



ADDITIONAL ISSUES RAISED AT OVERVIEW AND SCRUTINY ON 12TH April 2016

Issue Raised	Action/Comments
<p>A Member/officer briefing note on security and what we do to protect the council and those most vulnerable.</p>	<p>Briefing note prepared and sent to all Councillors on behalf of the Deputy Leader. Attached</p>  <p>Birmingham City Council Security Briefing</p>
<p>LOB – get someone to spend a day in the life.</p>	<ul style="list-style-type: none"> • Contact made to undertake Day in Life and ICT Surgery for both LOB and Community Libraries. • Initiatives meeting held SB Visited Birchfield Library 19th July agreed: subject to Staff benefit scheme approval <ul style="list-style-type: none"> ○ The SBS award of £10k for the summer reading challenge/improving the literacy of children ○ The SBS award for purchasing new books for children <p>SB will attend Summer Reading Challenge sessions on Thursday 25 August</p>
<p>Cllr Ward undertook to investigate how Members wishing to access information regarding cases via their mobile phones etc., especially when out and about, might be improved</p>	<p>Members Portal to address these issues is included within the new ICT & Digital Strategy to be considered at the 18th October Cabinet meeting.</p> <p>The briefing attached shows the current services available</p>  <p>Exec Briefing - ICT Support for Agile Work</p>
<p>Update On recommendation RO8:</p> <p>That options for Service Birmingham to sell its services more widely are explored and reported back to Corporate Resources O & S Committee</p>	<p>Since the last Scrutiny meeting discussions have been held for Service Birmingham to deliver ICT to Staffordshire Schools. Also Service Birmingham is selling its services to other parts of Capita, particularly other local government Accounts. This shared service now extends to delivering some support to Southampton, West Sussex, Barnet and Sheffield</p>

Birmingham City Council

Members briefing

Cyber security incidents

Introduction

Attempts to attack Birmingham City Council's information resources happen many times every day. Hackers try to break into the council's network and systems to steal or damage its data or to disrupt its services. The following briefing note outlines the level and broad categories of those attacks and gives some statistics and descriptions of the technologies deployed by the council. But before the attacks are described it is worth reminding ourselves of what information / cyber security is about.

The council has adopted a cyber security strategy called 'defence in-depth'. This can be thought of as a series of checks, controls and precautions that are in place to protect every piece of information used by the council in the delivery of its services.

The key objectives of cyber security are to maintain **Confidentiality** (information can only be accessed by an authorised person); **Integrity** (making sure that the information is accurate and complete); and **Availability** (making sure that the information is accessible when and where required to deliver a service.) The attributes of **CIA** are embedded in our People, Processes and Technology. When added together these attributes form the basis of our 'defence in-depth' cyber security strategy.

As discussed above, cyber security attacks fall into a number of broad categories:

Attacks involving people (social engineering)

Social engineering attacks involve deceiving people in some way – an example would be of a phone call by a person pretending to be a support engineer and asking you for your passwords or credentials to fix a problem. These types of attack take place in BCC from time to time. There are many variations and pretexts that are tried to con people into revealing information.

Email

The council sends and receives approximately 30 million emails per year. Email attacks are a major threat to the council. There are many variations of email attacks that are fundamentally similar. They involve the sender spinning a story or presenting a bogus screen that entices the user to divulge their credentials, or to click on a link in an email which then carries out some unauthorised activity.

Over the last year the councils email filtering service blocked approximately 100 thousand emails which had malware attached to them. January 2016 was the busiest month, with 24,000 blocked.

Website attacks

A very dangerous category of attack is the Denial Of Service attack (Dos) or (Ddos) when carried out by many attackers at the same time. In essence, this attack relies on the hacker sending many web page requests to the councils web sites at the same time; so many requests are sent in a short time

that the website can't cope with the number and slows down so that legitimate users can't get access. These types of attack happen on average 1500 times per month. The council has a defence system in place that detects and defends us from these attacks.

Other types of website attack try to find weaknesses in the council's web site pages and network devices. All web facing systems are tested for vulnerabilities before they are deployed to the public. Service Birmingham spends a lot of time ensuring that the council's software and hardware is up to date in line with the manufacturers guidelines. Any vulnerabilities found are fixed as soon as they become known.

Network attacks

On average the councils network is accessed at a rate of approximately 1000 requests per second. 24/7, 365 days per year. During the working day peak, the connection rate is higher, reaching 5000 requests per second or higher. Each of these requests is filtered and analysed for malicious intent. Any untrusted connection requests are dropped

Cyber defence

As discussed above, the council has invested in cyber security defences over many years. The current generation are placed in a 'sentry' position, outside of the council network. In that way most attacks are stopped before they ever reach the councils network, but not all.

The council has deployed 'firewall' technology that rapidly scans all network traffic passing into and out of the council's network. Each security system provides a range of monitoring tools that help Service Birmingham advise the council on threat trends and new types of attacks.

The council works with a range of security partners and Service Birmingham to ensure that it is up to date with new and emerging security threats and challenges and defences.

Personal cyber security precautions

Every member of BCC plays a role in protecting the councils information assets. Here are three practical top tips to help keep BCC information safe. The same good practice applies to your home systems and services.

- Do not click on an email link if you don't recognise the sender or subject. Just delete it.
- Do not reveal your user ID or password to anyone over the telephone.
- Do not use weak passwords that can be easily guessed.

These simple points will help to protect the councils and your own personal information

If you would like further information on this subject please contact the ICF at Birmingham City Council or Nigel Jones at Service Birmingham (Nigel_i_Jones@servicebirmingham.co.uk)

Executive Briefing: ICT Support for Agile Working

BCC staff increasingly need to access corporate data and applications from a non-traditional office setting; for example from home using their own broadband connection, from public locations using free WiFi hotspots or via the mobile network using 3G/4G.

Some staff and third parties are also asking to use their own devices to access data and applications either whilst in a BCC building on the corporate network or from external locations. For example: a BCC user may wish to use their own personal tablet to access data and applications or a third party organisation may want access to specific data or applications using their own devices.

Consideration of security and performance are increased when connecting to corporate data and applications from outside of the corporate network because the devices and/or the connection used are outside the control and management of the ICT support teams.

Question 1 What capabilities currently exist to allow workers to access data and applications whilst not directly connected to the corporate network using corporate or non-corporate owned devices? - See “Current Connection Scenarios”

Question 2 What are the gaps in the current capability and how are they planned to be filled? See “Future Considerations”

Current Connection Scenarios

This table shows if there is a current IT solution in place for data and applications to be accessed for each combination of device and connection method.

		Corporate		Non-Corporate	
		Laptop	Tablet / Smartphone	Laptop	Tablet / Smartphone
Corporate WiFi	Connecting within a BCC building directly to the corporate network	✓	✗ ¹	✗	✗
Public WiFi	Connecting using a WiFi hotspot, e.g. in Café	✗ ²	✗ ²	✓	✓
Home Broadband	Connecting using own home connection either wired or wireless	✓	✓	✓	✓
Mobile Network	Connecting using the national telecoms network, e.g. O2	✓	✓	✓	✓

Notes

1. BCC tablets are WiFi enabled but Corporate Smartphones are not; Corporate Smartphones cannot be configured to securely connect to the Internet via the current network without creating policy compliance issues and security vulnerabilities. Future smartphone updates are expected to remove this limitation.
2. This gap in capability is due to public WiFi networks being insecure for the period between connecting, authenticating (typically via a portal) and then securing the connection to the corporate network through solutions like NetMotion. This security risk could be easily exploited to gain access/control of the device. We are currently evaluating solutions to manage this type of connection.

Future Considerations

Corporate Devices Connecting using Public WiFi

Users of Corporate devices are not currently able to utilise public WiFi hotspots due to security vulnerabilities. A capability known as SSL VPN (Secure Socket Layer - Virtual Private Network) is currently being explored to enable such connectivity.

Skype for Business

A proof of concept is in initial planning stages with the aim to explore the recently launched cloud-based Skype for Business service. This is expected to enable Corporate Laptop, tablet and Smartphone users to use Skype features, whilst avoiding the security vulnerabilities that exist with the standard Skype services.

Outlook Web Access (OWA)

The decision has been made to temporarily turn off the OWA capability from July 2015 as a result of additional security requirements mandated by the PSN. This is under review.

Smartphone Single-Sign

When using a BCC Smartphone there are 3 passwords to manage: phone screen lock, network and the Corporate APN (access to the corporate network via 3G/4G). Work is underway to investigate if the user experience can be improved.

FAQs

Q: Can I connect to the corporate network using my BCC laptop when I am working at home?

A: Yes, you will need a home broadband connection (either wired or wireless), a BCC Laptop with NetMotion software installed and a NetMotion license.

Q: Can I connect to the corporate network using the free WiFi in a Café?

A: No, as stated earlier, there is a security vulnerability that means using free WiFi could endanger corporate data.

Q: Can I connect to the corporate network using my BCC Smartphone to check my emails and calendar?

A: Yes, if your phone is connected to the O2 network it can securely connect to check emails and calendars.

Q: Can I connect to the corporate network using my BCC Smartphone to use my desktop applications?

A: Not necessarily, not all applications are mobile enabled – it will depend on the application vendor what mobile offering is available.

Q: Can I use my BCC Smartphone to provide an internet connection which my BCC laptop can use to connect to the corporate network?

A: Yes, this is known as tethering. A BCC Smartphone can share its mobile data connection with your BCC laptop. For this you will need a BCC Smartphone, a BCC Laptop with NetMotion software installed and a NetMotion license.

Q: Can someone from another organisation get access to data or applications within BCC network?

A: Yes, this should be raised a specific request to Service Birmingham.

Q: Why do I have a different password on my BCC Smartphone and Network?

A: You have 2 separate passwords to manage when using a BCC Smartphone, the first unlocks the phone and is to secure the phone – you must enter this every time you use the phone. The second password provides access to the BCC network and is the same password that you use to access your PC – you will only need to enter this password when you change your network password.

IT Security Layers

		Corporate		Non-Corporate	
		Laptop	Tablet / Smartphone	Laptop	Tablet / Smartphone
MDM	Secures data on mobile devices, provides remote support capabilities and ability to remote wipe data on lost or stolen devices		✓		✓
Corporate APN	Provides secure connection for mobile devices to the corporate network via 3G/4G		✓		
NetMotion	Provides secure connection for laptops to the corporate network	✓			
2FA	Two factor authentication - increases authentication security, a requirement for PSN and UAG users	1		✓	✓
UAG	Provides web access to specific published applications (NB. 2FA required)	✓	✓	✓	✓
Citrix	Provides remote access to specific published applications, including desktop applications	✓		✓	

Notes

1. Users accessing the PSN "walled-garden" environment will continue to require 2 factor authentication, but other users of Corporate Laptops do not