Stevenage
BOROUGH COUNCIL

Part I – Release
to Press

Meeting:	**Audit Committee**	**Agenda Item:**	**7**
Portfolio Area:	Resources		
Date:	**22 July 2010**		

ICT SECURITY

Author – Henry Lewis, ext 2496
Lead Officer – Henry Lewis, ext 2496
Contact Officer – Henry Lewis, ext 2496

1. PURPOSE

1.1 To set out the Council's current arrangements for dealing with ICT security in the light of the recent loss of service. To seek Members views on measures recommended to further improve security and introduce new ICT business continuity arrangements.

2. RECOMMENDATIONS

2.1 That the Committee note the recommended improvements to ICT security set out in paragraphs 4.4 to 4.7 below.

2.2 That the Committee note the recommended ICT Business Continuity solution referred to in paragraph 4.10.

2.3 That the Committee note that a detailed action plan will be prepared to implement the recommendations once these have been approved at a meeting of the Senior Management Board on 20th July 2010.

3. BACKGROUND

3.1 There has been a significant emphasis upon ICT Security over the last two years. The Government has mandated the introduction of their secure extranet (GCS(X)) and this has become the key mechanism for communicating information to Government in the Revenue Services SDU.

3.2 In order to access GCS(X) the Council has had to put in a place a range of improvements and have been audited on our arrangements. The Council is due to be audited again in December this year against a revised GCS(X) standard. Additional enhancements are planned in order to meet the new security requirements.

3.3 Notwithstanding the improvements referred to above, the Council suffered a loss of service for two days on 29th to 30th April 2010 because of a virus that infected the Council's systems. The virus was introduced by an ICT contractor who logged in to the Council network using his own infected laptop. The contractor has admitted liability for the incident and has agreed to pay back any direct costs arising from it.

3.4 As a result of the incident, the ICT Team have reviewed our ICT security arrangements and propose a number of improvements set out in section 4 below. Most of these improvements relate to the security surrounding access to our local area network, which we believe to be the main area of outstanding risk. Improvements made in response to GCS(X) have tended to focus upon securing our systems from intrusion or attack from the outside world. We are now focusing upon the risks posed by our staff, members and trusted contractors, all of whom have access to our systems within our firewall and who may deliberately, or more likely inadvertently, cause a security incident.

3.5 The ICT Team has also been reviewing options for delivering an ICT business continuity solution. We are now in a position where the majority of our main business applications and data are held on virtual servers and our new Storage Area Network. This solution allows us to split our systems and data between sites so that the Council is protected should one site or the other fail and become inaccessible.

3.6 Concurrent with the above, we have been reviewing potential physical locations for the second ICT site. Details of our recommended option are set out in section below.

4 REASONS FOR RECOMMENDED COURSE OF ACTION AND OTHER OPTIONS

4.1 This section of the report covers three areas; the actions taken to manage the security incident from both an ICT and the Council's wider business continuity perspectives, proposed security improvements and proposals for improved ICT business continuity arrangements.

MANAGEMENT OF THE SECURITY INCIDENT

4.2 From an ICT perspective the incident was well managed. The key considerations are set out below:

- Systems were taken down within twenty minutes of the first virus alert being received in line with best practice to minimise its potential impact
- The correct approach was taken to delete the virus, albeit advice from the Council's security advisors changed during the first day's loss of service
- ICT staff communicated well as a Team. Key technical staff understood their roles and were able to concentrate on key tasks. ICT management focused upon communication with the rest of the organisation. The organisation itself responded well, particularly those staff who acted as liaison officers between ICT staff and the service departments
- ICT staff's willingness to stay late throughout the incident (including over the weekend and on the bank holiday) was invaluable. ICT staff confirmed after the event that they understand that this is what is expected of them and they would do so again in the future should a similar event recur. ICT staff do not receive any kind of stand-by allowance to guarantee their support in these types of circumstance

4.3 From the Council's perspective, the arrangements in place to manage issues of this kind also worked well. A review of the business continuity arrangements that took place after the incident concluded that:

- An early decision was made correctly to invoke the Council's Business Continuity Plan
- Regular meetings of the Business Recovery Group took place. This provided ICT with a forum to update senior managers and to ensure that actions and priorities were agreed
- The planning that had already taken place combined with an excellent response from managers across the Council and in Stevenage Homes Ltd allowed the Council to keep disruption to a minimum during the incident

LESSONS LEARNED AND RECOMMENDED IMPROVEMENTS

4.4 Although the loss of service was well managed, the incident nonetheless occurred and improvements need to be made to prevent a recurrence. The virus infected the Council's network because an infected laptop was connected directly into the Council's network. Although the laptop in question was owned by a Council contractor, it could just as easily have been caused inadvertently by a member of staff using a laptop or any other kind of portable media device.

4.5 There will always be circumstances when a contractor needs to be able to access the Council's systems. Typically this will be when a software engineer needs to run specialist software to diagnose problems or implement new solutions for the Council. The Council already requires contractors to take steps to control viruses on equipment that might come in contact with the Council's network and to indemnify the Council. However, as the recent experience has shown us, this is not enough. The only way of ensuring that contractor's equipment is secure is to operate what is known as a sheep dip system. This involves scanning contractor equipment before it is logged on to our network.

4.6 The sheep dip solution is not practical as far as staff and members are concerned. For staff and members, we must ensure that:

- The use of portable ICT equipment is minimised where it presents the greatest threat
- Improvements are put in place to ensure that anti-virus software and windows security software is kept up to date on these devices.

4.7 It is not possible to ban outright the use of all portable media devices. These include laptops, memory sticks, smart phones that involve the transfer of data as well as voice communications and digital cameras. However, we need to minimise the threat of a virus being passed into our network from these devices as well as the reputational risk of one of our staff passing a virus to a network managed by another organisation. The other key security risk particularly associated with portable media devices is data loss. For these reasons a number of actions are proposed as follows:

- An immediate ban on the use of memory sticks and memory cards pending a more thorough review. It is likely that the use of memory sticks will be reintroduced, but only encrypted memory sticks issued by the Council.

- A significant piece of work will be undertaken to review the current use of laptops, to standardise lap top builds and to introduce mechanisms to ensure that laptops can be updated remotely with the most recent windows and anti-virus software

- Discussions need to take place with Members and officers on the use of smart phones. These devices have clear business benefits and the risk of a virus being passed on to our network from such devices is low. However, they are high risk devices from a data loss perspective, particularly if the device used is owned by an officer or a member personally and is not locked down adequately to protect it should it be stolen

- Once these proposals have been agreed, ICT security policies will need to be updated and staff and members will need to receive further ICT security training

4.8 A detailed, prioritised, action list will be discussed with the Council's Senior Management Board on 20th July 2010. Financial implications arising from these new security priorities will also be discussed at that meeting.

ICT BUSINESS CONTINUITY

4.9 The Council recognises that improved ICT business continuity arrangements need to be put into place to protect the Council in the event that the computer suite at Daneshill House becomes unavailable. The preferred solution is to split the servers between Daneshill House and a second location and to replicate data between the two sites using the Council's existing dark fibre network link.

4.10 The preferred option is to locate servers at Cavendish Road. This option will not involve additional revenue costs and capital costs in this solution are also kept to a minimum. The other options that were reviewed were the County Council's building at Farnham House and the Business Technology Centre. The financial implications of pursuing this option will be discussed with the Senior Management Board on 20 July 2010.

4.11 It should be noted that although this solution will protect the Council from a number of scenarios, including fire or flood at Daneshill House, it is unlikely that the solution will protect the Council from a further virus. The Council will rely upon the improvements set out above to mitigate this risk.

5. IMPLICATIONS

5.1 Financial Implications

The additional costs associated with these proposals will be considered at the Senior Management Board meeting on 20 July.

BACKGROUND DOCUMENTS

- None