London Borough of Hammersmith & Fulham

Report to: Audit Committee

Date: 22/06/2021

Subject: **Cyber security – Six Monthly Update**

Report of: Adrian Dewey, IT Security Manager, Digital Services

Responsible Director: Veronica Barella, Chief Digital Officer

Summary

The Committee has asked that Digital Services provide six-monthly updates on Hammersmith & Fulham's cyber-security readiness. This is the update for June 2021.

Recommendations

1. Appendix 1 of this report is not for publication on the basis that it contains information relating to the financial or business affairs of any particular person (including the authority holding that information) as set out in paragraph 3 of Schedule 12A of the Local Government Act 1972 (as amended).

2. For the Committee to note and comment on the report including appendix 1.

Wards Affected: None

H&F Values

Our Values	Summary of how this report aligns to the H&F Values
• Being ruthlessly financially efficient	The delivery of appropriate levels of protection are reviewed against cost to deliver good value for money for the authority, balanced against levels of risk.
• Taking pride in H&F	The focus on cyber-security protects H&F against disruption and helps to maintain the council's reputation.

Contact Officer(s):

Name: Veronica Barella
Position: Chief digital officer
Telephone: 020 9753 2927
Email: veronica.barella@lbhf.gov.uk

Background Papers Used in Preparing This Report

National Cyber Security Centre guidance, Business Continuity Planning, Risk Management Strategy, HM Government National Risk Register, World Economic Forum Global Risks, Gartner Security and Risk Trends 2021.

BACKGROUND

1. Ransomware continues to be the most likely cyber threat to the provision of Hammersmith & Fulham’s IT service. Ransomware is a form of malware that prevents an organisation accessing its own files by encrypting them, and then demanding a ransom payment to provide the decryption key.

2. Digital Services has reviewed its defences against and readiness for a ransomware incident in light of the learning of the successful breaches that have happened in other authorities. Our defences fall into three groups.

   a) Protecting staff workstations against malware delivered by websites or emails.

   b) Protecting administrative accounts which could be used by an attacker to bypass defences and plant ransomware.

   c) Limiting the scope of an attack by keeping all software as up-to-date as possible.

   Appendix 1 is a themed risk-based overview, with indications of where we plan to improve our defences.

List of Appendices:

Appendix 1 – Analysis of ransomware defences