Information Security Special Interest Group Meeting Notes, 7th May 2015

Update on Information Security Improvement Programme, Jonathan Ashton

University is undertaking a major IS improvement programme. Activities include:

- Developing the capacity and capability of the Information Security team to provide better service
- Created one information security team
- Engaging with the collegiate University to understand local information security challenges, requirements and ideas
- Establishing an information security governance framework to provide support, guidance, oversight and assurance
- Delivering an information security improvement programme to develop the collateral we need

Areas of focus include:

- New website to improve users experience and opportunities for engagement
- Reviewing security arrangements of webservers
- Developing baseline security standards
- Cloud security framework
- Improved training and awareness programme
- Better incident response, coordination and communication

Benefits for ITSS

- Greater support from the centre
- Practical tools, templates etc.
- Baseline security standards to help you understand what "secure" looks like and support business case for improvement.

What we need from ITSS

- Secure IT systems!
- Engage with the team and tell us what help and support you need
- Communicate

  Let us know what you are up to (infosec@it.ox.ac.uk)
  Responding to surveys, questions etc.
  Reporting incidents (oxcert@it.ox.ac.uk)
- Set the baseline requirements
- Promote security within your units

Webserver security survey update

Results of Survey

- Over 3000 “webservers” detected
- Approximately 120 emails sent out
- 158 survey responses
- Approximately 15 other responses
- Many thanks
- Good news overall but areas of improvement identified

Areas of risk/improvement

- Data storage
- Input validation
- Third party/custom code

What next

- Defining and agreeing baseline security requirements
- Carrying out a more detailed review of the highest risk sites identified from the survey
- Piloting that process with a couple of sites (already chosen)
- Looking to include external vulnerability assessments
- Assist units with remediation of risks
- Main objectives are to find out what the real risks are and what needs to be done
- Looking ahead to future possible services etc.

Update from OxCERT

- OxCERT gave an update on recent threats and incidents they had dealt with.
- Focus was on the prevalence of malware
- Quantity of malware is growing exponentially
- Not sufficient to simply rely on traditional antivirus
- Units need to prepare for the fact that they will get malware (layered defence including detection and response).
- Strongly recommended to re-install machines that are compromised so have a plan in place
- Segregate untrusted networks (e.g. for BYOD) from critical departmental networks/systems.

Departmental perspective on an incident

- An IT Officer gave an update on a recent incident that led to financial fraud against an individual

- Lessons learned included layered defence; firewalls and access control policies; testing of security controls; enforcement of strong passwords

Group discussion and actions

- There was a lot of enthusiasm and support for information security and many good questions and interesting discussions.
- Very positive feedback on the idea of "baseline" security standards and willingness to peer-review
- ITSS want to see better services and support from the centre.
- One specific example was a definite interest in a vulnerability scanning/penetration testing service. At least one unit has followed up on these discussions and may lead to a follow-on session at the next SIG meeting.
- Interest in spawning technical/practical workshops to follow-up on some issues.
- Desire to have termly meetings of a similar format but with more time for questions as part of the schedule.
- Desire to extend the meeting in the pub next time (though mainly this was being pushed by the presenters!).