Coventry City Council

Briefing note

To Audit and Procurement Committee

Date 15th February 2016

Subject Briefing note on current Cyber Security

1 Purpose of the Note

At the Audit and Procurement Committee meeting on 26 October 2015, it was requested that a briefing note be submitted to the next meeting of the Committee in relation to the Council's approach to cyber security and how risks are being managed.

This note outlines the current measures in place on the Council's ICT services to prevent, manage or minimise the impact of Cyber-attacks.

2. Context

In an increasingly digital world, cyber threats are an issue for governments, companies, public sector organisations and individuals alike. A series of high profile attacks highlights the importance of remaining vigilant to the ever present risks associated with malicious attacks on systems, information and data held by organisations. These can cause not only financial loss, but also reputational risks.

As the Council adopts a more digital approach to service design and delivery, with all the associated advantages, there comes an inherent new set of risks that we need to consider and work to mitigate, particularly so that we can continue to operate robust systems and deliver services that residents and staff feel they can trust.

3. Current provisions

There are a number of different methods that could be employed. The main methods are:-

- Virus or Malware attack
- Denial of Service attacks (DoS)

3.1 Virus or Malware attack

This type of attack is where a piece of malicious computer code or software, which is normally capable of duplicating itself, is introduced into an IT system specifically to have a detrimental effect on that system. The most common method of infection is from an email or an infected file.

This type of risk is mitigated on all Council equipment by the implementation of an Antivirus program (McAfee Antivirus) on the PC or laptop. This is an application which is constantly scanning the PC/laptop and checking files as they are accessed for the presence of viruses or malware. The scanning is based on a virus definition dictionary, which is updated (on at least a daily basis) with any new virus signatures.

As an additional layer of security, all emails received by the authority, are scanned by 2 separate systems (Mimecast and Microsoft Forefront) to ensure they do not contain viruses or malware.

3.2 DoS/DDoS

A Denial of Service (DoS) is when, either accidentally or maliciously, a service is overloaded with requests to the point at which normal operations are affected. It is classed as a Distributed Denial of Service (DDoS) when the traffic causing the disruption has multiple sources. A DDoS is more difficult to stop because it does not come from a single source so cannot be blocked using rules on our firewalls.

These have the potential to affect internet services, external systems we access, external services including the website and indirect services such as those provided to schools.

3.3 Mitigation Measures

The ultimate mitigations for any type of cyber incident against the Council, is vigilance on the part of users and staff. Staff should ensure that they do not share any security details especially passwords, with anyone, including other Council staff and ICT.

Staff should also be vigilant about opening emails and attachments from unknown source. The best rule of thumb is ‘if in doubt, do not open it delete it’. If the email or file is from a legitimate source, then you can always ask the user to resend it.

In addition, we look at measures that can be put in place to prevent or mitigate the risks of such attacks. At present the following measures are in place:-

1) All PCs, Laptops and Servers on the Councils IT network are protected by McAfee Security suite, which is controlled centrally by ICT and cannot be disabled.

2) All incoming email is scanned automatically by 2 separate systems to ensure that it does not contain viruses or malware. In addition, the McAfee Security suite scans the email and attachments at the point it is accessed on a PC or laptop.

3) Multiple layers of firewall are in place on all external connections to the Council's network, preventing unauthorised access to data and systems

4) All systems that are accessible from outside the Council, such as the Customer portal, are located in a special area of the network that is separated from the main Council network.

5) Regular penetration tests are carried out on all external access points to the Council's network to ensure unauthorised access cannot be achieved.

6) JANet who provide our internet services has dedicated security and network teams that have expertise in dealing with DoS attacks. As well as investigating incidents targeted at them they assist customers when they are targeted. They have run security seminars in promoting awareness and good practice.

4 Ongoing and Further Work

It is best practice for the Council to consider these risks at a strategic management level and at the Audit and Procurement Committee. Cyber security is a risk that is reflected within our Corporate Risk Register that is considered actively by Strategic Management Board.

As we move more systems and services to the internet, we will develop work streams to review and address our ongoing Cyber security and resilience as part of our Strategic ICT work programme. This will be underpinned by regular programmes of security testing both internally and by specialist 3rd parties.

We will continue to review our approach to Cyber Security by reviewing best practice guideline and utilising specialist toolkits from leading organisations such as Gartner, SOCITM, NCC and others.

The success of these programmes of work will be validated as part of the ongoing ICT Audit programme.

We plan to continue to reinforce the role staff can play in helping to mitigate risks through targeted digital skills training, communication on Beacon and our interactions with customers.

Mark Chester, Head of ICT Infrastructure and Operations

Lisa Commane – Assistant Director ICT Transformation and Customer Services