ISLINGTON

Resources Directorate

Report of: Corporate Director of Resources

Meeting of:	**Date**	**Ward(s)**
Audit Committee	5th October 2021	All

Delete as appropriate	Appendix is Exempt	

THE APPENDIX TO THIS REPORT IS NOT FOR PUBLICATION

SUBJECT: CYBER-DEFENCE ASSURANCE UPDATE

1. Synopsis

1.1 This paper provides an update on the assurance around the Cybersecurity protections in place to ensure the integrity of the council's operations and data security.

2. Recommendation

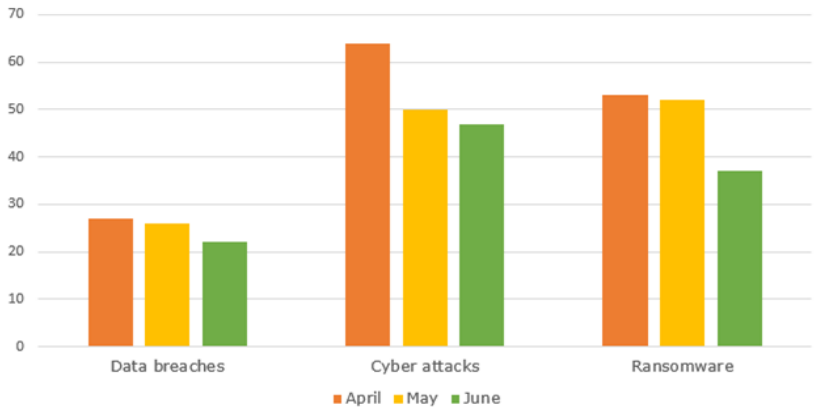
2.1 To note this report as a statement of the types of cyber-attacks and ransomware over the last calendar quarter and the actions IDS are taking. The current position for the council's cybersecurity assurance programme and the ongoing audits and activity.

3. Background

3.1 This paper summarises the external threat landscape faced by the public sector, recap on cybersecurity assurances in place to protect our operations and ensure we meet our data protection obligations. And includes the progress made in responding to audits and technical assessments and the initiatives we are working on to upgrade the Council's productive suite, recruitment and controls and protections.

3.2 During the Covid pandemic cyber-attacks leveraged the attention of the pandemic to launch phishing campaigns, propagate fake news, production of fake covid websites and zoom bombing. It is expected this will continue while the pandemic lasts.

3.3 As we move to hybrid working arrangements the external threat landscape is still challenging, IT Governance Q2 Cybersecurity quarterly review and more sophisticated Zero Day[1] exploits are emerging that focus on software bugs that present security vulnerabilities such as:



- Ransomware – According to Microsoft Protection Centre, ransomware continues to be a global problem. The public sector continues to face a high risk to the ransomware attacks which focus on extracting data before encrypting customer systems and holding the customer to ransom.

- Print Nightmare - Cyber criminals have exploited two critical vulnerabilities in the Windows print spooler. Print spooler is a Windows service used for printing documents and is enabled by default in all Windows client and server operating systems across all organisations around the world. The print spooler vulnerability is a zero-day bug and forced many organisations to stop printing.

3.4 IT Governance further noted Cyber-attacks continue to be by far the most common type of security incident when compared to data breaches and Ransomware. Whilst the term 'cyber-attacks' encompasses a broad range of threats, criminal hackers were most likely to breach organisations by exploiting system vulnerabilities (e.g., unpatched applications or servers).

4. Top 5 reported threats for Q2 2021

4.1 The table below gathered from various threat advisory sources illustrate the types of cyber attacks and ransomware reported over the last calendar quarter.

Threat	Commentary
Third party & supply chain attacks on the rise	A supply chain attack (also called a third-party attack) occurs when a system gets infiltrated through an outside partner or provider that has access to targeted systems and/ or data. As the number of digital and professional services partners increase, so does the attack surface.
After ransomware, enterprises are most worried about phishing attacks post-pandemic	Omdia's "2021 Enterprise Security in a Post-Pandemic World" survey, phishing was identified by 57% of respondents as a key concern, which was second only to ransomware concerns.

[1] A 'zero-day' attack takes place when hackers exploit a vulnerability before developers have a chance to address it.

New phishing attack techniques discovered by Microsoft	Microsoft has identified a phishing campaign that uses new techniques to avoid detection by email security filters. This is used in spear-phishing, which is a targeted form of phishing, where the message is designed to look like it's from a person the recipient knows and trusts.
Exploitation of previously disclosed vulnerabilities in Microsoft Exchange Servers	The National Cyber Security Centre (NCSC) have flagged in their weekly threat report, the continued exploitation of the 'Proxyshell' exploit chain that is targeting unpatched Microsoft Exchange Servers.
AI and ML-driven attacks	Cybercrime is evolving with advanced machine learning (ML) and artificial intelligence (AI) approaches. This is a significant emerging threat.

4.2 The activities IDS are currently taking to mitigate these threats are contained in Appendix 1 (Exempt)

4. Assessment Framework Recap

4.1 The Cyber Security Assurance report is based on the National Cyber Security Centre (NCSC) paper entitled:
"**Questions for boards to ask about cyber security**."

4.2 This is taken from NCSC's Cyber Security Toolkit for Boards and is a recognised and pragmatic approach to demonstrating assurance. It examines the basic questions of:

1. Embedding cyber security into your structure and objectives
2. Growing cyber security expertise
3. Developing a positive cyber security culture
4. Establishing your baseline and identifying what you care about most
5. Understanding the cyber security threat
6. Risk management for cyber security
7. Implementing effective cyber security measures
8. Collaborating with suppliers and partners
9. Planning your response to cyber incidents

4.3 The updated results of the assessment, controls and activities are contained in Appendix 1 (Exempt)

5. Implications

It is important that the council maintains a strong cyber defences and related assurance. Ongoing focus on improvements and assurance will continue to be an important part of technology investment and monitoring.

5.1 Financial implications:

There are no financial implications arising from this report. The measures and recommendations proposed in this report are not currently quantifiable. Any recommendations from this report, if adopted, will need to be expanded upon and reviewed with the financial implications assessed.

5.2 Legal Implications:

The Council must act economically, effectively, and efficiently in accordance with best value and principles of good governance and protect data. Under UK GDPR the Council must implement appropriate technical and organisational measures to meet security risks, whether from cyber-attack or otherwise (Article 32(1)).

5.3 Environmental Implications and contribution to achieving a net zero carbon Islington by 2030:

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

5.4 Resident 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.

No resident impact assessment has been completed as the cyber assurance provided in this paper is to ensure as far as is practicable that there is no impact to resident services or outcomes due to cyber attack

6. Reason for recommendation

6.1 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 – Summary of Cyber Assurance activity & Audits.

Final report clearance:

Signed by:

Dave Hodgkinson
Corporate Director of Resources

Date 17 September 2021

Report Author: Jon Cumming
Tel: 02075275175
Email: jon.cumming@islington.gov.uk

Financial Implications Author: Ivana Green
Tel: 02075277112
Email: Ivana.Green@islington.gov.uk

Legal Implications Author: Peter Felher
Tel: 02075273126
Email: peter.fehler@islington.gov.uk