·EDINBVRGH·
THE CITY OF EDINBURGH COUNCIL

Item no 23
Report no

Information Security Update

Finance & Resources Committee

25 August 2009

1 Purpose of report

1.1 This report updates the Finance & Resources Committee on the implementation of the Council's Information Security Strategy and presents proposals for the introduction of additional technologies to prevent data loss along with an accompanying online training programme for staff.

2 Background

2.1 A previous report was presented to the Audit Committee on 11 September 2008 which highlighted recent developments following Scottish Government and UK Government reviews of data handling and sharing of personal information. The report agreed to reinforce policy, establish a wide-ranging communication programme and noted the importance of establishing and maintaining an Information Asset Register.

2.2 In parallel, Audit Scotland reported in 2008 on a review of cultural aspects of information handling and security in the Council. This report highlighted that the Council has a strong data handling environment with:

- a sound framework of policies, guidance and documentation;
- appropriate technological and physical security measures;
- a risk-based approach to security founded on knowledge of information sources and transfers; and,
- effective leadership from Corporate Services with regular reporting to the Audit Committee.

2.3 A range of opportunities for improvement were identified by the external auditor and progress against these actions is highlighted in this report.

3 Enhancing Information Governance Arrangements

3.1 The establishment over the last year of a Corporate Information Asset Register has identified the need for better involvement and commitment from departments to information governance. Whilst a policy framework and guidelines can be developed and maintained by Corporate Services, implementation requires commitment at a departmental level.

3.2 An Information Management Group with representatives from each department has been established and initial meetings held. This interdepartmental group meeting on a monthly basis has a remit to develop, refine and progress information management issues across the Council. The Information Management Group is chaired by the Head of E-Government and includes the Council Records and Information Security Managers, Internal Audit and departmental representation.

4 Enhanced Security Management of Laptops and Removable Media

4.1 The introduction of enhanced security measures for laptops and removeable media was a key action identified by external audit. It is likely that encryption of data on hard discs will become a mandatory requirement in the future, particularly where information is shared with central government, Police or NHS. In particular key additional features the Council should seek to introduce include:

- the ability to encrypt data on computer hard discs, particularly laptops, making it difficult for any unauthorised person to obtain access to data;
- control of the use of external storage peripherals such as 'USB sticks' and ' external hard drives'; and,
- central reporting and auditing of file status, for example to identify all files copied to removable USB pen drives by an individual.

4.2 A proposal for deployment across the Council has been developed. The proposal is based around the use of software products from Checkpoint Software Technologies (UK) Ltd. The solution can be managed centrally and integrates with our existing ICT architecture and management tools.

4.3 The proposed implementation of Checkpoint will:

- implement full disc encryption on all 5,000 laptops across the Council substantially reducing the risk if these devices are lost or stolen;
- allow management of peripheral devices such as USB sticks or portable hard drives on all 7,000 Microsoft Windows computers on the corporate estate;

- include detailed testing and pilot project stages in particular to test the approach to managing peripheral devices. This will help to ensure that genuine business needs are not hampered by the new software and that the technical configuration of the system is closely aligned to Council policy; and,

- establish a security framework for peripheral devices with educational establishments, which cannot currently be covered by this solution due to the large number of Apple Mac computers on the Learning and Teaching computer estate.

4.4 The project will be managed through the Smart City Programme Management Office (PMO) and will follow the established PRINCE2 project management methodologies and PMO governance arrangements.

4.5 A comprehensive communications and consultation plan will be critical to its success and this will be incorporated into the planned approach. The project is expected to be completed within approximately six months. As part of this project it is intended to update Council information security policy to complement the introduction of this technology.

5 Training & Awareness Programme

5.1 Since the previous report in August 2008 a series of Information Security briefing sessions have been held for Council staff. Nearly 100 managers have attended these sessions. Posters have been created to raise awareness of Information Security. Content on The Orb has been updated to provide additional supporting information for staff.

5.2 Whilst this awareness activity is welcomed it is clear that much further work is required to ensure all staff are aware of their responsibilities in terms of information security. A significant proportion of incidents are caused by mis-handling of information by staff and training and awareness should support staff in this area.

5.3 A plan has been prepared for the introduction of online training for Council staff on Information Security. This training will be integrated into the Council's e-Learning suite and departments should consider making it a mandatory element of certain employee's induction. Separate modules will be provided on:

- Information security for users;

- Information security for IT professionals;

- Freedom of Information;

- Data Protection; and,

- Data Handling.

6 Financial Implications

6.1 A one-off cost in 2009/10 of £458k will enable the implementation of enhanced security management of laptops and removable media and the online training module. In addition the plan will require the use of £143k of BT labour costs, for which it is planned to use the pre-paid resources within the core ICT contract. It is proposed that the costs of this programme in 2009/10 are covered by use of the BT Efficiency Fund.

6.2 Additional ongoing service and support charges for the technology in future years are £133k per annum. It is proposed that these recurring annual costs from 2010/11 will be recharged to departments based on the number of computers deployed in that department.

6.3 An independent 'Value for Money' analysis has been carried out on this proposal from BT and it found that "the costs within the BT proposal do appear to be within acceptable limits and compare well to costs of other similar projects".

7 Environmental Impact

7.1 There is no environmental impact of this report and its recommendations.

8 Recommendations

8.1 It is recommended that the Finance & Resources Committee:

a) notes the progress in implementation of the Council's Information Security Strategy;

b) notes the strengthening of information governance through the creation of a cross-departmental Information Management Group;

c) endorses the plans outlined in Section 4 of the report for the introduction of additional controls for encryption and peripheral device control;

d) endorses the proposals outlined in Section 5 of the report for the introduction of enhanced training and awareness programmes for staff;

e) endorses the proposal for funding of this programme from the BT Efficiency Fund in 2009/10 and thereafter from 2010/11 with additional service and licensing costs recharged to departments;

f) refer this report and recommend to the Council that the project be taken forward and £458k of resources be released from the BT Efficiency Fund.

Jim Inch
Director of Corporate Services
13/8/09

Appendices	None
Contact/tel/Email	Donald Crombie, Council Information Security Manager. Tel: 529 7987 Andrew Unsworth, Head of E-Government. Tel: 469 3965
Wards affected	All
Single Outcome Agreement	Outcome 15: Our public services are high quality, continually improving, efficient and responsive to local people's needs.
Background Papers	