ISC11D035

Title:	**Annual Security Review & Penetration Testing**
Author:	Paul Hooper (ISD)
Date:	26 January 2012
Circulation:	ISSC - 3 February 2012
Agenda:	ISC11A002
Version:	1
Status:	Open

Issue

To report on the annual security review and penetration testing for the previous year..

Recommendation

Recipients are invited:

- To receive the report.

Resource Implications

No change to service is required and therefore there is no impact on resources.

Equality and Diversity

The report has no impact on groups with protected characteristics.

Timing of decisions

No decisions are required.

Further Information

- Raymond Scott (ISD), x3561, r.scott@uea.ac.uk

Background

Following a hacking attack on servers in the Climatic Research Unit (CRU), ISD was asked to undertake a review of the security of the UEA Network. ISD engaged with an external security company to aid them in the discovery and make recommendations for change on security issues.

Discussion

Annual Security Review & Penetration Testing

Background

Following a hacking attack on servers in the Climatic Research Unit (CRU), ISD was asked to undertake a review of the security of the UEA Network. ISD engaged with an external security company to aid them in the discovery and make recommendations for change on security issues.

A programme of work was constructed to address the vulnerabilities and recommendations for change made by the external auditing company.

Year two funding of the security project has not been made available. As a result, this year's work is focusing on internal auditing and improvements where no or little funding is needed. When external auditing is done we will be able to understand the risks but not necessarily be able to provide an enterpr

Work undertaken in the previous year

One area that required further investigation after the initial report from the external security company was for UEA to perform additional internal audits across schools and departments within the University. In 2010/11 the following schools and faculties completed an audit with the co-operation of Faculty IT Support staff:

- HUM: (ART, AMS, FTV, HIS, LCS, LDC, MUS, PHI, PSI)
- FMH: (AHP, MED, NSC)
- SSF: (DEV, ECO, EDU, LAW, NBS, SWP)
- SCI: (BIO, CHE, PHA, CMP, ENV, MTH)

Appendix A shows the methodology used to undertake these audits. The audits highlighted areas where further work and understanding is needed. The main areas needing further investigations include:

- Greater understanding of requirements for scientific equipment
- How different types of data are being managed (how much data exists, where it is stored, access control / rights, backup facilities, resilience requirements)
- Improvement of asset management

Following on from the Integration Project responsibility for implementing the recommended changes made in the audits now passes to the Faculty IT Support team. This new team have been constructing a programme of work to complete security actions highlighted in the audits and to investigate areas where further information is required.

In 2010/11 penetration testing was undertaken by an external security company in several areas. A secondary review was completed of CRU which highlighted additional work that was needed. With the support of the Faculty IT Support team and the local UNIX support team these additional actions were completed.

Further penetration testing was undertaken on core central information systems which highlighted several tasks that needed to be undertaken. This work was prioritised and scheduled with the owners of the systems. All tasks scheduled for 2010/11 were successfully completed with some additional actions scheduled for 2011/12.

Work to take place in the current year

At the end of 2010/11 a framework agreement was reached with an external security company 7Safe to provide consultative services. It's planned that the ISD will work with 7Safe to perform a series of IT security audits, penetration tests, assessment of internal auditing processes, advising on user education and any high impact security events that take place. A roadmap of work has been constructed for the next five years which is being finalised.

It's intended that further audits and penetration tests will take place in the following areas:

- UEA London
- VCO
- ENV Scientific Equipment
- Filestore / Email Systems

Internal Audits will continue within other areas of the University, including:

- Central Units & new departments created as a result of the Integration Project
- Associated Companies using UEA Network (e.g. Students Union)

Appendix A: UEA School ICT Security Audits (paper presented to ISSC in June 2010)

Each school, department and associated or external company using UEA ICT infrastructure will need to be included within a University wide ICT infrastructure security audit. This will allow us to identify insecurities and bad practice within the university and to identify areas where improvements to ICT services may be needed to accommodate enforcement of best practice.

Methodology

Each school, department or company will be sent a security audit template. The member of staff in charge of IT Support for that area will then answer the questions being asked within the template.

This template will then be sent back to ITCS for review. A team of ICT experts will then meet to discuss the results in the template. This team will compose of someone from networking, systems, desktop services and if needed experts in database and web services. Network scans will take place for the area being reviewed to identify equipment and practices deemed to be unsafe that may have been missed by the IT support staff completing the template.

After completing a review, recommendations will be recorded in the template against the areas of concern. A meeting will then take place with the IT Staff who completed the template to discuss the answers that they gave and to allow for more probing questioning to take place. Discussions will take place on the recommended changes to identify any issues in implementing the changes and to allow for amendment of the recommendations as a result of the discussions.

An action log will be completed in agreement with the IT Support staff on the changes that should be made with timelines for completion. Subsequent meetings will be booked to monitor progress and to highlight any problems that may be occurring during implementation.

Audits that may be considered as contentious will be reviews by the security project operational board.

Accepted Areas of Risk

As schools, departments and companies go through the process there maybe areas that are identified that are unable to be changed to meet best practice. In these circumstances the details of the situation will be recorded in a risk log which is located on a secure network share that the security project team have access to. When the item is recorded the security project manager will be alerted who will discuss the situation with the security project team and operational board. Where possible mitigation will be identified and put in place and the likelihood and impact of the risk recorded. Regular reviews of the risk log will take place to re-assess the risk each item recorded and the mitigation put in place. Appendix B shows an example risk log that is being used.

Example

Scientific equipment identified in a school running with software that is only compatible with an old outdated and unsupported operating system e.g. windows NT4. Attempts to find updated software have revealed that none are available. The scientific equipment would be prohibitively expensive to replace and has a requirement to be running on a UEA network connection.

The details of this risk will be recorded. Mitigation to the risk will look at the possibility of isolating the equipment on the network or providing a sandbox environment on a supported OS. This would allow the equipment to continue running with some degree of protection...