ISC10D020

Security Project - Progress Report

This paper provides an outline of the work that has been identified in response to the security assessments that were undertaken following the security breach in CRU. ISD is taking a project management approach to the work which has a wide ranging impact across UEA. Much of the work is of a highly technical nature and this is being overseen by the ISD management team who are acting as an operation project management board for the project. A further aspect to the work involves changes to, or the introduction of, policy and where appropriate the ISD Research Board, Education Board, ICT forum and LLR forum are being consulted.

Given the high profile of the work we feel it is appropriate to ask ISSC to act as the project board for this particular project and will provide an update on progress for each meeting.

Projects Aims and Objectives

The aim of this project is to introduce safer working practices in a cost-effective manner with consideration made to the benefits gained and available budgets. The project will provide ongoing assurance to the University about security and data by providing protection of the core assets of the University without overly impinging research and teaching activity.

This project supports the key principles in the ISD Strategy 2008-13 for “Getting the basics right “, “Continuous improvement” and “Investing for the future”. The key objectives of the project include:

- Agree appropriate levels of security
- Review the current infrastructure, equipment and software being used within each school to assess if it meets appropriate levels of security
- To implement UEA wide business processes and policy to accommodate improved security levels within each faculty and University department
- Provide an agreed security model with levels of security appropriate for various services
- To implement improvements in security to current infrastructure and changes in the current infrastructure to support additional technologies (e.g. Mac, Linux)
- To implement enhanced levels of security in desktop PCs, servers, email, filestore, network, mobile devices/storage and personal behaviour
- Provide a mechanism to demonstrate appropriate levels of security have been implemented
- To implement a process for agreeing changes (ITIL)
- To implement improvements in guidance and training on security
- Produce guidance on assurance models and engendering an IT conscious culture

Summary of key work and progress for 2010/11

Inevitably the network problems in the run up to Christmas have taken priority and this has caused some delays to the security project and we will need to make some changes to the project schedule, including a more detailed review of the actions that are required in the network area.

Work has been done to identify the investment requirements to support the work of this project, and while it has been possible to absorb some of this into the ISD Capital and Revenue plans there still remains a significant budget shortfall and we require an additional capital investment of £850K and an revenue investment of £101,000. The funding request is being considered by ET. A breakdown of the budget proposal is included as an Appendix.

Strand 1: Review Policy and Strategy (Steve Mosley)			
Status	**Item**	**Progress**	**Recommended Changes**
Completed	Review Computer Suite Access Policy		
ON TRACK	*Review, agree and production of security policy, guidance and training (25/10/10 - 31/08/11)*	Revisions to GISP are being presented to ISSC on 4th Feb. These include revisions to password assignments, password checking and enforcement and system administrator password policies. Work has now started on information classification, data retention policies, anti-malware and security controls, ready for the June ISSC.	
BEHIND SCHEDULE	*Procurement of annual security audit/penetration testing by 3rd party (25/10/10 - 07/02/11)*	Discussions have taken place with Steve Boardman to establish if we can recommend a single tender to 7safe or if we need to approach several companies who are also CHECK accredited. Given the nature of the work a single tender was considered to be more appropriate. A requirements document and single tender procurement document is currently being constructed for approval.	We would like to add a month to the timescale; we do not think that this will cause any impact.
ON TRACK	*One off detailed security review (02/11/10 – 04/04/11)*	7safe have completed the review of CRU ICT after the changes were completed. A report has been received and is being reviewed to asses for further actions. CIS Applications are being reviewed by 7safe this week.	
BEHIND SCHEDULE	*Develop policy for dedicated and regular service downtime for appropriate patching of systems (01/11/10 – 01/02/11)*	ITILPM has only recently returned to work causing a delay in the start to this work.	To mitigate the delay all systems are being patched to the latest release.

ON TRACK	*Review Disaster Recovery (DR) Plan (02/08/10 – 23/11/11)*	High level ISD Policy with SPC Team has been completed. Lower level plans for systems are not due to start yet.	
	Review of UEA companies connected to the network (02/02/11 – 29/03/11)	Work in this area is not due to start	
	Create and maintain central registry of servers with BP (05/04/11 – 18/04/11)	Work in this area is not due to start	

Strand 2: System Changes (Jon Woodley)			
Status	**Item**	**Progress**	**Recommended Changes**
ON TRACK	*Review Approach to password changing (25/10/10 – 17/12/10)*	The initial technical investigation has taken place and is subject to policy changes that are due to be submitted to ISSC.	Pending the completion of policy changes.
	Identify and remove local server usernames & root/administrator accounts (04/04/11 – 20/09/11)	Work in this area is not due to start	
	Reduce dependency on anonymous LDAP usage (with aim to remove ultimately) (24/05/11 – 21/12/11)	Work in this area is not due to start	

Strand 3: Data Security Changes (Paul Hooper)			
Status	**Item**	**Progress**	**Recommended Changes**
ON TRACK	*Review of data storage SLD and service description (25/10/10 – 19/11/10)*	The initial technical investigation has taken place and is subject to policy changes that are due to be submitted to ISSC.	Pending completion of records management policy and records retention schedules.
ON TRACK	*Procure and implement data encryption tools for desktop PC/Laptops (22/11/10 – 18/03/11*)	Systems team have item in POW for filestore encryption but not email. The email element to this strand	The email element to this strand will be moved to a separate item with an option approasial / recommendations paper to be produced for 6 weeks time.
ON TRACK	*Review Mobile devices / laptop security risks and implement solution (25/10/10 – 21/03/11*)	Systems team will be looking at mobile devices whereas DTS will be looking at laptops. A	This item will be changed to only include mobile devices.

		requirements and recommendations report is going to the ICT Forum in Feb and then onto ISSC for agreement.	Laptop security will be added to desktop changes as a separate item. Data security on both devices will be moved to the data encryption item.
BEHIND SCHEDULE	*Secure USB Pens with one-off devices and implement associated infrastructure (17/01/11 – 28/02/12)*	Work has not started in the area as yet.	Work in this area can easily be caught up which will allow the item to remain on-track.
Completed	*Develop growth in research storage to prevent local storage of data (25/01/11 – 28/03/11)*		
	Develop secure equipment and media disposal service (01/02/11 – 23/08/11)	Work in this area is not due to start	
	Development of data archiving service (01/08/11 – 03/10/11)	Work in this area is not due to start	

Strand 4: Email Changes (Jon Woodley)			
Status	**Item**	**Progress**	**Recommended Changes**
BEHIND SCHEDULE	*Develop best practise on email mgt and use (conditions of computer use) (25/10/10 – 07/02/11)*	The main guidance was developed just after the CRU issues. Amendments are yet to be made to include policy on email archiving.	Dependency on completing the ICO undertaking exists causing the delay. A meeting is planned to occur on 2nd Feb to review what is required.
ON TRACK	*Develop email archiving (08/02/11 – 17/10/11)*	Settings to be informed by policy on email management and data retention policy. Solution has been implemented and is currently running a pilot. This item will address the use of insecure and corruptible .PST files. Stages involved in the live rollout of this item are : • Refer to best practice of email mgt for requirements • Assess current solutions • Perform Proof of concept	Remains on-track but delays are expected if the email management policy on archiving of emails is not finalised.

		• Purchase product • Pilot solution & gain feedback for changes • Ensure DR plans are in place and tested • Provide documentation on use • Initial Go live (applied to user mail box which will be rolled out on a dept by dept basis) • Assess requirements for import of .PST files • Manually import .pst files (in partnership with Quest) • remove ability to use .pst files	

Strand 5: Server Changes (Jon Woodley)			
Status	**Item**	**Progress**	**Recommended Changes**
ON TRACK	*Develop Guidelines to setup servers (29/11/10 – 11/04/11)*	Work in this area has started and a draft document will soon be completed.	
	Investigate open ports and close inappropriate ones (12/04/11 – 21/06/11)	Work in this area is not due to start	
	Consolidate School servers and provide central solution where appropriate (22/06/11 – 26/07/11)	Work in this area is not due to start	

Strand 6: Desktop PC Changes (Dominic Belisario)			
Status	**Item**	**Progress**	**Recommended Changes**
BEHIND SCHEDULE	*Revise desktop security guidelines (25/10/10 – 24/12/10)*	Work has started in this area but both DTS and SPC teams need to work together to produce the final document.	The project manager will arrange a meeting between the two groups to establish the requirements. A revised end date of 31st March is recommended.
BEHIND SCHEDULE	*Recommend guidelines for 3rd Parties who support systems used by UEA* (06/12/10 – 31/01/11)	Work in this area has not started.	
BEHIND SCHEDULE	*Develop Virus patch dashboard (10/01/11 – 08/03/11)*	SCCM Reporting needs to be setup to allow this work to continue. Free Training provided by Viglen	DTS need to book the SCCM training with Viglen and develop

		as part of the Managed PC Procurement project will enable DTS and Systems Team to setup SCCM reporting.	basic requirements document.
	Review Desktop & OS Selection Policy (01/02/11 – 11/04/11)	Work in this area is not due to start	
	Check all public PCs are physically secure (09/03/11 – 22/03/11)	Work in this area is not due to start	
	Install University approved malware and spyware software on PCs and Servers (23/03/11 – 12/07/11)	Work in this area is not due to start	
	Review if we block/limit use of USB devices (ensuring only secure devices are used) (12/04/11 – 19/07/11)	Work in this area is not due to start	
	Resolve desktop/SAN sync issues (13/07/11 – 26/07/11)	Work in this area is not due to start	
	Identify equipment running unsupported OS + fix (27/07/11 – 02/11/11)	Work in this area is not due to start	
	Move from remote desktop access on PC to server based remote desktop (01/08/11 – 17/07/12)	Work in this area is not due to start	

Strand 7: Security Implementation and Advice (Paul Hooper)			
Status	**Item**	**Progress**	**Recommended Changes**
ON TRACK	*School level security audit / checklist (25/10/10 – 28/02/11)*	A draft of the security audit template has been completed and will be used in the individual school reviews. A school level checklist has yet to be compiled.	

BEHIND SCHEDULE	*Science Faculty:* recommend changes (02/08/10 – 28/02/11)	CRU and BIO/MTH have been reviewed with BIO/MTH in the process of completing the recommended changes. Areas that are investigated in the review include: • Authentication of laptops/desktop PCs and servers (Windows/Mac/Linux) • Isolation or upgrading of PCs running outdated operating systems attached to scientific equipment. • Securing existing laptops/desktop PCs (physical and software) e.g. removal of admin rights • Assessment of where data is stored and moving this data to a central secure solution. • Assess if additional staff need to move to Outlook OWA. • Assessment of servers their setup and use with suggested changes in practice.	The timescales for work within the SCI faculty are overly optimistic. It is proposed that work within SCI continues past the end date and is run in parallel with the other faculty reviews. This would require a revised end date of 14/06/2011.
	Humanities and Arts (ART,AMS,FTV,HIS,LCS,LIT,MUS,PHI,PSI): recommend changes & implement (07/02/11 – 25/03/11)	Work in this area is not due to start	
	Social Sciences Faculty (DEV,ECO,EDU,LAW,NBS,SWP): recommend changes & implement (28/03/11 – 20/05/11)	Work in this area is not due to start	
	Faculty of Health: recommend changes & implement (23/05/11 – 06/09/11)	Work in this area is not due to start	
	Associated Companies/Collaborative Groups and Partner Institutions (01/08/11 – 23/04/12)	Work in this area is not due to start	

Strand 8: Network Changes (Pete Andrews)			
Status	**Item**	**Progress**	**Recommended Changes**
BEHIND SCHEDULE	*Replacement of DNS/DHCP & NetReg solution (01/10/10 – 29/07/11)*	The manufacturer meetings have been completed. Work was due to take place on the "publish tender document" but the network core replacement work has caused a delay in this area. The date for publishing the tender document is now estimated to be at the end of Feb with a subsequent knock-on effect to the remaining items of work in this area. When complete this piece of work will allow the following functionality: • Ensure only UEA registered equipment is on the network • Process to remove unused network addresses from DNS/DHCP	Propose moving end date to 30th Sept 2011. This would have an impact on start of year. As a consequence it's recommended to assess the impact of delaying this item until next academic year.
ON TRACK	*Review appropriate design for network segmentation (24/09/10 – 31/07/12)*	The network team have highlighted that the item to construct a matrix of network access/permissions will pose them problems. Due to current workloads they are unable to perform this and have requested, as this is a broader element than just networking, that another team/person collates this information.	Propose that the Network Team, Project Manager and ICT Director establish a different approach to move this item on. • Broccade consultancy could be used to aid with the initial setup to allow CIS Applications and Residences to be segmented with the creation of a DMZ.
BEHIND SCHEDULE	*Switch Configuration (24/09/10 – 08/08/11)*	Explore 802.1 for VOIP is behind schedule and more understanding of the required infrastructure is needed (so that changes do not affect the live service). Broccade consultancy could be used to aid with the initial setup.	Recommendation as per previous item.
ON TRACK	*Review Network Core Replacement and Firewall Replacement (02/08/10 – 28/07/11)*	Network core has been replaced. Further time is needed to resolve issues with legacy setup that existed on old cores.	

ON TRACK	*Review Network Tools (23/07/10 – 26/07/12)*	The review of current network tools is in progress. Work on campus peer-to-peer usage and interdepartmental usage statistics has not started.	

Strand 9: Research Support Changes (Chris Collins)			
Status	**Item**	**Progress**	**Recommended Changes**
ON TRACK	*Process for sign-off of IT aspects of research grant applications* (06/12/10 – 09/05/11)	Work is on schedule with the current processes being mapped, documentation on services and associated costs and a checklist for applications being completed. Work is continuing with gaining agreement with the user community and research board.	

Strand 10: Risk Log (Paul Hooper)			
Status	**Item**	**Progress**	**Recommended Changes**
BEHIND SCHEDULE	Create Risk Log (25/10/10 – 10/01/11)	Work has not started in this area	Work in this area can be caught up quickly with minimal impact.

Risks Associated with the Project

Budget

Risk	Risk reduction strategy/contingency	Owner	Likelihood (H, M, or L)	Impact (H,M, or L)
Current budgets available are not sufficient to cover costs of the project	Gain support of the executive team to fund the project (critical risk to project)	JC-F	**H**	**H**
Difficulty in securing full funding E.G. Cost Escalation (cost growth)	• Close Maintenance of budget • Early warning to project board	PH / Strand Managers	**M**	**M**
Several items in the plan such as networking are reviews and may therefore identify a requirement for additional capital expenditure	• Monitor progress of the project and highlight to the board if further expenditure is required	PH	**M**	**L**
Budgets may be removed as the impetus to change lessens over time or government funding to Universities is reduced	• Keep communicating the need within the University • Gain support of the executive team	PH	**M**	**M**

Communication

Risk	Risk reduction strategy/contingency	Owner	Likelihood (H, M, or L)	Impact (H,M, or L)
Far-reaching effects of the project within UEA (Interface into other Business Areas)	• Influence other groups • Develop work around	PH	**M**	**L**
Lack of willingness across the University to enforce emerging plans or resistance from some people to change how they do things – *Lack of buy-in*	• Communicate clear message of why change needs to happen and benefits of alternative practice. • Executive team to define new policy and communicate need	PH	**H**	**M**
Working with collaborative/partner institutions and subsidiary companies of the University may introduce communication problems	• Create full communications plan identifying when communication needs to happen, what the message is and to who it should be communicated to	PH	**M**	**M**

External to project, but within UEA

Risk	Risk reduction strategy/contingency	Owner	Likelihood (H, M, or L)	Impact (H,M, or L)
Another department / partner / research collaborative group not adopting the security changes	Executive Team and project board to communicate need to change and the benefits to be gained	Strand Managers	**M**	**M**

Partner Institutions / Research collaborative groups or University subsidiary companies may see the changes as over-impinging and take their business elsewhere.	Executive Team and project board Communicate need to change and the benefits to be gained	PH / Strand Managers	**M**	**L**
Software suppliers providing new tools may not be able to deliver product/support for the product that meets University needs	Produce a detailed requirements document in the procurement process	PH / Strand Managers	**L**	**M**

External to UEA

Risk	**Risk reduction strategy/contingency**	**Owner**	**Likelihood (H, M, or L)**	**Impact (H,M, or L)**
Likelihood of new / changing legislation	Monitor external environment for changes that may impact on this project	Project Board	**M**	**M**
Rapid change in technology may lead to new challenges or increase the scope of the project	Monitor new and emerging technologies	PH / Strand Managers	**M**	**M**
CRU situation may occur elsewhere increasing attempts to breach security	Monitor for potential problems.	Project Board	**L**	**M**

Plan

Risk	**Risk reduction strategy/contingency**	**Owner**	**Likelihood (H, M, or L)**	**Impact (H,M, or L)**

Slippage with the project schedule	Provide regular highlight report on progress and identify areas where issues are causing or have potential to cause delay	PH	**M**	**M**

Quality

Risk	**Risk reduction strategy/contingency**	**Owner**	**Likelihood (H, M, or L)**	**Impact (H,M, or L)**
Clear quality standards have been (or will be) established for the project and its products. – *How Success is measured*	• Acceptance Test & sign-off for system changes • Annual audit and penetration test to identify how consistently improved security is being applied and any problem areas	PH	**L**	**M**
IT staff may create local accounts / give admin rights in order to get around an issue that they cannot resolve.	Monitor for issues and report the project board	PH / Strand Managers	**M**	**L**
Changes are not applied consistently across the University	Quality assurance to audit for consistent application of changes	PH / Strand Managers	**M**	**M**
Changes being implemented may have impact on the operational effectiveness of the University.	• Trial changes before implementation with full testing plan • Produce document on mitigation needed to reverse any change made	PH / Strand Managers	**M**	**H**

Reputation

Risk	Risk reduction strategy/contingency	Owner	Likelihood (H, M, or L)	Impact (H,M, or L)
Deliverables have adverse affect e.g. network changes cause University wide problems	Trial all changes before implementation. Monitor for issues and report to project board	PH/Strand Managers	**M**	**H**
ICT infrastructure becomes too rigid and people find the University hard to work in	Consult with each community before and after the change to establish its impact. Report issues to the project board.	PH/Strand Managers	**L**	**M**

Resources

Risk	Risk reduction strategy/contingency	Owner	Likelihood (H, M, or L)	Impact (H,M, or L)
Lack of understanding of project management standards by everyone in the project team	More communication of standards	PH	**L**	**L**
The project is likely to need a large number of workdays - *Confidence in level of Staffing*	Dependant on project plan	PH	**H**	**M**
The project team will be expected to support end-users after project completion. - Management to Service *(ongoing support = low risk, no support beyond*	Build in Handover into Programme of Work	Strand Managers	**L**	**M**

project closure = high risk)				
The activities of project team members will depend on different line managers and departments within the University *(e.g. a high number of different managers may obstruct coordination of the team)*	Good Communication between department heads/line managers	PH/Strand Managers	**H**	**M**
Teams are not able to resource project tasks due to conflicting priorities or work needed in other POW items	Negotiate time with Directors / Heads of Department	Strand Managers	**L**	**M**
Key staff leave or are off ill	• Manage staff holiday during the critical installation period. • Develop agreements with partner institutions to draw upon staff with corresponding skill sets. • Use contractors if required.	PH/Strand Managers	**M**	**L**

Scope

Risk	**Risk reduction strategy/contingency**	**Owner**	**Likelihood** **(H, M, or L)**	**Impact** **(H,M, or L)**
Lack of understanding of the current problem	Communicate reasons for change to ISSC and disseminate to wider University community	PH / Project Board	**L**	**H**
Mismatch between Auditors and operational	Monitor and report issues that occur to the project	PH /	**H**	**M**

requirements of ICT in an HEI	board	Project Board		
Innovation or the introduction of new features. - *Scope Creep*	Resource change control with full Project Board agreement	PH / Project Board	**M**	**M**
Scope of this project is too big for the given time span	Project Board to monitor progress	PH / Project Board	**M**	**M**

Appendix – budget

Deliverable	2010/11			2011/12			2012/13		
	Capital (one-off)	Revenue (one-off)	Revenue (recurrent)	Capital (one-off)	Revenue (one-off)	Revenue (recurrent)	Capital (one-off)	Revenue (one-off)	Revenue (recurrent)
Annual Security Audit & Review Firewall Rules			£25K			£25K			£25K
One-off Security Audit		£20K							
Two-Factor Authentication				£10k		£2k			£2k
Network and Server Logging				£20k		£5k			£5k
Data encryption tools for PC/Laptop/Email	£50k		£5k			£5k			£5k
Increase Research Storage	£250k			£250k					
Data Archiving				£100k		£5k			£5k
Data Publication	£25k								
Secure USB Pens & Limit/Block USB use	£10k			£20k		£5k			£5k
Data Versioning				£20k		£8k			£8k
Document Collaboration				£20k					
Develop Email Archiving / Review Email Quota	£70k		£8k			£8k			£8k
Physical security of Public PCs	£10k								
Sandbox				£25k		£5k			£5k
Mac Infrastructure				£20k		£5k			£5k
Remote Desktops				£5k					
Replacement of DNS/DHCP & NetReg	£50k		£24k	£50k		£24k			£24k
Network Segmentation (interim solution) & Implement changes to firewall rules		£10k							
Network Core & Firewall Replacement							£100k		
Review Networking Tools				£20k		£4k			£4k
Sub total	£465k	£30k	£62k	£560k	£0k	£101k	£100k		£101k
Total	**£557k**			**£661k**			**£201k**		