Resources for Chapter 1 – What is information security?

RESOURCES

- **Template for an information security strategy proposal**

Template for an information security strategy proposal

"Reputation is like fine china: once broken it's very hard to repair."
— Abraham Lincoln

Information risk management, or information security, is a crucial part of <ORGANISATION>'s operations. This document explains the case for improving our capabilities in this area, and provides an outline strategy to do so.

What is the point of information security?

The bedrock of <ORGANISATION> is trust. Research integrity relies upon the ability to trust data. External investment depends upon <ORGANISATION>'s reputation, especially where it comes to medical data. Sharing research data with collaborators depends upon mutual trust. Equally, students and staff need to be able to trust <ORGANISATION> with their personal information.

Without adequate information security, the reputation of the University cannot be maintained. With our foundation of trust broken, funding will be awarded to other, worthier recipients, and lucrative partnerships will be dissolved. Research papers may no longer be accepted for publication. Lawsuits and fines could bring further financial losses, compounding reputational harm, and impacting <ORGANISATION>'s ability to recruit the best and brightest students and staff.

In summary, the goal of information security is to enable the University to be, and to be seen as, a safe pair of hands. The role of the <Infosec Department> is to advise, monitor and support the University in this area.

What is the current situation?

The level of threat to the University is increasing. Previous critically damaging data breaches at other institutions (including <provide recent examples here> QMUL[1], Indiana University[2], Iowa State University[3] and the University of Maryland[4]) have shown that universities are seen both as sources of saleable personal information, and as resources for attackers to repurpose to suit their own needs. Information from official sources also indicates that research data may be sought for the purposes of industrial espionage. Finally, it is known that nation states are focusing strongly on the arenas of online attack and defence, and may see <ORGANISATION> as a source of intelligence.

Within <ORGANISATION>, incidents are increasing in frequency and severity <stats here>. The frequency of near misses and the risk of a catastrophe are also at <high/alarming/unacceptable> levels. <Give concrete example here>.

Other issues of relevance to our sector include:

An increasing appetite for partnerships and research collaborations handling sensitive information.

A strategic emphasis on an integrated approach to education, research and innovation.

The widespread use of unsuitable tools, such as email, for handling highly confidential information.

A lack of a coordinated approach to information security across <ORGANISATION>.

Information security is perceived as someone else's problem, but it is everyone's responsibility.

A widespread view that information risk management can be left until more important issues have been addressed.

What are our options?

Do nothing

This is, as should be clear from the previous section, untenable. As threat levels are increasing, doing nothing actually means losing ground. This approach will result in increasing numbers of serious incidents, loss of reputation, and other damage to the University.

Apply stringent security measures across the whole University

This option would define a set of detailed security measures suitable for most environments, and apply them to all of the University; certain areas of greater risk would be subject to enhanced security measures. This approach has the advantage of being consistent, and is often adopted in corporate environments.

However, this "one size fits all" approach is inevitably going to be overkill in some environments, while inadequate in others. The University structure is also federated, so blanket implementation is likely to be a challenge to implement.

In short, this approach has two intrinsic defects.

- We cannot do it: it is too expensive and it is impractical.
- We should not do it: it is incompatible with the principles of federation, openness and academic freedom.

[1] http://my.qmul.ac.uk/news_and_events/2014/121863.html
[2] http://news.iu.edu/releases/iu/2014/02/data-exposure-disclosure.shtml
[3] http://www.news.iastate.edu/news/2014/04/22/serverbreach
[4] http://www.umd.edu/datasecurity/ and http://www.wusa9.com/story/news/local/2014/03/26/university-of-maryland-congress-data-breach/6942023/

A targeted approach

The University has legal and contractual obligations which inform our overall tolerance for risk. A targeted approach to information would focus most investment on areas of greater risk, such as those handling personal data, while providing advice and support to all University members. This would foster a culture of responsible risk taking consonant with <ORGANISATION>'s enquiring and innovative nature.

To achieve this goal, <ORGANISATION> could create three sets of good practice baseline recommendations, each relating to a level of risk. University members would be given the right support to select and tailor the most suitable baseline in any given situation. Their decisions on information risk would be independently validated[5] against the University's risk tolerance, while operational activities to manage information risk would be integrated into normal reporting lines.

The underlying principles of the targeted approach are as follows.

- Independent oversight by the <Infosec Department>.
- Integration with other normal University activities.
- Tailored security measures based on good practice, risk tolerance and business needs.

Recommended option

It is recommended that the University adopt the targeted approach to information risk management, to enable a pragmatic, responsive and cost-effective implementation of its requirements.

What action is required?

<ORGANISATION> should develop its information security approach as follows.

1. Assign overall responsibility for information risk management to a top level role.
2. Appoint a Senior Information Risk Owner for every <School/Department/Faculty>.
3. Create a detailed plan for independent governance of information risk that avoids conflicts of interest, includes segregation of duties, and leverages <ORGANISATION>'s existing resources and expertise.
4. Engage further with key areas handling medical, personal and other sensitive information to assess risks and requirements.
5. Develop information risk management baselines.
6. Formally integrate information and strategic/local risk management processes.
7. Invest in a broad-reaching programme of awareness and support for University members, with additional support for key areas. The key message: Information security is everyone's responsibility.

[5] In order to avoid the classic problem of "marking one's own homework".