Leeds CITY COUNCIL

Originators: Andy Nutting
Tel: 07545 604251

Report of the Assistant Chief Executive (Policy, Planning and Improvement)

Corporate Governance and Audit Committee

Date: 29th September 2010

Subject: Information Security Report

Electoral Wards Affected:	**Specific Implications For:**
	Equality and Diversity ☐
	Community Cohesion ☐
☐ Ward Members consulted (referred to in report)	Narrowing the Gap ☐

Executive Summary

Breaches of information security and losses of data, both nationally and at a local level, have focused public authorities to become more accountable for security failures or for the contravention of procedures which lead to the loss or disclosure of sensitive information.

Leeds City Council has recognised the need to protect its information assets from both accidental and malicious loss or damage. Information security is taken very seriously by the Council and this is evidenced by the ongoing work to improve the security of its information.

This report focuses on the work the Council is undertaking, both from a technical and non-technical perspective, to reduce the impact and mitigate against any attempts to breach information security. It covers the actions being taken to protect the Council from risks and threats to information security and the systems that have been or are being introduced to monitor and record attempts to breach information systems.

1.0 Purpose Of This Report

1.1 Corporate Governance and Audit Committee receive an annual report outlining the steps being taken to improve the Council's information security. After presentation of this report in March 2010, Committee requested a further report detailing any security breaches that the Council has been subject to and the work done to reduce the impact and mitigate against such attempts. The content of this report provides Members of the Committee with this information.

2.0 Background Information

2.1 Leeds City Council has recognised the need to protect its information assets from both accidental and malicious loss or damage. Information security is taken very seriously by the Council and this is evidenced by the ongoing work to improve the security of our information as outlined in this report.

2.2 This report provides Committee Members with an update on the more strategic and cross-council activity ongoing to provide assurance on our approach to information security. In this regard it covers actions taken to protect the Council from risks and threats to information security and the systems that have been or are being introduced to monitor and record attempts to breach information systems.

3.0 Main Issues

3.1 Threats to Council information come in a variety of forms and can be either technical or non-technical in nature. The Council is working towards ensuring that it can protect and secure information by investing in the policies, processes and technology solutions that will help prevent malicious attacks, misuse of information and the theft or loss of information. A comprehensive programme of work is ongoing to develop and implement policies and processes aimed at providing improved security and governance for the Council's information and the establishment of appropriate resources to ensure these are embedded into the culture of the organisation.

3.2 During 2009/10 the Council continued its significant investment in network defence systems. This investment ensured that the Council was granted connection to the Government Secure Intranet (GSi) through the Government Connect Programme, which amongst other things, allowed the secure transfer of data between the Revenues and Benefits Team and the Department of Work and Pensions.

3.3 The systems in which the Council has made this investment fall broadly into four categories:

- Edge Systems – designed to prevent unauthorised access from outside the Council's ICT network, or the introduction of malicious code in any form into the network;

- Network monitoring – designed to highlight unusual or unauthorised activity on the Council's ICT network;

- End user device systems – designed to control and protect the end user devices such as desktop computers and laptops, and prevent unauthorised hardware, such as USB memory sticks from being plugged into the network that could potentially introduce malware such as viruses;

- Security Information and Event Management software. These monitor the above systems and create alerts when unusual events are recorded, and also issue reports on network performance and security in a timely manner.

3.4 The procurement of these systems took place during 2009/10 and the ongoing implementation will be completed by 31st December 2010. The introduction of these systems will enable the Council to log and compile accurate information in respect of attacks to Council IT systems and improve the efficacy of our defences. Furthermore, a corporate Incident Management Policy is currently being drafted to establish an agreed corporate process for recording all information security incidents, both technical and non-technical.

3.5 The systems described in paragraph 3.3 have not been in place to record and provide accurate information about attempted security breaches during 2009/10. However, Corporate ICT Services are confident that they have been effective in trapping and dealing with virus attacks either at the edge of the network or on client devices and are confident that there were no major virus outbreaks or attacks to the system during this period. This is evidenced in part by the none occurrence of disruption of our systems by viruses. Furthermore, the Council has received no complaints from, or had to issue a report to the Information Commissioner's Office in relation to the breach of Principle Seven of the Data Protection Act relating to the security of personal data.

3.6 In respect of accountability for information security, Corporate ICT Services are responsible for the procurement and deployment of the technical infrastructure for the security of the Council's information. The Business Transformation Team are responsible for the development and implementation of corporate policy and procedures to support both technical and non-technical security of the Council's information, and for embedding these across the Council.

3.7 The theft or loss of a device can be embarrassing for the Council, and can lead to the imposition of a financial penalty and/or lead to consequences for citizen's, partners or employees. During 2009/10 nine laptop devices were reported to Corporate ICT Services as having been stolen or lost. A review of each incident showed that no sensitive data was accessed as a result of the loss, the laptop either having an encrypted hard-drive, thus making the recovery of the data impossible, or the information contained on the device having a business impact score of 0, meaning the information contained on the device would not harm the Council.

3.8 After the USB memory stick incident within the Council in 2008, a procedure was quickly put into place to ensure that only Council procured encrypted USB memory sticks could be used by employees on Council devices. Furthermore, all laptops devices have had a host based Intruder Protection Software (HIPS) installed, which protects the laptop when operating on the network and when staff are working away from the office. Corporate ICT Services are now in the process of installing McAfee 'Device Control' Data Loss Prevention (DLP) software, which will only allow authorised devices and encrypted USB sticks to be accessed on Council IT equipment. This work will be completed by the end of 2010/11. In addition to this, McAfee 'Vulnerability Manager' is now being deployed to ensure that all devices connected to the Council's ICT network have the appropriate software patch levels applied. This is important as this solution will report on any devices which are below a fixed level. McAfee security systems are the preferred ICT security solution for the Council.

3.9 In line with the Council's commitment to comply with Government Connect requirements, Corporate ICT Services have installed or are in the process of installing additional new software systems during 2010/11 to protect, monitor and control the security of our information systems. These include:

- 'LogRhythm' Security Information and Event Management (SIEM) – Gathers and analyses information (event logs) from various areas within the network to identify possible security breaches, including intrusion (outside attacks) and misuse (internal attacks). This system is currently undergoing commissioning, but is already monitoring the Intruder Detections, prevention systems and email systems. It will be extended as new systems and devices come on stream;

- McAfee 'Web Gateway' system – Allows web to be used whilst proactively protecting against threats from spyware (used to obtain information from a user's computer system without the user's knowledge or consent) and targeted attacks on the network;

- 'Clearswift' Mailscanner – Used for web content filtering and monitoring, keeping network free of malware (malicious software or programme code designed to infiltrate a computer system) such as viruses and spyware; and,

- McAfee 'IntruShield' Intruder detection and Prevention System – this will monitor the network and identify and report any unusual activity aimed at attempting to compromise the confidentiality, integrity or availability of an information asset, so that it can be picked up early and block attacks before they reach the target.

3.10 Whilst substantive investment has been made in procuring and deploying technologies, these alone won't protect the Council from all information security threats. The misuse of information can be both intentional and accidental and is difficult to mitigate against. Policies and procedures need to be developed and implemented in order, not only to support the processes required to successfully deploy the technologies and systems, but to ensure the Council does not succumb to non-technical information risks and threats.

3.11 An Information Assurance strategy (Information Security and Information Sharing) is being developed, which will set out how the Council is to meet its information management and security responsibilities ensuring that all information is handled and stored with due regard to its value and risk. As part of this strategy a Threat Landscape Matrix (TLM) is to be designed that will seek to identify threats to information security, identify those that pose a risk to the Council and, determine and action the most effective mitigations against those risks. The TLM will, for the first time, provide a tool that will allow the Council to identify and prioritise security risks and to mitigate against these before they have the potential to become serious security incidents by allocating appropriate resources accordingly.

3.12 To support the Information Assurance strategy the following policies have either, been drafted and are in various stages of consultation, or are to be drafted during 2010/11:

- Removable Media & Mobile Computing- establishes the principles and working practices that are to be adopted by all users in order for information to be safely stored and transferred on removable media, including laptops. This policy is drafted and is currently going through consultation with Trades Unions;

- Clear Desk and Clear Screen - ensure staff have an awareness of the importance of keeping both paper and electronic documents and records safe when they are working at their desk or on their screen and that they have knowledge of how to protect them from unauthorised access. This policy is drafted and is currently going through consultation with Trades Unions;

- Protective Marking & Asset Control - To ensure that all information and information systems upon which the Council depends are adequately protected to the appropriate level and to provide a consistent and clear methodology for the marking of information assets. This policy is drafted and is currently going through consultation with Trades Unions;

- Information Sharing – protect all information assets owned and used by the Council from the risks posed by inappropriate disclosure. This policy is currently being drafted;

- Acceptable Use – protect all information assets owned and used by the Council from the risks posed by inappropriate use, including virus attacks, compromise to network security and services, disclosure of information as well as legal and regulatory issues. This policy is drafted and is currently going through consultation with officers;

- Information Risk Management – managing the risks associated with the handling and sharing of information assets across the Council and with third parties. This policy is to be drafted once the Information Assurance strategy is approved;

- Incident Management Reporting - to ensure that the Council reacts appropriately to any actual or suspected security incidents relating to information systems and information. This policy is currently being drafted.

3.13 The development of these policies forms part of the Information Governance Project. The aim of the Information Governance project is to ensure all Information Governance policies are developed and embedded across the Council through an effective communications, engagement and training plan. Corporate ICT Services are contributing to the development of these policies in order to ensure that they support the implementation of security systems and related technologies.

3.14 Discussions are ongoing with each Chief Officer for Resources and Strategy (CORS) about identifying a resource within each Directorate who will be a contact for providing advice and guidance about information assurance and who will also coordinate delivery of the information assurance strategy, and associated policies.

4.0 Implications For Council Policy And Governance

4.1 Information Security is one of six modules of the Information Governance Framework approved at Executive Board in November 2008. The Information Governance Framework will be supported by the development of policies, procedures, guidance and best practice across the six modules of the Framework.

4.2 All Information Governance policies and procedures will follow a consultation process to obtain support and approval and this includes the Council's Information Governance Management Board (IGMB), Resources and Performance Board and the Corporate Governance Board.

5.0 Legal And Resource Implications

5.1 Sufficient capacity with the appropriate knowledge and skills to deliver and implement the systems and technologies are required by Corporate ICT Services in order to ensure the Council is able to mitigate against security risks and threats to its information assets.

5.2 Capacity within Directorates to deliver, embed and monitor compliance to information assurance policy and practice is required, but resources for this can be identified from existing FTE's within the Directorates.

5.3 In order for the Council to comply with its obligations under the Data Protection Act it must deploy technologies to ensure the security of personal information. The developments that have already taken place and the actions that are currently being undertaken will ensure the Council identifies and mitigates against current and emerging threats and prevent security breaches occurring.

6.0 Conclusions

6.1 Improvement to Information Security are being addressed through changes to policy, skills, processes and technology. Whilst information security incidents within the Council have been kept to a minimum over the last twelve months, as this report demonstrates a number of initiatives are currently underway which will make a significant contribution to identifying threats and further minimise the risks associated with poor information security management.

6.2 The security of the Council's information assets continues to be a high visibility activity, and new threats and their mitigations are being monitored continuously to ensure that the threat horizon is managed at all times.

6.3 The Information Assurance strategy and associated policies and processes will provide an internal regulatory framework for ensuring the Council's information is processed and stored in a secure manner and will compliment the introduction of new technologies and systems for protecting and monitoring data.

7.0 Recommendations

7.1 Corporate Governance and Audit Committee is asked to consider the contents of this report and the assurances provided as to the Council's approach to information security.

Background Documents Used

Annual Information Security Report – 17th March 2010

Briefing Note – Security of Personal Data and the Requirements of the Data Protection Act – Gillhams Solicitors & Lawyers

Information Governance Project – Project Initiation Document