	In Use		
13	Hacking	Application servers	Generic accounts	13	Remove or disable generic accounts	M	In Use		
14	Malware	Application servers	Security Misconfiguration	37	Multiple antivirus	H	In Use		
15	Hacking	Network accessible storage (NAS)	Cloud storage	26	File encryption	L	In Use	Q2 2013	
16	Hacking	Core business applications	SQL, LDAP, XML injection	32	Defensive programming	M	In Use		
17	Hacking	Core business applications	Remote access	4	VPN with strong authentication	H	In Use		
18	Hacking	Core business applications	Cloud storage	4	VPN with strong authentication	H	In Use		
19	Hacking into shared cloud storage	Intellectual property	Remote access	4	VPN with strong authentication	H	In Use		
20	Hacking	Critical applications	Remote access	4	VPN with strong authentication	H	In Use		
21	Hacking	Critical applications	Remote access	4	VPN with strong authentication	H	In Use		
22	Hacking into shared cloud storage	Patient identifiable data	Cloud storage	4	VPN with strong authentication	H	In Use		
23	Hacking into shared cloud storage	Patient identifiable data	Remote access	4	VPN with strong authentication	H	In Use		
24	Hacking	Database servers	Security Misconfiguration	43	Server configuration standards	H	In Use		
25	Hacking	Database servers	Poor or incorrect configuration	43	Server configuration standards	H	In Use		
26	Hacking	Database servers	Generic accounts	13	Remove or disable generic accounts	M	In Use		
27	Email forwarding	Email	Forwarded to insecure email service	27	Restrict mail redirection	L	Production	Q2 2013	!
28	Phishing	Email	Untrained staff	18	Security Awareness Training	L	Feasibility	Q2 2013	!
29	Accidental security breach	Staff	Passwords	18	Security Awareness Training	L	Feasibility	Q2 2013	!
30	Email interception	Email	Forwarded to insecure email service	27	Restrict mail redirection	L	Production	Q2 2013	!
31	Loss or theft of laptop	University laptops	Email stored in laptops	10	Full disk encryption	H	In Use		
32	Loss or theft of laptop	University laptops	Files stored in laptops	10	Full disk encryption	H	In Use		
33	Loss or theft of laptop	University laptops	Credentials stored in laptop	10	Full disk encryption	H	In Use		
34	Loss or theft of USB flash memory	USB flash memory	Sensitive data on USB memory	42	Penetration testing	H	In Use		
35	Accidental security breach	Staff	Ignorance of policies	44	Policy Affirmations (PASS)	L	Development	Q2 2013	
36	Information handling error	Staff	Untrained staff	45	Information Classification Scheme	L	In Use	Q2 2013	!
37	Denial of service attack	Web servers	Poor or incorrect configuration	43	Server configuration standards	H	In Use		

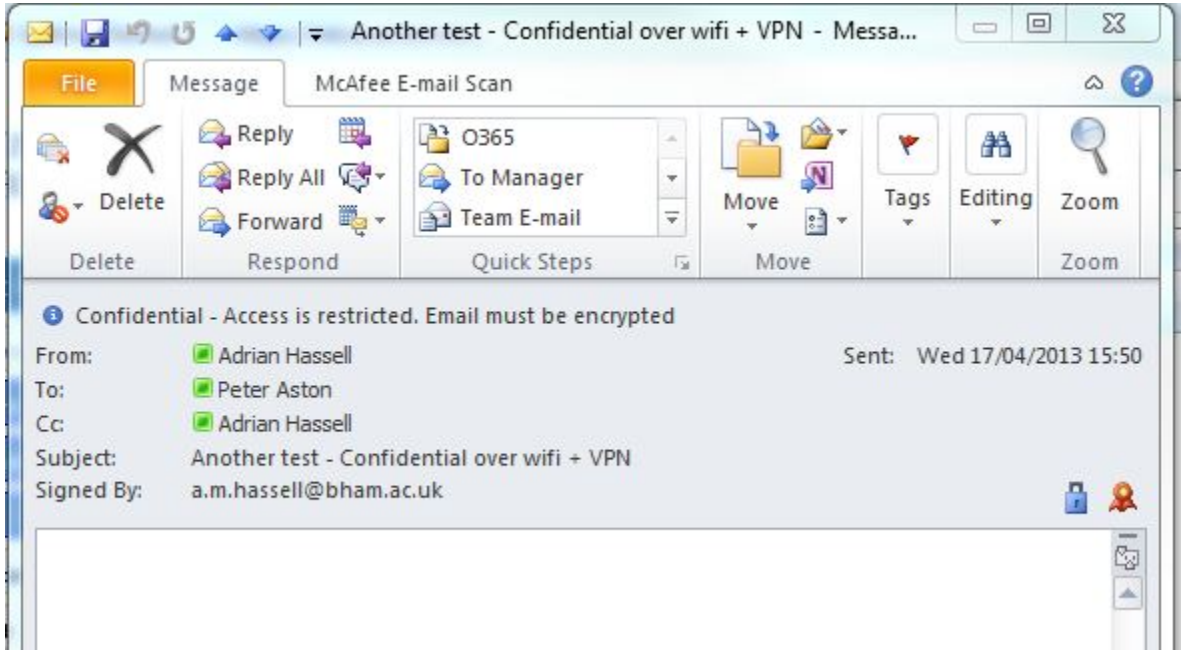
Security measures and initiatives



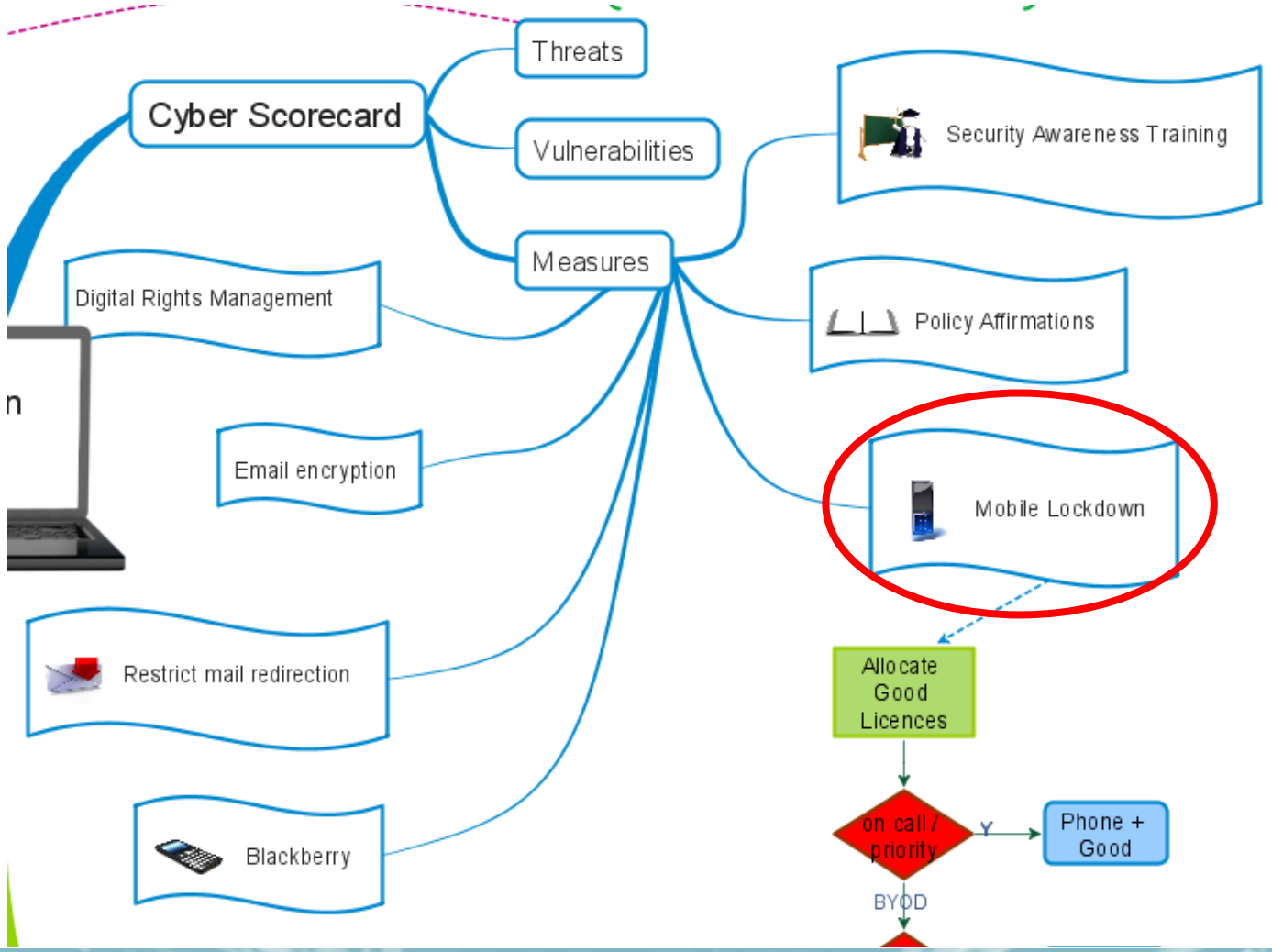
Encrypted email – menu option in Outlook



Determined by information classification



Security measures and initiatives



Mobile device security

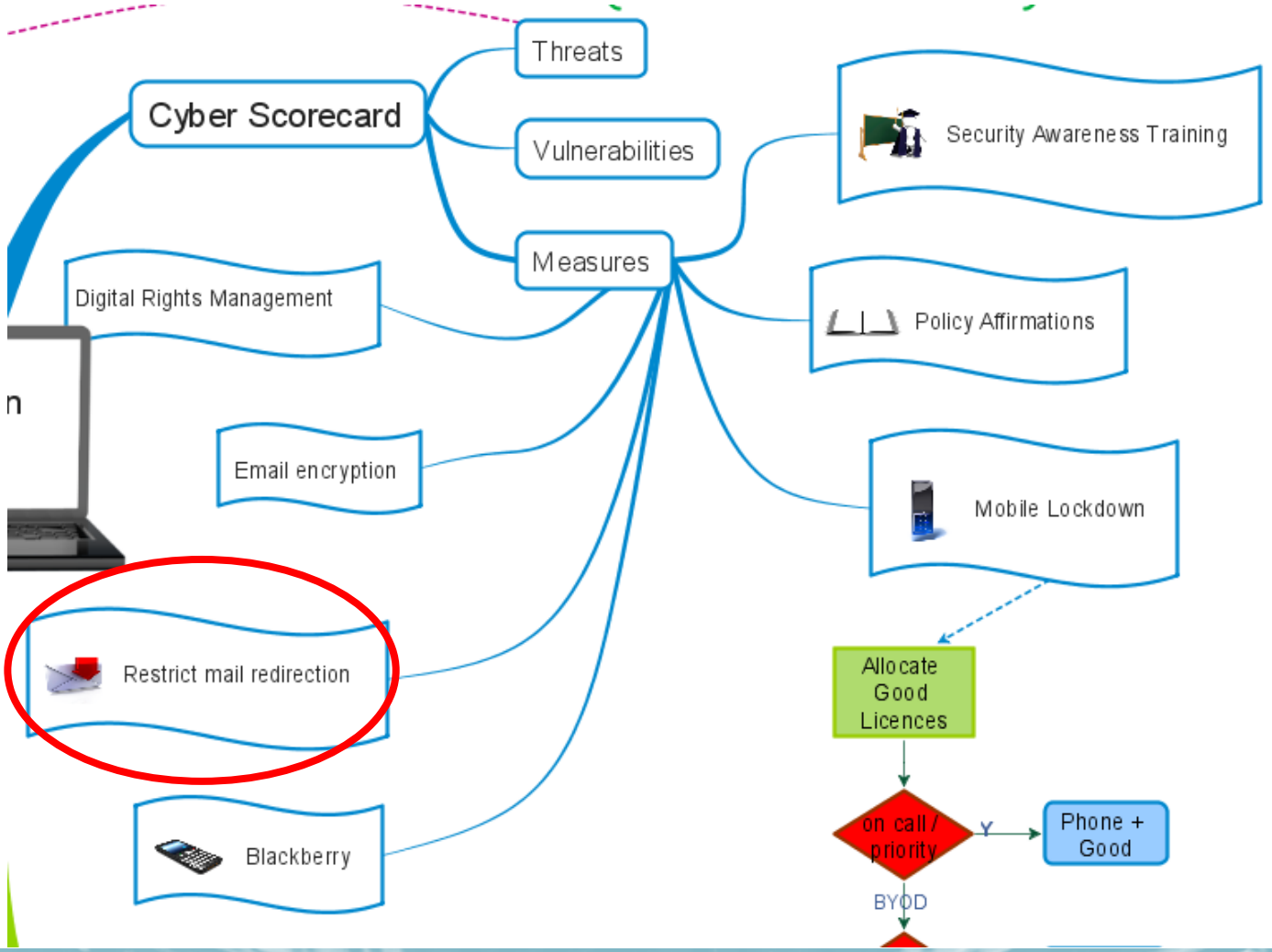
- Vulnerability: University email stored in mobile devices
  - May contain confidential information
  - Intellectual property – secrets, unpublished research
  - Personal details – subject to Data Protection Act
  - Commercially sensitive – contracts, budgets etc.
  - Possible harm to University's reputation or interests. Fines or penalties
  - Warning to universities from Information Commissioner!
- Threats
  - Casual / opportunistic
  - Targeted – press, organised crime, activists, state-sponsored

Mobile device security

- Toolset: Good Technology
  - FIPS140 certified
  - Available for IOS, Android
  - Supports mail (inc encrypted), calendar, tasks, contacts
  - Separate from other ‘private’ data on devices
  - Used by over 70 of the FTSE 100 enterprises
- Measures
  - Any email download to mobile devices must use Good
  - Exceptions recommended by Head of School, approved by Head of College
  - Non 'Good' email access from mobile devices to be via OWA – browser only without download
  - Review of adoption of Good in Spring 2014
  - Funded from local departments

  - Excludes: Blackberry, PCs, Macs

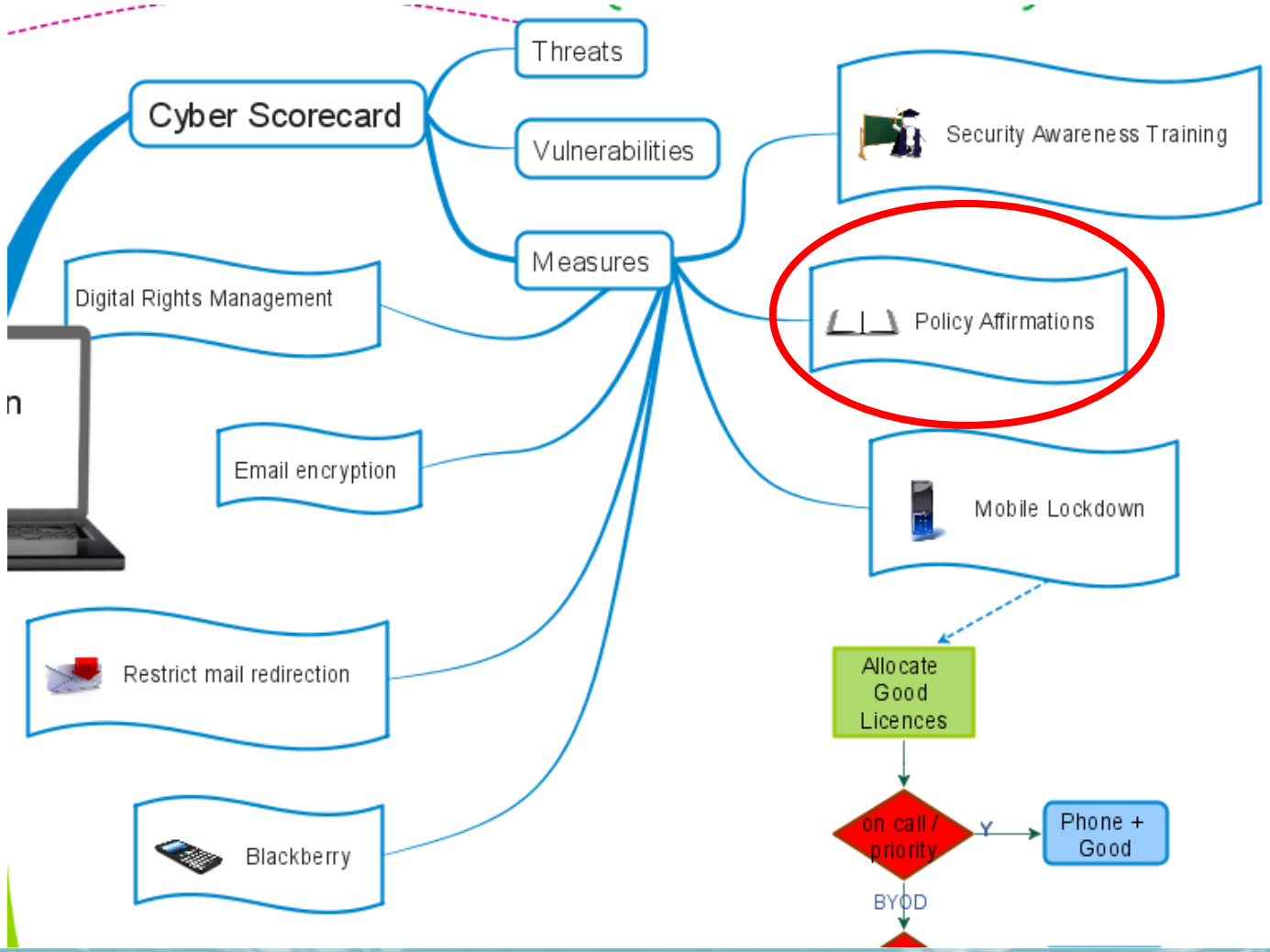
Security measures and initiatives



Email redirection

- Vulnerability: University email in insecure services
  - Based on risk assessment of email service
    - Hotmail, Gmail, Yahoo already compromised
  - Forwarding to NHS and ‘trusted’ email systems not affected
- Threats
  - Casual – widely available hacking information and scripts can be used by low skilled ‘script kiddies’
  - Targeted – hacktivists, tabloid press, organised crime, state-sponsored
- Controls / Security Measures
  - Restrict automatic mail redirection

Security measures and initiatives



Agenda

Why Information Security is an issue

External agencies

Information Classification

Enhanced security tools

Changing behaviours

Engagement

- Briefing Sessions
  - College Boards, Corporate Services, ‘all staff’ groups
- Common Documents Classification
- Information Security booklet
- Information Asset Owners & Coordinators
- Decide who needs / gets Good
- University Committees

Poacher

Advisor

Gamekeeper

Q and A