ISLINGTON
For a more equal future

Resources Directorate

222 Upper Street, London N1 1XD

Report of: Corporate Director of Resources

Meeting of: Audit and Risk Committee

Date: 21 May 2024

Ward(s): All

The appendix to this report is not for publication.

Subject: Cyber Defence Assurance for London Borough of Islington – Annual report

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 the Audit and Risk 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.

3.2 During the last year, Islington Digital Services (IDS) has consolidated its position regarding Cybersecurity, by reviewing and refreshing technical solutions where appropriate,

maintaining a strong approach to training and awareness, reviewing countless solutions for cyber compliance and maintaining a robust approach to architecture and policy standards. Following the IDS reorganisation, additional positions have been created in the Cybersecurity team which are subject to external recruitment.

4. The Cyber Environment

4.1 In last year's report we wrote of the volatile global cyber security environment. This continues to be a significant factor, though arguably the biggest threat to the Council has been in the form of phishing attempts where people attempt to secure money through social engineering. Through our partner networks, we continue to be aware of fellow organisations who have been compromised through sophisticated technical attacks and continue to adopt a robust defensive position across technology, policies and standards. We mentioned Artificial Intelligence briefly last year, and this continues to be a concern in terms of data handling, which is why we moved on preventing access to non-prescribed generative AI solutions such as ChatGPT.

4.2 The Information Commissioners Office is the regulator responsible for data protection and, therefore, is to be informed in the event of a significant data breach. They collate intelligence regarding incident types. Responsibility for responding to these incident types is spread across the Cybersecurity and Information Governance teams. In terms of protections, the Council has a secure email system in place which would help mitigate against incorrect addressing (the most 'popular' type of incident), robust training, awareness and policy to try and prevent some of the more 'human' breaches, and very strong technical systems regarding the more sophisticated attacks which we are continually reviewing and refining. We continue to have 24/7 capability to respond to any relevant out-of-hours incidents.

5. Summary

5.1 Islington continues to be one of the leading authorities in London regarding Cybersecurity. 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 and has attending departmental management teams to further enhance the relationship between IDS and the business. We have implemented additional threat intelligence capabilities to add to our peer networks and OSINT sources to try and stay ahead of the bad guys.

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 Last year, we finished the summary reflecting on People, processes and technology. By focussing relentlessly on these, we'll do all we can to keep Islington's data safe.

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

UK cybersecurity law can be grouped into the following areas:

1. Data protection and privacy law applying to personal data
2. Security of network and information systems law
3. National security laws
4. Criminal laws relating to cyber crimes.

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)).

Officers may wish to adopt and have regard to the Government Cyber Security Strategy 2022–2030 (publishing.service.gov.uk) There are appropriate organisation structures, policies, and processes in place to understand, assess and systematically manage security risks to the network and information systems supporting essential functions of the Council's business. The Council has appropriate management policies and processes in place to govern its approach to the security of network and information systems.

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 equalities implications arising from this report.

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 – Highlights from 2023/24 and Outlook for 2024/25 (exempt from publication)

Final report clearance:

Signed by:

Corporate Director of Resources

Date: 13 May 2024

Report Author: Tim Rodgers, Head of Cyber Security
Email: timothy.rodgers@islington.gov.uk

Financial Implications Author: James Blood
Email: James.Blood@islington.gov.uk

Legal Implications Author: Jabeen Story
Email: Jabeen.story@islington.gov.uk