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: 23rd May 2023

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The appendix to this report is not for publication.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 an annual cybersecurity report to provide an update on the cybersecurity environment and assurance that appropriate protections are in place to ensure the integrity of the council's operations and data.

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

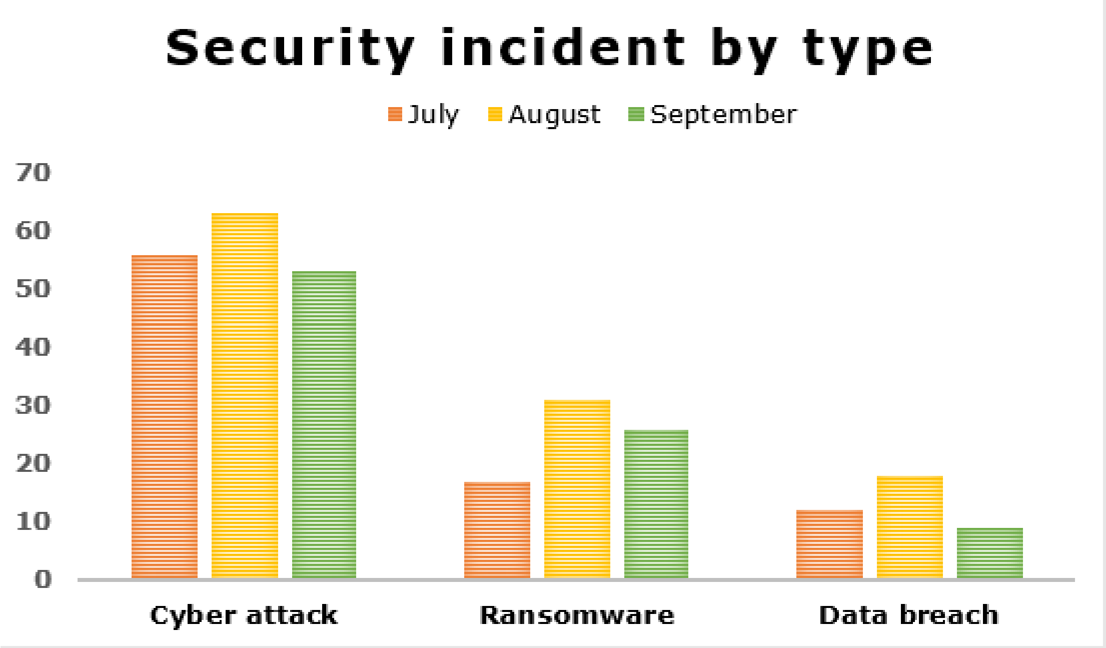
3.1. This is the Annual Report to Audit Committee on the state of the council's cyber defences in the context of the broader cyber environment. It reflects the senior leadership's acknowledgement that cybercrime is a significant risk and resolve to keep cybersecurity central to all digital activity to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

3.3 During the last year, Islington Digital Services (IDS) has recruited a new Chief Technology Officer and new Head of Cyber Security. With new leadership comes fresh ideas and new energy which will ensure we maintain the necessary momentum to protect residents and the council from cyber threats.

4. The Cyber Environment

4.1 The environment remains as volatile as ever. Rogue nation states, geo-political uncertainly, opportunist attacks, and the risks from human error and/or not following policy are all issues which impact on the secure operations of this local authority. The investment in cyber security protections have improved our resilience, and the continued engagement of LBI with other local government partners and central government co-ordinating bodies provides ‘strength in the union’. However, threats continue to evolve and become more sophisticated so as always, there is no room for complacency. This is especially true with the adoption of new technologies such as ChatGPT which can be used for creating credible phishing emails, as much as it can create content and author reports. Islington will retain and strengthen its standards, information security frameworks and connection protocols with other organisations. We must learn from the adverse experiences of others to ensure we do not succumb to the same risks. We will continually improve and refresh our security posture.

4.2 There has been a decline in the number of ransomware attacks noted by IT Governance in their quarterly review of global publicised data breaches. Nevertheless, cyber-attacks are not always disclosed due to the potential adverse publicity they bring. And even if the actual number of incidents has fallen, the threat from ransomware attacks remains high as does that from more traditional cyber-attacks methods such as phishing.



5 Summary

5.1 Islington continues to make strong progress in this crucial area. However, complacency can be fatal. The Cyber Security team continues to develop and provide an excellent service to everyone in the Council and maintain its pivotal role in the provision of technology solutions. In this fast-changing environment we use our intelligence gathering capabilities, strong internal and external relationships, and intellectual curiosity to get ahead of the attackers and protect the data of everyone who works or lives in Islington.

5.2 We will continue to seek accreditations and show demonstrate achievement, and in so doing improve our defences against new and persistent threats. We will adopt new models and technologies and ensure our people are fully trained and alert to the risks when handling sensitive data in a complex organisation.

5.3 People, processes and technology; All three elements are essential to protecting information and we will focus on each diligently in the coming year.

6 Implications

6.1 Financial Implications

All costs associated with Cyber Security are budgeted for and funded through the Digital Services budget within the Resources directorate. There are no budgetary pressures 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-premises hardware that will require further energy consumption as part of this paper.

All data processing is in the cloud on a leveraged platform where we have cyber solutions which the Council is refining and optimising. Once the maturity has been gained, the Council will add additional appropriate workloads in the cloud to increase its cyber resilience. This will most likely result in a future energy increase though most cloud infrastructure providers are striving to reduce the carbon footprints for their services.

6.4 Equalities Impact Assessment

The council must, in the exercise of its functions, have due regard to the need to eliminate discrimination, harassment and victimisation, and to advance equality of opportunity, and foster good relations, between those who share a relevant protected characteristic and those who do not share it (section 149 Equality Act 2010). The council has a duty to have due regard to the need to remove or minimise disadvantages, take steps to meet needs, in particular steps to take account of disabled persons' disabilities, and encourage people to participate in public life. The council must have due regard to the need to tackle prejudice and promote understanding.

Equality impacts would only be considered if individuals within a protected group were affected by one of the following:

- A new policy
- Procedure
- Function
- Financial decision
- Restructure

As this document is just a statement on current positions, and not any of the items within the list which affect individuals, it would not have any impact on protected groups and, therefore, no equality implications.

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:

- Exempt Appendix 1 – Highlights from 2022/23 and Outlook for 2023/24

Final report clearance:

Signed by:

Corporate Director of Resources

Date: 15 May 2023

Report Author: Tim Rodgers, Head of Cyber Security

Email: timothy.rodgers@islington.gov.uk

Financial Implications Author: Charlotte Brown (Strategic Business Improvement Manager)

Legal Implications Author: Sonal Mistry (Senior Lawyer - Governance)

Environmental Implications Author: Gearoid Kennedy (Sustainable Energy Partnerships Manager)

Equalities Implication Author: Hezi Yaacov-Hai (Policy, Engagement and Complaints Officer)