Independent Review Team – UEA/CRU

Formal Record

Notes of Interviews with Jonathan Colam-French (Director Information Services), Iain Reeman (ICT Systems Director) and Mike Salmon (IT Manager to the CRU - 40% time)

Interviewers Sir Muir Russell & Prof. Jim Norton

Interview carried out at UEA on 27th January 2010

Introduction

1. Sir Muir set the scene by reiterating the objectives of the Independent Review and detailing the members of the Review Team. He explained the purpose of the meeting as exploratory, building on the initial discussions held in December. The Review would focus on the honesty and scientific rigour with which data had been collected, processed and presented in the context of the scientific norms relevant at the time, as well as FoI issues in relation to access to both scientific data and personal data.

Background

2. Questioning established the overall University context for both Information Security and the handling of Freedom of Information (FoI) requests. A high level 'Information Systems Policy' and a related Information Security Policy[1] had been agreed and put in place five years ago under the aegis of the University Information Systems Strategy Committee (ISSC), which includes representatives of all four Faculties. Low level, detailed, security policies had been developed and put in place two years ago[2].

3. In common with other areas of the Science Faculty, the CRU operated largely independent of the central IT functions of the University. Central IS had, in recent years, made significant efforts to better support the Science Faculty and some use of central facilities (such as the Storage Area Network) had been achieved. The University IS team did not provide desktop, remote access, hosting, database or software support to the CRU, nor any quality control or assessment. CRU had their own local architecture based on a mix of individual PC based and server based processing. In common with many other research groups across the university, this was distinct from the UEA preferred model of client – server operation, see attached chart. Internet communications for the CRU were however routed over the university network and through the university firewall. The CRU had its own IT Manager (Mike Salmon) for whom CRU was 40% of his workload. The CRU had originally had no central backup

[1] The following documents were received by the Review on 8th February: "High Level Information Security Policy"; and "General Information Security Policy".

[2] A draft "Security Manual" was also received by the Review on 8th February.

arrangements for the individual researchers' PCs however Mike Salmon had introduced automated backup (using open source software) to a simple server held securely within the Central IS machine room. Jonathan Colam-French (Director Information Services) indicated that, whilst the central IT function were aware of the existence of the CRU Backup Server, they had no knowledge of the nature of the information held on the server as it was managed from the CRU.

IT within the CRU

4. Mike Salmon indicated that researchers within the CRU worked individually or in small groups. There was no master index of resources, be these data, algorithms or software. No systematic approach to the creation of metadata existed. There was no central database of underlying climate data; rather individual researchers assembled sets of data drawn from different primary sources outside the CRU (for example the Met. Office Hadley Centre for Climate Change). These might arrive by network (Janet & GÉANT), or on portable hard disks. *Secretary's Note: Mike Salmon subsequently indicated in an e-mail of 3rd February that the benefits of a central data catalogue had long been recognised within the CRU and past attempts had been made to create such a resource. These attempts had foundered on the lack of resources – research grants made no provision for this and central UEA funding had not been available.* A typical data set might comprise 10GBytes of data *(Secretary's Note: Mike Salmon subsequently clarified, in an e-mail of 3rd February 2010, that "data sets" were typically 100 – 200 GBytes and could reach 500GBytes. A simulation might use up to 20 runs and so data requirements could easily reach into the Terabyte region)*. The data might be stored locally (cheaper), on the University Storage Area Network (SAN) or split between the two. There was no policy for the systematic archiving of data. Individual researchers were responsible for acquiring or developing their own software applications (usually written in Fortran or IDL). There was no formal quality control policy or review policy.

FoI Issues

5. Jonathan Colam-French (Director Information Services) indicated that the initial response by Mr David Palmer, with respect to FoI requests related to personal data potentially held by the CRU (e.g. in e-mails), had been based around a range of issues including "disproportionate cost"[3]. Jonathan Colam-French promised

[3] In a subsequent communication, Jonathan Colam-French confirmed that a full analysis of CRU FoI requests was being prepared for the Vice-Chancellor and would be fully available to the Review.

to provide copies of both the University FoI policy documents and the IT Strategy documents.[4]

Lessons learnt

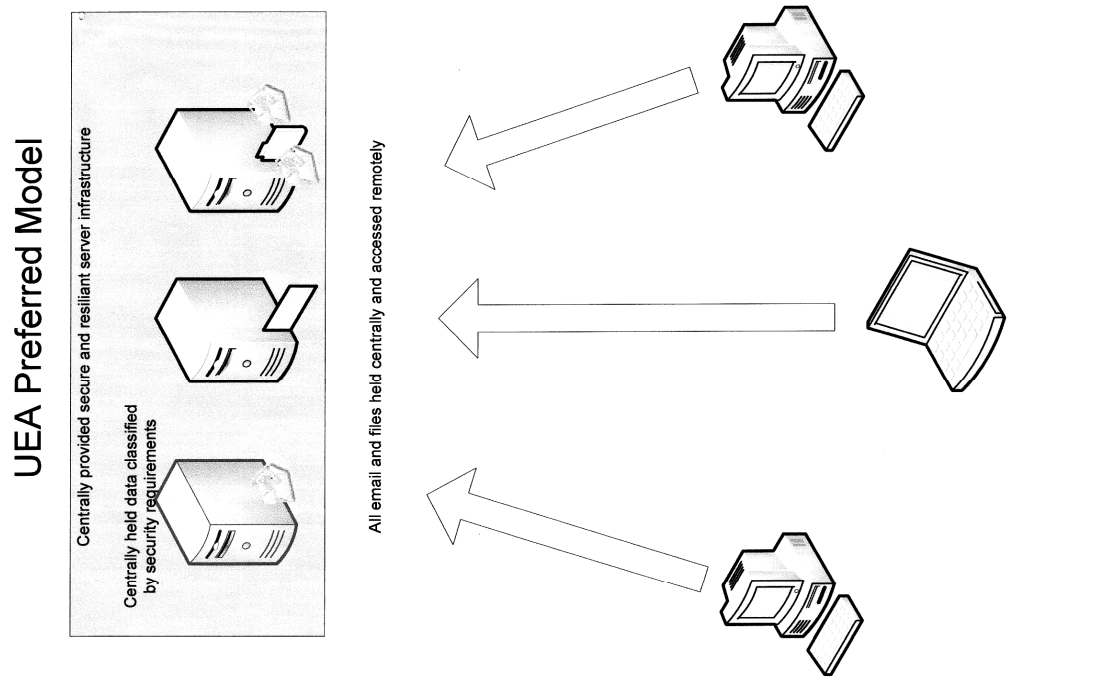
6. Iain Reeman (ICT Systems Director) indicated that "lessons had been learnt" and ISD expected (subject to the results of a security audit report) to bring forward proposals within the University for:

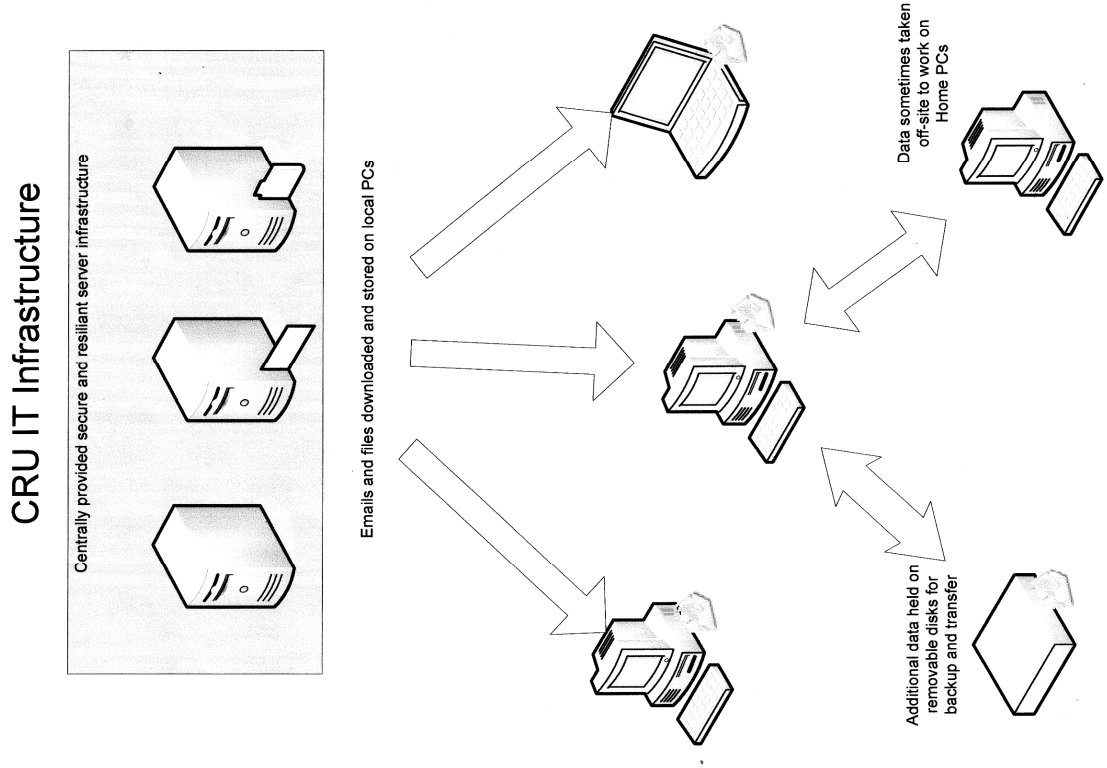
   - Greater compliance with centrally defined IS policies and architecture;
   - An audit of research data held in digital storage across the University; and
   - Clear data retention (and destruction) policies.

Jim Norton

2nd March 2010

[4] A copy of the "Code of Practice for responding to requests for information under the Freedom of Information Act 2000 – Final Draft 22/11/04 was also received by the Review on 8th February. The IS strategy is available at http://www.uea.ac.uk/is/strategies/infostrategy


UEA Preferred Model
Centrally provided secure and resiliant server infrastructure
Centrally held data classified by security requirements
All email and files held centrally and accessed remotely


CRU IT Infrastructure
Centrally provided secure and resiliant server infrastructure
Emails and files downloaded and stored on local PCs
Data sometimes taken off-site to work on Home PCs
Additional data held on removable disks for backup and transfer

Page 1, footnote 1

“High Level Information Security Policy”; and “General Information Security Policy”.
http://www.uea.ac.uk/is/itregs/ictpolicies

Page 3, footnote 4. Code of Practice

http://www.uea.ac.uk/is/strategies/infregs/FOIA+Code+of+Practice+for+Responding+to+Requests