ISLINGTON
For a more equal future

Resources Directorate

Islington Council 7 Newington Barrow Way N7 7EP

Report of: Corporate Director of Resources

Meeting of: Audit Committee

Date: 13th June 2022

Ward(s): All

The appendix to this report is not for publication

Subject: Cyber Defence Assurance for LBI

1. Synopsis

1.1. This paper is to provide an annual update on the assurances around the cybersecurity protections in place that ensure the integrity of the council's operations and data security.

2. Recommendations

2.1. To note, this report as a statement of the current position for the council's cybersecurity assurance programme and the ongoing audits and activity.

3. Background

3.1. This paper provides an update on cybersecurity activities over the last year and highlights how the cybersecurity posture has improved for the council.

3.2. This is the Annual Report to CMB and Audit Committee on the state of the council's cyber defences in the context of the broader cyber environment. It reflects the senior leadership's acknowledgement that cybercrime is a significant risk and resolve to keep cybersecurity central to all digital activity to protect our services and the private information of residents.

4. The Cyber Environment

4.1. In recent months, all UK Government and non-Government entities have been alerted to a heightened threat to security. The geo-political unrest outside the UK has forced many, including LBI, to be on high alert for both state-sponsored and opportunistic malicious/hostile cyber activity.

4.2. The National Cyber Security Centre (NCSC) guidelines continue to be the reference point for LBI. These frameworks have helped identify how 'in the wild' attacks may affect the LBI digital and non-digital estate and to guide what activities should be actioned to promote resilience.

4.3. Industry cybersecurity researchers and leading vendors continue to highlight opportunist cyber-attacks against End User Computing (laptops), Data Stores and Cloud environments, with specific focus on Ransomware, which continues to be the malware that causes the most organisational-wide problems, across multiple industries including local government.

4.4. According to the IT Governance quarterly cybersecurity review, ransomware protection has improved, and this is reflected by a steady decrease in ransomware incidents - from over 50 reported occurrences in April 2021 down to below 25 such occurrences by September 2021. This is further corroborated by the 'State of Ransomware 2021 Sophos Report' where it concludes UK organisations managed to block 39% of ransomware attacks before the hackers could encrypt the data with their own password. Which means, protection from the remaining 61% is reliant on organisational security capabilities and awareness of its people – supported by good policies and processes.

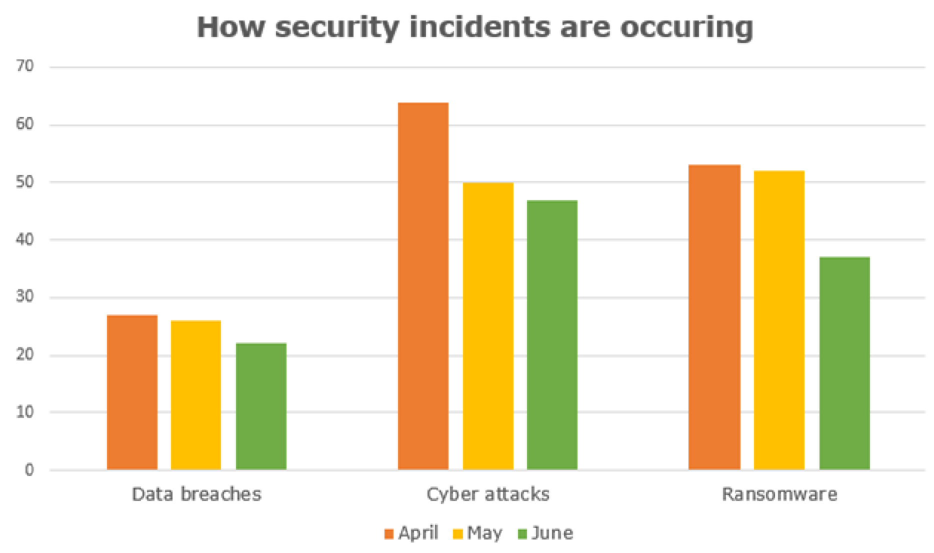

Figure 1: Data breaches and cyber-attacks quarterly review: Q2 2021 (itgovernance.co.uk)

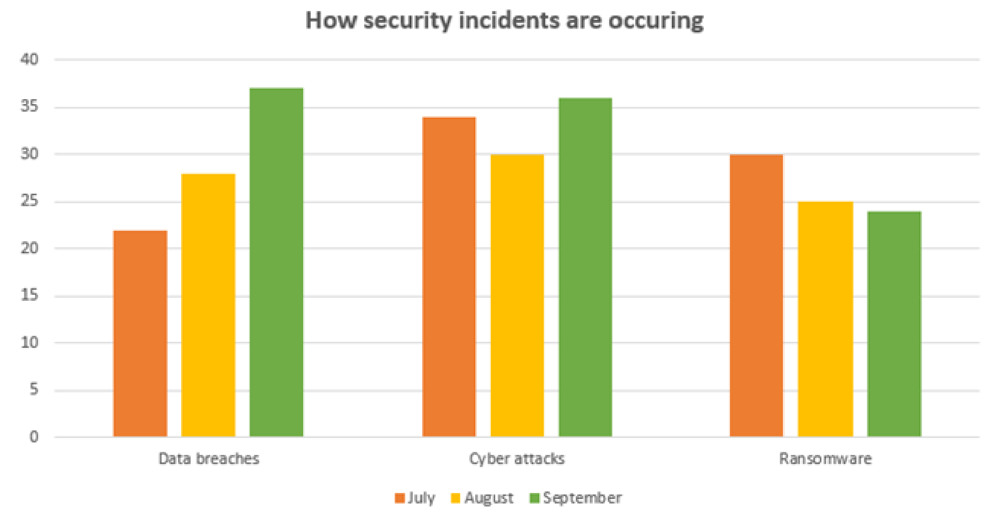

Figure 2: Data breaches and cyber-attacks quarterly review: Q3 2021 (itgovernance.co.uk)

4.5. The IT Governance finding further notes, data breaches have seen an increase due to the rise in social media/phishing and malware instances. Overall, the survey found that occurrences of cyber-attacks by hackers remain steady.

4.6. Motivations for hackers are not always known but there is often a financial driver. A person's data profile fetches £1 per person in the dark web currently, on the other hand, one employee's corporate data profile can fetch up to £10 or more. Beyond financials, the malicious nature of unauthorised access and its impact is seen constantly in the news.

4.7. The UK Government remains an attractive target for a broad range of malicious actors. Of the 777 incidents managed by the National Cyber Security Centre (NCSC) between September 2020 and August 2021, around 40 percent were aimed at the public sector identified by the UK Government's 'Cyber Security Breaches Survey 2022' report1.

4.8. The government has identified that 'Cyber Security Cybersecurity Resilience' will continue to play an important role and that all critical government functions must be significantly hardened to cyber-attack by 2025; with all government organisations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030.

4.9. Finally, data from Gartner shows that 72% of public sector IT leaders are continuing organisational digitisation, which places renewed focus on digital cyber resiliency2. The government's National Cyber Strategy 2022 found that other factors like state espionage will likely continue to exploit national-strategic vulnerabilities. Whilst our government is working with allies to disrupt sophisticated shared threats from Russia and China, Iran and North Korea continue to use digital intrusions to achieve their objectives to increase their sovereign based digital footprint through their own state-based digital products or through digital theft and sabotage.

[1] Cybersecurity Breaches Survey 2022

[2] The ability to anticipate, withstand, recover and adapt to adverse conditions, stresses, attacks, or compromises on systems.

5. Summary Self-Assessment

Updates have been provided against the self-assessment framework that was used last year. The updates are based on the National Cyber Security Centre (NCSC) paper entitled: “Questions for boards to ask about cyber security”. Cybersecurity remains a complex and technical topic.

The results of the assessment are contained in Appendix 1 (Exempt).

6. Implications

6.1. **Financial Implications**

All costs associated with cyber security are budgeted for and funded within the Islington Digital Services budget. There are no additional costs resulting from this report.

6.2. **Legal Implications**

Under UK GDPR, the Council has a duty to assess risk and to implement technical and organisational measures to meet security risks (whether from cyber-attack, or from physical or organisational matters), taking into account: the state of the art; the costs of implementation; and the nature, scope, context or purposes of the data processing; as well as the level and likelihood of the risk (Article 32(1)).

6.3. **Environmental Implications and contribution to achieving a net zero carbon Islington by 2030**

There is no additional on-premise hardware that will require further energy consumption as part of this paper. All data processing is in-cloud on a leveraged platform.

6.4. **Equalities Impact Assessment**

There are no implications in this report in relation to achieving a net zero carbon Islington.

7. Conclusion and reasons for recommendations

7.1. It is recommended that this report be noted as a statement of the current position for the council’s cybersecurity assurance programme and the ongoing audits and activity.

Appendices:

- Appendix 1 - NCSC Assessment Questions (Exempt)

Final report clearance:

Signed by:

Authorised by Dave Hodgkinson

Corporate Director of Resources

Date: 24 May 2022

Report Author: Jon Cumming, Director of Digital Services
Tel: 020 7527 5175
Email: jon.cumming@islington.gov.uk

Financial Implications Author: Steve Key, Director Service Finance
Tel: 020 7527 5636
Email: Stephen.Key@islington.gov.uk

Legal Implications Author: Uma Mehta CBE, Assistant Director of Law
Tel: 020 7527 3127
Email: Uma.Mehta@islington.gov.uk