Forensic Computer Examination and Network Investigation
UEA Incident

Introduction

QinetiQ will undertake a forensic investigation into the relevant elements of the UEA ICT infrastructure in order to establish the full circumstances leading to the publication of data from the Climate Research Unit on various Internet Websites. The questions to which we seek answers in relation to the investigation are set out below. Some are obvious but are included for completeness. It will probably be appropriate for further discussion on some points to clarify what can be achieved and the timescales/level of resource required.

It is understood that QinetiQ will undertake a scoping exercise to establish what might be achieved and to estimate the time and costs associated with this and that this has been agreed with NDET. Anything that cannot be achieved within this agreement should be referred to the SIO prior to work being undertaken.

FOI2009.zip

This is the file purporting to contain the data taken from the UEA and published on the Internet. It is currently available at www.megadownload.com. It is not known if this is the same file that was uploaded to the Real Climate website on 17th November 2009, which resulted in the UEA being notified of the breach to their security, as this is reported to have been entitled FOIA.zip.

We would like to establish the following:

- Summary of what it contains.
- Is all of the material in FOI2009.zip also contained on CRUback3?
- Where is the above data held on CRUback3
- How and from where the data in FOI2009.zip was complied.
- Was FOI2009.zip created on UEA systems or elsewhere?
- Has the data in FOI2009.zip been altered since being taken?

Network Investigation

Firewall Logs, CRU Web Server, CRUback3 & other seized/imaged desktops, laptops & servers

- How the data was accessed and or taken?
- What was accessed and or taken?
- When it was accessed and or taken (single or multiple occasions)?
- Where did the access come from i.e. internal or external?
- Who accessed and or took the data?

J. Gregory
D/Supt