SURREY COUNTY COUNCIL
AUDIT REPORT

REVIEW
OF
EMAIL SECURITY

2010/11

Prepared for: Paul Brocklehurst, Head of IMT
Paul Jennings, Support and Delivery Manager
Grisilda Ponniah, Corporate Information Governance Manager

Prepared by: Simon White, Lead Auditor

Sue Lewry-Jones
Chief Internal Auditor
Surrey County Council
County Hall
Kingston upon Thames
Surrey
KT1 2EA

November 2010

Additional circulation list:

External Audit	Audit Commission
Service Finance Manager	Susan Smyth
Head of Finance	Phil Walker
Strategic Director	Julie Fisher
Risk and Governance Manager	Cath Edwards
Audit and Governance Committee	All
Cabinet Member for Change and Efficiency	Tim Hall
Chairman of Change and Efficiency Select Committee	Helyn Clack

Glossary:

ACL Access Control List. A list of permissions granted to a user

Data Governance Board A Corporate Group that ensures the council's data is collected, owned, secured, of good quality, used to maximum business benefit and effectively managed to comply with legal and best practice requirements

elearning Electronically supported learning and teaching

GCSx Government secure intranet enabling safe and secure transfer of information between local authorities and other GCSx approved bodies

Governance Panel Group of officers who ensure that the Council has a robust method of scrutiny and appraisal of Governance

IMT Information Management and Technology

Lotus Notes Business email solution deployed by Surrey County Council

S::Net Surrey County Council intranet

USER.ID A unique electronic file that identifies a legitimate Notes user and contains key user security information

Audit opinions:

Effective	Controls evaluated are adequate, appropriate, and effective to provide reasonable assurance that risks are being managed and objectives should be met.
Some Improvement Needed	A few specific control weaknesses were noted; generally however, controls evaluated are adequate, appropriate, and effective to provide reasonable assurance that risks are being managed and objectives should be met.
Major Improvement Needed	Numerous specific control weaknesses were noted. Controls evaluated are unlikely to provide reasonable assurance that risks are being managed and objectives should be met.
Unsatisfactory	Controls evaluated are not adequate, appropriate, or effective to provide reasonable assurance that risks are being managed and objectives should be met.

1. INTRODUCTION

1.1 Email is an essential business tool and has become integral to service delivery. Surrey County Council uses Lotus Notes to provide email services across the authority and delivers around 5 million internal emails each month and sends/receives close to 7 million emails. Around 6 million emails are blocked as SPAM over the same period.

1.2 Security of email is essential to ensure that confidential information is not compromised and that the provision of email systems is robust.

1.3 Specifically, the Chief Internal Auditor has been asked to review the effectiveness of controls to ensure the security of confidential information contained in emails and closely monitor management plans to improve this, reporting back to Cabinet in December 2010.

1.4 This Internal Audit review of the security of emails was undertaken following agreement of the Terms of Reference included at Annex A. This report sets out the findings and recommendations of the review. The completed Management Action Plan accompanies this report as Annex B.

2. WORK UNDERTAKEN

2.1 Internal Audit reviewed the policy and procedures including the IMT Security Policy and conformance criteria for email usage, interviewed key staff and performed audit testing of Lotus Notes Security where necessary.

2.2 The audit reviewed recent email data breaches and identified specific weaknesses and identified lessons learnt and controls that have been implemented following the incidents.

3. MANAGEMENT SUMMARY

3.1 In 2008 an audit review of information security found that "controls around information assets are inadequate to protect and secure all information owned and maintained by the Authority. A concerted effort is required, with the support of senior management, if a programme of information security is to be implemented to safeguard information assets and attain information security best practice." In response to the audit report a Data Governance Board was formed to oversee improvements in information security.

3.2 The Annual Governance Statement 2009/10 made specific mention to data security and control issues that arose in the year. In 2010, following two further information security incidents, Internal Audit were commissioned to review email security.

3.3 Review of the recent data breaches involving email found that user error was the cause of the information loss. Technical solutions have been identified by IMT and the Corporate Information Governance Manager, (see 4.1 below) that would reduce the risk of information security incidents occurring again, but will never eliminate the possibility.

3.4 Greater education and awareness in users is more likely to have a lasting impression on the chance of further incidents than technology enhancements. Previous initiatives within the Council have not been driven to their logical conclusion, employee completion rates for the information security elearning were found to be less than 50% in both Adults and Children Directorates – the source of the recent information breaches.

3.5 Further to, the review has found that the Data Governance Board, formed to drive information security within the authority, has not met since February 2010 and that whilst progress has been made in strengthening control over information security, greater rigour

needs to be applied to ensure that information security continues to be improved. A number of technical solutions have been introduced and IT controls will be improved with the desktop refresh, but a continued programme of education and cultural change is required to raise user awareness and ensure users apply measures consistently to all information.

3.6 The IT Security Policy provides the standards and instructions for users when using IT systems provided by the Council. Failure to comply with the IT Security Policy may lead to disciplinary action. A Protective Marking Policy has been implemented to ensure users consider the implications of sharing information but requires greater awareness to ensure users take the steps necessary to comply with the policy. Guidance needs to be issued that translates both the IT Security Policy and Protective Marking Policy into practical steps and best practice lessons that users can follow to avoid data loss and strengthen information security. Where appropriate this should be supported with technical solutions to assist compliance with the relevant policy.

3.7 It is the opinion of Internal Audit that **some improvement is needed** to ensure that users are aware of their responsibility to comply with information security guidance and the protective marking policy and to ensure that all technical solutions are explored to reduce the risk of an information security incident occurring.

4. FINDINGS AND RECOMMENDATIONS

4.1 Recent Data Incidents

Finding

The Adults Social Care breach in Aug 2009 was a spreadsheet sent to the correct addressee at Woking Borough Council (WBC). The spreadsheet contained more information than was required and was consequently classified as a breach. There were no implications around email security.

The Adults Social Care breach in May 2010 arose when an Officer at a Day Service Centre was under pressure to submit an information request in the absence of her manager. The user was not confident with IT and mistakenly entered text in the address field on an email. The error was not noticed before the email was sent. The text submission selected a comparative group address entry from the address book and as a result the email was distributed to an email group containing a large number of external email addresses. The subsequent review into the incident identified a number of technical recommendations that could help prevent a future repeat occurrence:

- Technical solution configured that would warn users before a Protected or Restricted document is delivered to an external address (complete).
- A naming convention established for global distribution lists that would prevent text being mistyped (outstanding).
- Clear guidance issued on the administration of group email addresses (outstanding).
- Lotus Notes users reminded of principles of data protection (outstanding).

The Children's Service breach in June 2010 occurred when a user mistyped a group email address. The user had set up their own group in their local address book - but mistyped and selected a group email address from the SCC address book that contained a number of external addresses. Following notification of the incident, the email was deleted from

internal notes databases where it had been received in error, and a correction sent out to external addresses.

Review of the incident was overseen by the Corporate Information Governance Manager, who notified the Information Commissioners Office, as was appropriate. Reviews were conducted by the relevant services with key findings recorded on the incident log by the Corporate Information Governance Manager.

Recommendation

The Corporate Information Governance Manager should work with IMT to ensure that outstanding actions identified following review of data breaches are completed.

4.2 Data Security Incident Procedures

Finding

The procedures for reporting a data breach are contained in the IMT Security Policy conformance criteria for Security Incident Management that informs employees to contact the IMT Service Desk who will in turn notify the IMT Technical Services Team. Users would have to be familiar with the IMT Security Policy to know where to look for guidance as the results of an s::net search do not readily identify the actions required in the event of a data breach. Without clear and accessible guidance, compliance with information security procedures is unlikely to improve.

Risk

Failure to publicise and make users aware of incident reporting procedures may lead to non-compliance.

Recommendation

Step-by-step guidance on the appropriate response to a data security breach should be provided as a quick link on the s::net homepage. This should be supplemented by the advice of the Security team following formal notification of a security incident.

4.3 Data Incident Review

Finding

The IT Security Policy states that the Security Team will determine what action should be performed in the event of an information security incident. However, there is no clear guidance published on the review of an incident following its treatment and closure. At present, the Data Protection Officer is notified of any review following an incident and maintains a log of incidents and the recommendations. This is not shared beyond the Service senior management so key learning points from security breaches are not shared across the council.

Recommendation

Findings from information security incidents should be reported to the Governance Panel, in the absence of a Data Governance Board, and recommendations tracked for completion by the Panel. Where changes of working practice are required these should be communicated to all users through s::net.

4.4 Data Incident Log

Finding

Data breach incidents are recorded on a log and maintained centrally by the Corporate Information Governance Officer. Further information is required on each individual incident to allow greater scrutiny of the log. Under existing arrangements the log of incidents is not reviewed by the Data Governance Board - the Board has not met since February 2010. Further to, details on the log are not completed in their entirety consequently the trend and learning from information security incidents are not discussed or shared at a senior level within the organisation.

Recommendation

The log of security incidents should be completed fully for each individual incident and subject to scrutiny at a senior level to ensure senior managers are aware of incidents within their area and across the authority, and that lessons are learnt to minimise the likelihood of future occurrences.

4.5 User Database Management

Finding

At present there is no guidance on the retention of old and archived emails other than the best practice instructions for management of a users inbox - the Notes Tips eLearning product recommends that users mailbox size does not exceed 800MB and 15,000 emails.

There is no guidance on the retention of old emails. Lotus Notes database management guidance should be created to support users on data retention and ensure users comply with the Records Management Policy.

Risk

Failure to offer clear guidance on the retention and storage of email may further hinder information security.

Recommendation

Consideration should be given to incorporating guidance into a best practice guide for users to help them manage their email accounts and ensure that system performance is optimised. Users should be encouraged to delete or archive obsolete emails and maintain a system of filing that ensures the inbox is kept to a manageable size.

4.6 IT Security Policy

Finding

The conformance criteria for email usage forms part of the IT Security Policy and outlines the guidance users should abide by when using the corporate email facilities. The conformance criteria provide clear guidance on acceptable use and unacceptable content. However, there are areas where further development would be beneficial.

There is currently no guidance on when content should be encrypted and consequently the conformance criteria states that sensitive information should not be sent. This does not reflect current practice whereby sensitive information is exchanged by email throughout, and external to, the authority. Guidance on the transfer of sensitive information should be developed and communicated to all staff to consolidate the existing protective marking guidance and coordinated with the Protective Marking Policy which states that documents marked ‘Restrict’ should only be shared through Secure Email.

Modifications have been made in Lotus Notes to ensure that emails marked restricted will be barred from being sent to external addresses unless from a GCSx user account. However, this would not prevent restricted information from being circulated if the user has not followed the protective marking policy.

The conformance criteria does not make explicit that non compliance will lead to disciplinary action only that compliance will 'reduce the risk of action being taken against the council and/or individuals'.

There is no guidance in the document that determines the correct action for archiving, storage and periodic destruction of emails. Consideration should be given to incorporating directions for users to manage their email accounts so system performance is optimised - see 4.5 above.

Changes to the policy should be clearly communicated and all users reminded of their responsibility when using County systems. Employees should acknowledge their understanding of policy.

Risk

Insufficient policy guidance may result in corporate liability or failure to safeguard information security.

Recommendation

The conformance criteria for email usage should be revised to ensure that a policy on the safe transfer of sensitive information is included making explicit the appropriate use of encryption if required.

Effect of policy compliance should be revised to include the threat of disciplinary action in the event of non-compliance.

Guidance should be included to ensure users are educated on email database management to ensure that system performance is optimised and that the risk of accidental release of information is reduced.

The conformance criteria for email usage should be incorporated into the ‘Lotus Notes – Basic Skills’ training and communicated to users regularly including printed materials and posters with timely reminders when revisions are made to the policy.

Users should be required to acknowledge their understanding of the IT Security Policy through completion of the information security elearning annually and this noted on their personnel file on SAP.

4.7 Information Security elearning

Finding

An Information Security elearning module was developed by IMT to support the drive for better working practices across the authority. There has been significant effort made to raise awareness of Information Security using the elearning within the organisation and this has been successful in large parts. However, the completion rate in Children and Adults directorates is very poor, 29% and 46% respectively - areas from which the recent data breaches emanated.

Risk

Failure to educate staff in Information Security would expose the authority to the risk of data loss and could lead to censure by the Information Commissioner.

Recommendation

Up to date completion figures should be produced to ensure that Services are aware of their completion rate and emphasis placed on rolling out the elearning to all employees.

4.8 Administrator Activity Logs

Finding

Lotus Notes records an activity log in a local folder and on the server. However, this log is only maintained for a maximum of two weeks. Actions of administrators are recorded for a maximum of two weeks in line with all audit trails.

Previous audit work identified a weakness in the monitoring of system activity - particularly around system administrator privileges. Activity logging does not meet Government Connect Code of Compliance requirements that stipulate:

- Audit logs recording user activity's, exceptions and information security events are available to be produced to assist in investigations and access control monitoring.
- All logs are maintained for a minimum of six months.

Risk

Failure to maintain an audit log beyond two weeks allows unauthorised activity to take place unchecked if the action is not noticed immediately. The failure to record the allocation and removal of administrator activity heightens the potential to perform high-risk activity unchecked.

Recommendation

Activity logs should be maintained for all system administrator access that meets the Government Connect Code of Compliance requirements as a minimum. Proactive tracking should be enabled to trigger an email warning when administrators perform high-risk functions and tasks.

4.9 Access Control List

Finding

Lotus Notes uses an Access Control List (ACL) to determine the access rights a user has in a Lotus Notes database. Authority to perform administrator functions is only granted if the user is listed in the relevant ACL. A log tab records the privileged users removed from the ACL. The log history is not time limited, the only restriction is server space, and can only be viewed by system administrators.

4.10 USER.ID files

Finding

A Notes USER.ID file is a unique file that identifies a legitimate Domino server or Notes user. A USER.ID file is a passport to enter Notes. Notes USER.ID files are created by a Domino administrator and contain key security information including access rights and privileges. The Notes USER.ID file would typically appear on a user's local drive. Control over the administration of USER.ID files has not improved since Internal Audit reported on this in January 2010 as administrators are still retaining USER.ID files locally. It is accepted that the implementation of 'Install Pump', a proprietary software tool for

managing Notes administration, is scheduled for the end of 2010 and will strengthen the control over USER.ID files.

Risk

Failure to safeguard the administration and retention of USER.ID files could lead to unauthorised access of user notes databases within the organisation.

Recommendation

Efforts to strengthen the administration of USER.ID files should be prioritised accordingly. Management should ensure that Install Pump is implemented by the end of Autumn 2010.

4.11 Perimeter Controls

Finding

Perimeter security controls should prevent unauthorised access to the key processing hardware of the email system. The servers for Lotus Notes are located in the County Hall Data Centre and replicated at the Data Centre in AO3. Physical inspection by the auditor found that perimeter controls were working adequately although the environment in the Data Centre was found to be cluttered with disused packaging. It is acknowledged that the Data Centre has passed its useful life and due for replacement, however effort should be made to ensure the physical environment is clean and free from clutter.

Risk

Failure to remove environmental hazards may expose the data centre to unnecessary risk.

Recommendation

Ensure all waste packaging is removed from the data centre in a timely fashion and that the environment is kept clean and clutter free.

4.12 Environmental Controls

Finding

As part of this review, the auditor considered the environmental controls in place for the Data Centre. Through discussions with staff it became evident that the centre has passed its useful operational life. IMT acknowledge the environmental controls are insufficient to ensure the continued operation of the data centre and have commenced planning to identify a long-term replacement to the existing Data Centre.

Risk

Episodic or prolonged failure of the data centre would expose the authority to an unnecessary risk of email failure or data loss.

Recommendation

The authority should ensure that sufficient priority and resource is committed to identifying and implementing a replacement Data Centre. As such, a paper is due to go to cabinet in Autumn 2010 with recommendations for the replacement of the existing Data Centre. IMT should ensure this proceeds as timetabled.

4.13 Disaster Recovery (DR) Testing

Finding

A full disaster recovery test of Lotus Notes has not been run in recent years. Regular recovery of individual databases has been sufficient proof of concept that a full DR recovery is possible. A full DR recovery test would require considerable staff resource.

Recommendation

Consideration should be given to whether a full DR recovery is of merit.

5. ACKNOWLEDGEMENT

5.1 The assistance and co-operation of all the staff involved was greatly appreciated.

Email Security– 2010/11

TERMS OF REFERENCE

BACKGROUND

Email is an essential business tool and has become integral to service delivery. Surrey County Council uses Lotus Notes to provide email services across the authority and delivers around 5 million internal emails each month and sends/receives close to 7 million emails. Around 6 million emails are blocked as SPAM over the same period.

Security of email is essential to ensure that confidential information is not compromised and that the provision of email systems is robust.

Specifically, the Chief Internal Auditor has been asked to review the effectiveness of controls to ensure the security of confidential information contained in emails and closely monitor management plans to improve this, reporting back to Cabinet in November 2010.

PURPOSE OF THE AUDIT

The audit will seek to determine that:

- Email policies, standards and procedures exist.
- Email policies, standards and procedures are current, complete and accurate.
- Access to Lotus Notes information assets is properly authorised.
- Access to Lotus Notes resources is properly restricted.
- The Lotus Notes hardware platform has been defined and mapped with any inherent risks or exposures have been identified.
- Email service can be restored in the event of data loss or disaster.
- Management have appropriately responded to previous audit findings in this area.

WORK TO BE UNDERTAKEN

Internal Audit will review the policy and procedures including the IMT Security Policy and conformance criteria for email usage, interview key staff and perform audit testing of Lotus Notes Security where necessary.

The audit will review recent email data breaches and report on the specific weaknesses and identify lessons learnt and controls that have been implemented following the incidents.

OUTCOMES

The findings of this review will form a report to Cabinet. This report will provide an overall audit opinion on the effectiveness of systems in place and set out recommendations for Surrey County Council Management. Subject to the availability of resources, and the agreement of the auditee, the audit will also seek to obtain an overview of arrangements in place for:

- Data quality and security;

- Equality and diversity;
- Value for Money;
- Business continuity, and
- Risk management.

The outcome of any work undertaken will be used to inform our future audit planning processes and also contribute to an overall opinion on the adequacy of arrangements across the Council in these areas.

REPORTING ARRANGEMENTS

Auditor:	Simon White, Lead Auditor
Supervisor:	Sue Lewry-Jones, Chief Internal Auditor
Reporting to:	Cabinet
Audit Ref:	IR / 104