ISLINGTON

Report of: **The Corporate Director of Finance and Resources.**

Meeting of	Date	Agenda Item	Ward(s)
Audit Committee	6 June 2016		

SUBJECT: The TicketViewer Breach and Cybersecurity

1. Background

1.1. Islington Council is a digital organisation; we exploit the benefits of digital technologies to help staff work efficiently, to collaborate with partners to support residents and to offer online services to citizens. We are now highly reliant on our ICT capabilities in almost all we do.

1.2. Like all digitally enabled organisations, Islington Council is under constant attack; in April 2016 Digital Services blocked 924,096 spam and phishing emails, many of which seek to compromise the Council's infrastructure and information; and of the 40 million attempts to connect to our network we check every day around 85% are blocked as unwanted.

1.3. The threat is sustained and growing. Our attackers come in many forms from the archetypical teenage hacker in their bedroom; through to crime syndicates and the proxies of nation states.

1.4. The vast majority of these attacks are untargeted – those perpetrating them have nothing specific against Islington Council – and they simply seek random victims to exploit for their own ends. A smaller number may be targeted at us.

1.5. Our attackers have many motivations, including financial gain, publicising their causes and malice whether they be specific to Islington Council, the wider public sector, the UK, or general western interests.

1.6. Whilst the threat of malicious attacks is great, as a digitally enabled organisation we also face the risk of unintentional vulnerabilities or accidental actions resulting in information security breaches. These can result in significant business disruption and reputational damage. If criminals become aware of them, they may exploit them further.

1.7. The council benefits from government and industry security information sharing arrangements to keep us up to date with the latest vulnerabilities and threats and has access to specialist and specific support from the PwC cybersecurity team through our internal audit contract.

1.8. Both malicious and accidental actions can cause information security breaches. Both must be managed as security incidents.

2. Recommendations

2.1. Recognise there needs to be a balance between delivering the digital transformation programme at the required pace and maintaining appropriate and proportionate information security controls, and that this an agreed approach to risk.

2.2. Request internal audit explore broader information security risks, focussing their work on the identification and protection of our higher risk information assets, largely those containing sensitive personal information and accessed from outside the council's network to enable self-service and information sharing with partners.

3. The changing nature of the threat and our response

3.1. Cybersecurity has traditionally relied on strong perimeter defences to prevent attackers from accessing our internal network and information on the assumption that the "baddies" were on the outside and the "goodies" were on the inside, and if we built a big enough walls we could keep them separate.

3.2. While this approach remains an essential part of our security it is no longer sufficient; for us to use and provide digital services we have to enable the flow of information to and from our partners and our citizens; and our attackers are constantly finding new ways of using these channels to get inside our network and attack us from within.

3.3. Common forms of cyber-attack that seek to use legitimate routes into our network for malicious purposes include attachments on emails containing malware; links to websites which automatically install malware on our computers and the exploitation of web forms.

3.4. Attackers who are specifically targeting us will also seek to exploit human factors, either by subverting our employees or contractors (insider threat), or by relying on poor security behaviours to gain a foothold.

3.5. We have responded to both implementing security-in-depth where vulnerable systems like email have multiple layers of protection so if one is compromised we still have other defences and by educating staff on how to identify and handle attacks. This is often referred to as a 'layered defence'.

3.6. Some of our most effective defences are mundane; such as regular checking for vulnerabilities; ensuring unused network accounts are removed promptly and updating security patches across our entire infrastructure quickly.

3.7. Despite these efforts, best practice across the cyber-security community is to operate on the 'assumed breached' principle. This approach starts from the premise that successful cyber-attacks are inevitable and every network has been, or will be, compromised. We are responding to this by preparing for different types of attacks to minimise the impact and restore normal services as quickly as possible.

4. Three Islington case studies

4.1. These case studies highlight the risks are real and relevant to Islington and illustrate the work Digital Services is doing to protect Islington's information and services.

4.2. In summer 2015 we were informed by government security services that we had been targeted with carefully crafted emails containing links to sites hosting malware; external advice indicated this was an advanced, persistent threat most likely from state sponsored hackers seeking particular information that Islington might hold to support their economic objectives. Extensive checking demonstrated our defences had repelled this attack and our network had not been compromised.

4.3. In autumn 2015 we suffered a ransomware attack similar to that which affected Lincolnshire County Council and was widely reported in the media. Prompt reporting by the first user affected combined with early detection allowed Digital Services to contain the attack to one service area, remove the ransomware and restore the encrypted files within a day, with minimal impact on Islington services.

4.4. On Christmas Day 2015 one of Islington Council's campaign websites was hacked and our content replaced with alternative content. Alerted by a concerned citizen the Council's out-of-hours service invoked Digital Services incident plan and the unauthorised content was promptly replaced and the campaign site further strengthened.

5. The TicketViewer Breach

Background

5.1. A concerned citizen legitimately using the TicketViewer system noticed they could see potentially personal and/or sensitive personal information relating to other people and alerted the council. The TicketViewer system was shutdown immediately to prevent further breaches and following an initial investigation to verify the situation we self-reported to the Information Commissioners Office and initiated an internal audit led cybersecurity review.

5.2. The TicketViewer breach was not the result of a malicious attack, but a combination of unintentional vulnerabilities that occurred without the Council realising. While the TicketViewer breach has many similarities with cyber-attacks, those who identified the weakness reported it to the Council rather than exploiting them.

5.3. If the failure had been exploited maliciously, the entire contents of the parking database could have been stolen by cyber criminals and/or placed irretrievably in the public domain causing embarrassment to citizens and exposing the impacted citizens to the risk of crime. The vulnerabilities could have enabled a malicious criminal to attack other systems.

Audit findings

5.4. The internal audit led review found the breach was caused by a combination of factors:

5.5. Firstly, the service was hosted on infrastructure managed and maintained by third parties, and was not subject to the same management controls as our core infrastructure.

5.6. Secondly, there was a misconception that the system did not contain any personal or sensitive personal information, so the need for additional controls was not identified.

5.7. Thirdly, there were design faults in the application, which was developed in-house some years ago, which allowed simple manipulation of the results of one search to access other records; and did not separate the pictures of the offences from other more sensitive information.

5.8. Fourthly, misconfiguration of the web server enabled any user to see other people's records on the system.

5.9. Fifthly, misconfiguration of the application firewall allowed unfettered access to the system, and opened up the possibility of the contents of the database being copied off our network. While this is possible, extensive forensic investigation found no evidence that this happened.

5.10. While the TicketViewer system was hosted separately from most other Council systems there were links to other applications and attackers could have silently secured control of the TicketViewer system and used this as a platform within our boundary defences to attempt to compromise other systems. While this is possible, extensive forensic investigation found no evidence that this happened.

5.11. Digital Services commissioned an external reconnaissance test to identify any other potentially vulnerable applications outside the main data centre and found no similar circumstances.

Current situation

5.12. The TicketViewer system remains unavailable. This is an inconvenience for citizens and is impacting on business processes. There is a strong desire to restore the ability to view information supporting parking tickets online in a way which is secure.

5.13. The Digital Services led review of the business processes and supporting technology is drawing to a close. The fieldwork is complete and the results are being collated to produce a detailed technical action plan to support the broader audit recommendations.

5.14. A Web Services Standard has been produced, and approved by the council's Technical Design Authority (TDA) which introduces specific technical controls which all new web-based systems must comply with. The standard includes guidance from Microsoft and the Open Web Application Security Project (OWASP). Systems built to this standard will mitigate many of the most common forms of external threat.

Next steps

5.15. While the detailed results are being collated some clear themes have emerged:

5.16. TicketViewer functionality is available in the new parking management system – Taranto - and utilising this, rather than the original locally developed system, will provide greater assurance that the system is robust. We estimate it will take three months to implement this module.

5.17. The alternative internet connection and supporting infrastructure at Old Street unnecessarily duplicates functionality available on the core network and introduces additional risk. The feasibility of channelling all internet traffic via the two main connections is under investigation.

5.18. Data centre consolidation plans, which are likely to reduce the number of data centres operated across Camden, Haringey and Islington, needs to consider whether the Old Street data centre is better integrated into other existing facilities.

Additional work with PwC as our internal auditors is under consideration. This will examine broader information security implications, particularly in high risk applications where sensitive personal

information is potentially exposed outside the network to support self-service functions and information sharing.

Implications

Financial implications:

5.21. The Information Commissioner's Office (ICO) has powers to levy a financial penalty of up to £500,000 for each data breach. The ICO is still investigating the TicketViewer breach and we are not yet aware if the Council will be fined or face other compliance action.

5.22. Dealing with a cybersecurity incident has significant financial implications; including the initial response, investigations, expert advice and implementing any recommendations; and also the loss of service and potential loss of income or additional expense in providing services.

5.23. This must be weighed against the cost of remediation and/or investment to prevent or reduce the risk and impact of information security breaches.

Legal Implications:

5.24. Principle 7 of the Data Protection Act states that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Most fines levied by the ICO have been for breaches of Principle 7.

5.25. The EU has just published the final text of the General Data Protection Regulation, which is due to become law on 25 May 2016, and will be enforceable from 25 May 2018. This regulation will enable fines of up to €20Million for data breaches.

5.26. While the Ticket Viewer breach involved an internally-developed bespoke system, care should still be taken when procuring third-party solutions or cloud services, as the data and information security risks remain with the Council. Due diligence should still be undertaken, and the Council sufficiently assured that risks are appropriately mitigated and/or liability is shared before committing to contracts with third parties.

Environmental implications

5.27. None

Resident Impact Assessment:

5.28. The loss of personal and sensitive information relating to residents clearly has an impact on them individually; and the resulting loss of service may have an impact on many residents.

Conclusion and reasons for recommendations

5.29. Digital technologies bring risks as well as opportunities; the Council needs adopt and maintain an appropriate balance to provide effective services while accepting appropriate risk.

5.30. With around 400 applications in use, increasing citizen self-service over the internet and the commodification of advanced hacking tools there remains a danger of further data breaches despite our extensive efforts to protect our applications and information.

24 May 2016

Signed by	…….	……..
	Corporate Director of Finance	Date
Received by	…….	……..
	Head of Democratic Services	Date

Appendices

- None.

Background papers:

- None.

Report author: Adrian Gorst, Digital Services
E-mail: adrian.gorst@islington.gov.uk