ISLINGTON

Resources Directorate

Report of: Corporate Director of Resources

Meeting of:	**Date:**	**Ward(s):**
Audit Committee	25 May 2021	All

Delete as appropriate	Non-exempt	

THE APPENDIX TO THIS REPORT IS NOT FOR PUBLICATION

SUBJECT: CYBER-DEFENCE ASSURANCE

1. Synopsis

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

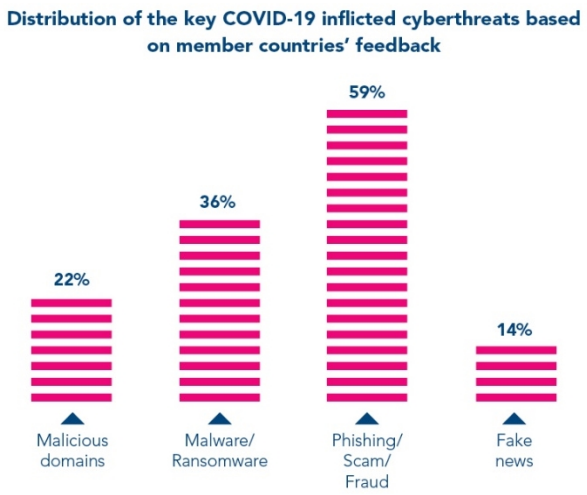
2. Recommendation

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

3. Background

3.1 This paper summarises the cybersecurity assurances in place to protect our operations and ensure we meet our data protection obligations. It gives context to the current cyber-environment which has been dominated by Covid. The frameworks and methods to assess our resilience are also explained.

3.2 The external risk profile has increased with the advent of Covid. This graph from an Interpol report[1] shows the profile of attacks. Phishing attacks are a popular vector in times of crisis as people are willing to take more risk on issues such as PPE, test and vaccine opportunities – or simple online 'deals'. Layer on the added vulnerabilities created by working from home, fake security alerts etc and it is a rich environment for those with no scruples.



3.3 Some statistics from September 2020 by ZDNet Government state:

- The number of unsecured remote desktop machines rose by more than 40%
- Remote desktop 'brute-force' password attacks grew 400% in March and April 2020
- Email scams related to covid-19 surged 667% in March 2020 alone
- Users are now three times more likely to click on pandemic-related phishing scam
- 90% of newly created coronavirus domains have a scam purpose
- More than 530,000 zoom accounts sold on dark web
- 2000% increase in malicious files with "zoom" in name
- Covid-19 has driven between 72% and 105% of the ransomware spike

3.4 The cyber environment is at its most dangerous - right at the time we are most dependant on it for remote working.

4. Assessment Framework

4.1 Cyber Security is a complex and technical topic. To ensure the assurance provided is appropriate this 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 considered to be 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

[1] https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

7. Implementing effective cyber security measures
8. Collaborating with suppliers and partners
9. Planning your response to cyber incidents

4.3 The results of the assessment 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)).

4.3 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.

4.4 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

- Exempt Appendix 1 – Summary of Cyber Assurance activity & Audits.

Final report clearance:

Signed by:

Dave Hodgkinson
Corporate Director of Resources

Date: 7 May 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