University of Glasgow

Responding to the Security Gap Analysis

James Currall

April 2006

Introduction

The University engaged Boldon James to conduct a gap analysis of its existing implementation of information security management using BS 7799, the standard for information security management, in April 2005. This exercise was conducted as a 'review' rather than an 'audit'. It had the aim of facilitating improvements throughout the University, by helping it manage effectively threats and risks to information systems, on which the University is highly dependent.

The report was delivered to the University in its current form in mid-September 2005. In the report Boldon James recognises that the University has already implemented many controls in line with its information security requirements. It then goes on to highlight the information security gaps that need to be addressed to implement information security management effectively.

The report identifies a range of potential gaps in the University's information security management procedures and controls and made 94 recommendations under 37 numbered headings. The following were highlighted as containing the 'most important gaps to address':-

- Risk Management
- Information Security Policy
- Information Security Infrastructure
- User Training
- Reviews of Security Policy

The Approach

A careful study of the recommendations indicates that they fall into a number of broad categories as follows:-

1) Those recommendations, the subject matter of which is already addressed in existing policies, procedures and guidelines, and the recommendations are that such policies and guidelines should be presented in slightly different ways and that such policies, procedures and guidelines should be reviewed at intervals.

   These recommendations (numbering 12 items) will be taken forward by reviewing and recasting according to the recommendations.

2) Those recommendations that the Information Policy and Strategy Committee (IPSC), its IT Security Working Group and IT Services will schedule into their work plans to ensure that they are completed progressively between now and the end of December 2006.

   These recommendations (numbering 20 items) will be addressed over the next 6 months, with a completion date of the end of December 2006.

3) Those recommendations that concern conditions of employment, rules and regulations for the use of communications and IT facilities and computer misuse (by either staff or students).

   These recommendations (numbering 13 items) are being tackled in a major review of the use of communications and IT facilities being undertaken by IT Services and Human Resources, with input from Central Services, the Senate Office and the Data Protection and Freedom of Information Office. This work will put in place new guidelines, rules and regulations and acceptable use policies which will be presented to the University Court and Senate in Autumn 2006.

4) Those recommendations, mostly concerned with reporting lines and responsibilities that the University understands but which it feels are not founded on a solid grasp of how the University is governed and managed.

   In relation to these matters (numbering 8 items), the University is happy with the present arrangements but takes note of the reasons for the recommendations and will bear them in mind as changes are made in the future.

5) Those recommendations that will involve change over an extended period (mostly involving changes in culture).

   These recommendations (numbering 23 items) will be addressed in initiatives over the next few years, however proposals in this area will be completed by the end of September 2006.

6) Those recommendations that are speculative, not really relevant, not practical in a higher education environment or not a cost-effective form of risk reduction.

   The spirit of these recommendations (numbering 18 items) will be taken into account in future IT security planning.

Overall

It is clear from the report that IT Services have done a great deal of what needs to be done to put in place a robust Information Security Infrastructure. To build on that the following are required:

- a greater management recognition of the importance of information security and active promotion (in the messages coming from senior management to staff and students and the resourcing available),
- other parts of the University following Information Services example (where they don't already),
- a higher profile for training/awareness in the area of Information Security,
- some formalisation of existing good practices and extension of those.

It is worth noting that the operators of the HE/FE network have on occasion cited Glasgow as an example of good practice in relation to some aspects of Information Security.

An exercise such as that conducted by Boldon James is useful, in that it draws attention to areas that have been given a lower priority in the past than they might require in future and allows the University to build on what it has already done both by spreading good practice and by developing new policies and procedures to meet new challenges.

The IPSC Security Working Group is to be combined with the Information Continuity Group and in its strengthened incarnation, this group will study the Boldon James report carefully, looking at all 37 numbered sections to identify any courses of action that will be of benefit having due regard to the risks that are to be mitigated, the benefits to the University and the resource implications.

The Most Important Gaps

The text below in italics is drawn directly from the executive summary of the Boldon James Report. It provides details of the most important risks as identified in the "Security Gap Analysis". The ordinary text that follows each italic point is the action that is being undertaken to address it.

Risk management

Gaps include, but are not limited to, the following:

- *The risk methodology currently employed does not consider all impact types for breaches and losses of confidentiality, integrity and availability. Other factors that should be considered include damage or loss to image and reputation, breaches of personal privacy and legal obligations;*

  The methodology employed was designed to be extensible and it will be reviewed by September 2006 to ensure that it covers a wider range of impacts as suggested by Boldon James.

- *Risk management findings and recommendations are unlikely to be consistently presented to SMG (Senior Management Group) in a manner that enhances common understanding and ease of SMG decision making. Consideration should be given to regularly providing SMG with summary details of risk assessments, investment cost / benefit analyses, security incidents and findings of security audits.*

  Whilst recognising the need for security matters to be taken seriously at the most senior levels of management, it would seem to be a better use of SMG's time, that risk management findings and recommendations should be referred to the Secretary of Court (SoC) for management action via IT Services and other departments and that the SoC should ensure that the SMG is always made aware of the most important security risks when making decisions. The SoC clearly also has an important role in ensuring that security matters receive appropriate treatment as part of audit processes.

Information security policy

Gaps include, but are not limited to the following:

- *Policy should be owned by SMG to establish the correct level of direction and support for policy across The University. SMG should consider issuing a signed Information Security Policy Statement to emphasise its direction and support;*

  Hitherto, security policy has been developed through Information Policy and Strategy Committee (IPSC). IPSC submitted the overall policies and policy framework for Court approval in 2004. The Court indicated that it was happy to delegate consideration of detailed security policy to IPSC, so long as it was within the agreed framework. This arrangement seems to work well in practice, as IPSC has the competence to deal with the level of detail required.

- *Policy documentation should be better structured to ease understanding of responsibilities. High level documentation is required to list each supporting policy, with summary descriptions and responsibilities;*

  A review of the policy documentation will be undertaken, with the aim of ensuring that this recommendation is fully met by September 2006.

- *Policy documentation should be regularly reviewed e.g. annually. Reviews should take into account policy effectiveness and efficiency, considering recorded security incidents, and the findings and recommendations of risk assessments and information security audits.*

The Information Security Working Group of IPSC will undertake regular review of all information security related policies every summer, to take account of how they are working in practice and to ensure that new threats are adequately covered. The group will then make appropriate proposals for revision to IPSC, making sure that the resource implications are properly identified.

Information security infrastructure

Gaps include, but are not limited to the following:

- *A resource is not currently appointed that directly reports into SMG and has responsibility for all information security matters, including the establishment, implementation, maintenance and improvement of information security management. Consider the need for an Information Security Officer role with specialist knowledge and skills, who is given recognised authority throughout The University;*

  The current IPSC Information Security Working Group convenor has appropriate specialist knowledge and skills, which taken together with the considerable skills and experience in that group from across the University represents the resource required. In this role, the convenor reports to the Secretary of Court, whose pivotal role was outlined in the section on Risk Management above. It should also be noted that the convenor has no direct responsibility for specific IT or Information Systems and thus operates at 'arms length' from those directly responsible for systems.

- *Further consideration should be given to the management of on-going implementation, maintenance and improvement of information security policy. Revised Terms of Reference should be created in line with responsibilities. Those with responsibilities should be given recognised authority throughout The University;*

  The primary responsibility in this area rests with IT Services and specifically with the convenor of the IPSC Information Security Working Group and with the Computer Emergency Response Team (CERT) that monitors and investigates security related matters and advises widely on information security issues. As part of an exercise to review the rules and regulations for IT use and the roles and responsibilities of all IT staff, guidelines will be produced by December 2006 to clarify responsibilities and the authority for action.

- *It is recommended that both SMG and IPSC (Information Policy and Strategy Committee) meet at more regular intervals to progress information security management initiatives, ideally on a quarterly basis.*

  The relationship between SMG and IPSC is covered in the section on Risk Management above in relation to the role of the Secretary of Court who is also the convenor of IPSC.

User training

- *There is a lack of information security policy implementation and awareness throughout The University. Direction and support should come from SMG, including identification and enforcement of responsibilities.*

  The dividing line between on the one hand protecting users of IT systems from their inevitable lack of understanding or expertise via automated processes and on the other hand conducting time-consuming training is a narrow one. Too much automation produces a culture where people are unaware of the risks, whilst too little, even with a great deal of training, results in security breaches. The Higher Education community as a whole is constantly looking for new ways to raise awareness of the risks, whilst not taking people away from their work or making their work more difficult to do. The IPSC Information Security Working Group has considered how awareness, through training and other means, can be raised and will continue to do so and

make appropriate recommendations for action. The group will make recommendations in response to the Boldon James report by December 2006.

Reviews of security policy

- *There is regular liaison between the Head of Internal Audit and the Computer Emergency Response Team (CERT) staff to discuss security matters, which results in regular reporting to the Secretary of Court and the University's Audit Committee on matters of concern. This process should be formalised and supported by a properly resourced program of compliance auditing.*

  This will continue, but directly through the Secretary of Court following the changes in the arrangements for Internal Audit.

- *To address these most important gaps and all gaps identified in Section 3 (the detailed recommendations) [in the report], SMG must direct and support information security management. SMG must ensure that policy implementers are given recognised authority throughout The University, whilst all users of The University's information systems are aware of and comply with policy.*

  Authority in these matters derives from the Secretary of Court who can provide appropriate authorisation for specific courses of action as appropriate.