INFORMATION ONLY ITEM
AGENDA ITEM NO. 16

BRISTOL CITY COUNCIL

Audit Committee

28 January 2011

Report of: Strategic Director (Corporate Resources)

Title: Update on the take up of online Information Security training

Ward: N/A

Officer Presenting Report: Manager, Information Management

Contact Telephone Number: 0117 922 3119

RECOMMENDATION

That the Audit Committee notes the information in the report.

Summary

Information Security remains Red on the Corporate Risk Register.

The key action to mitigate the risk to ensure that all staff take a short mandatory training course. In November uptake of the training was weak, and the Committee asked for a progress report in January.

The significant issues in the report are:

Numbers of staff completing security training are still inadequate. Only 41% compliance has been achieved against a target of 90%.

More action has already been taken to increase this number.

Policy

1. The council's Information Security policy is available at http://intranet.bcc.lan/ccm/navigation/policy-and-procedures/information-management/information-security/.

Consultation

2. Internal

Plans to improve security are agreed by the Information Assurance Board and the Strategic Leadership Team.

3. External

Security plans and standards conform to external recommendations, in in particular those the central government authority on Information Assurance, CESG – http://www.cesg.gov.uk/).

Context

4. In November 2010 I reported to this Committee on progress and plans to improve information security. The committee was overall satisfied with measures taken, but asked for a progress report on uptake of mandatory staff security training.

5. Unfortunately uptake is still considerably below target despite several reminders to staff and managers. As at 18th January 41% of staff have completed the training.

6. The following actions have been taken to improve this situation.

- On 11th January SLT reiterated their support and committed to ensuring staff in their directorates complete the training.
- Targeted personal emails to all staff who have not yet completed were sent out 14th-19th January
- A personal message from the Director of Resources was published on the front page of the Source 18th January
- The subject is included in the January "Team Brief" for explicit discussion at all staff meetings across the council

7. If this fails to produce the required improvement I will take the following action:

- Notify each strategic director of the take-up within their directorate and ask them to take action to bring it up to 90%
- Write to the managers of all staff who have not taken the course asking them to ensure compliance.
- Any staff who fail to comply after appropriate reminders and without good reason will be subject to disciplinary action.

Proposal

8. Audit Committee are asked to note the information in this report.

Other Options Considered

9. None relevant

Risk Assessment

10. The latest version of the council's Information Security risk from the corporate risk log is attached as Appendix A.

Equalities Impact Assessment

11. Not relevant

Legal and Resource Implications

Legal

None sought

Financial

The work described in the report is being undertaken within existing budgets.

Land

Not Applicable

Personnel

Potential for disciplinary proceeding against individual members of staff.

Appendices:

Appendix A - Updated Information Security Risk

LOCAL GOVERNMENT (ACCESS TO INFORMATION) ACT 1985 Background Papers:

None

Appendix A – Summary of Information Security Risk

(from the Corporate Risk Register)

Risk 027	Information Security - Failure to take adequate steps to properly safeguard sensitive and confidential personal data.	**Inherent Score (Red/Yellow/Green)**	**9: Red**
Risk Owner	Rob Scott	**Residual Score Red/Yellow/Green)**	**6: Red**

Mitigation	***Due date***	***Status***
Revise and rollout policy and standards	Mar 2011	Behind schedule
Carry out reviews to identify weaknesses in data transfer / mobile devices	Mar 2011	On schedule
Security training for all staff	Nov 2010	Behind schedule
Recruit Security Team	Jul 2010	Behind schedule
Information Security policy and standards to be completed and rolled out		Complete
Information systems classified according to new scheme.	Mar 2011	On schedule
Incident reporting and recording system to be developed.		Complete
Achieve PCI DSS compliance.	Oct 2010	Complete
Appoint Information Security Manager		Complete
Agree a data classification scheme		Complete
Update guidance on data transfer, encryption and use of mobile devices, data organisation		Complete