London Borough of Hammersmith & Fulham **Audit, Pensions and Standards Committee** **24 September 2019**	

CYBER SECURITY
Report of the Cabinet Member for Finance and Commercial Services – Councillor Max Schmid
Open Report
Classification: For decision **Key Decision:** No
Consultation: Consultation has also taken place with H&F's Business Continuity Manager, Risk Manager, and Website Manager. IT Services has consulted with RBKC and WCC as there is shared Office 365 infrastructure. Discussion and consultation have taken place with WCC and RBKC technical staff and their Senior Information Risk Officer.
Wards Affected: All
Accountable Director: Veronica Barella, Chief Information Officer

Report Author: Adrian Dewey, IT Security Manager	**Contact Details:** Tel: 020 8753 1104 adrian.dewey@lbhf.gov.uk

1. EXECUTIVE SUMMARY

1.1. Hammersmith and Fulham council, like all organisations, is constantly under threat from determined attackers. To date, the actions undertaken by the Council's IT team and its suppliers continue successfully to protect our network.

1.2. Following a report to Cabinet on 9th October 2017 entitled 'Cyber Threat Remediation', actions were taken to reduce Hammersmith and Fulham's exposure to the cyber-security risks described in the 2017 report and the cyber-security risks successfully remediated. Since the 2017 report some new cyber-security challenges have developed and have been successfully remediated.

1.3. Hammersmith & Fulham, along with many council's, operates social media accounts to communicate with the public. The organisation would suffer reputational risk if the accounts were compromised and used to post unauthorised material. Hammersmith & Fulham uses best security practice to manage its social media accounts and protect against the risk of unauthorised access to them.

2. RECOMMENDATIONS

It is requested that the Audit Pensions and Standards Committee note the following;

2.1. Recommendations made to Cabinet on 9th October 2017 have been successfully implemented, and reduced Hammersmith & Fulham's exposure to cyber-security risk to an acceptable level through;

- multi-factor-authentication
- EM+S Office 365 licensing
- monitoring of suspicious login attempts
- review of file types that can be used with Office 365

2.2. Hammersmith & Fulham's increasing use of Microsoft's Office 365 cloud-based service continues to pose cyber-security challenges, and will require regular review.

2.3. Configuration changes made to Sharepoint Online have reduced the information security risk arising from its general deployment to acceptable levels. The replacement of the Virtual Desktop environment across the council (white boxes) with Windows 10 laptops for most users has enabled flexible working as well as delivering high levels of information security control. Hammersmith & Fulham's social media accounts are well protected against the risk of being hacked and used to distribute unauthorised material.

2.4. The Council's IT operations continue to meet the security requirements of the UK Cabinet's Office Public Service Network (PSN) Code of Connection. As part of the compliance process Hammersmith & Fulham is annually audited by an independent security testing company providing independent assurance on the council's overall arrangements.

3. REASONS FOR DECISION

3.1. The report to Cabinet on 9th October 2017 'Cyber Threat Remediation', looked at Hammersmith and Fulham's exposure to cyber-security risk, and recommended a number of actions to reduce the exposure. These actions were implemented, and successfully reduced the exposure. Sections 4.1 – 4.8 (below) provide more detail.

3.2. Since the last report new cyber-security issues relevant to Hammersmith and Fulham have developed. Sections 4.9 - 4.21 provide more detail, including actions taken to reduce the organisation's exposure.

4. PROPOSAL AND ISSUES

Progress against the objectives set in the Cyber Threat Remediation report

4.1. The report authorised action to introduce mutli-factor-authentication (MFA), upgrade Office 365 licenses to gain access to advanced MFA features, increase the monitoring of suspicious Office 365 login attempts, and review whether additional blocking of the file-types that can be imported into Office 365 was required.

Multi-factor authentication

4.2. Multi-factor authentication has been implemented. Unauthorised logins to the H&F Office 365 environment from the internet have been reduced to zero. Enabling MFA required significant non-technical effort to ensure all users registered a mobile phone number through which they receive the MFA security challenge. The O365 accounts of officers and Councillors are protected through this technology.

Office 365 licence upgrade

4.3. EM+S Office 365 licence upgrade implemented. Previously, everyone had to authenticate every 3 days even when using corporate machines. The new licence has allowed MFA to be implemented in a way that minimises the number of extra steps required for logging into O365, while preserving the security benefits of MFA. The new 'Conditional Access' feature allows rule-sets to be created so that logins from trusted networks or devices are exempted from the MFA challenge.

Increased monitoring of suspicious Office 365 use

4.4. While MFA was prepared for introduction, the Council's Agilisys Service Desk was commissioned to provide monitoring of the Office 365 activity logs for Hammersmith & Fulham. Prior to deployment a number of suspicious logins were observed. The accounts were locked and the staff account owners contacted and guided through changing their passwords

4.5. Since the deployment of MFA, no further suspicious activity of this type has been observed in the activity logs.

Protection against brute-force password guessing attacks

4.6. While MFA was prepared for introduction, we continued to see elevated numbers of attempts to login to Office 365 using automated password

guessing. While these attempts have never been successful, for a time they caused account lock-outs which disrupted the ability of officers to work.

4.7. The account lock-out thresholds for the Office 365 and internal networks have been adjusted so that only Office 365 external access is locked-out. Officers or members connecting via the internal corporate network can continue to work.

Review the blocking of files and attachments for adequacy

4.8. The Council's IT Security Manager has reviewed the paths through which data can be accessed and moved in and out of the Office 365 environment. No new blocking was deemed necessary.

New threats and Hammersmith & Fulham responses since the previous report

4.9. The external threats to the Council's cyber-security have not changed significantly since the last reporting period. However, the organisation has continued to migrate data from the internal network to permanent storage within Office 365 for cost and business efficiency reasons. The Office 365 platform is more directly exposed to the internet than the internal network, so Hammersmith & Fulham's ability to configure and control Office 365 is key to avoiding new threats.

Internal file-shares replaced by Office 365 Sharepoint Online

4.10. IT Services is in the process of migrating all of the organisation's documents currently stored in file-servers on the internal network to Sharepoint Online in Microsoft's Office 365 cloud environment.

4.11. Sharepoint Online is by design a collaboration tool. Its default configuration makes it easy to share documents with other users both inside and outside the organisation. Hammersmith & Fulham has reviewed the collaboration features and taken the following action:

4.12. Sharepoint Online sites for teams within Adult and Children's Social Care have had the ability to directly share documents (by sending links to other users) removed. This is because generating links makes it impossible to audit who has access to a Sharepoint site. As these teams work with significant amounts of information classified OFFICIAL SENSITIVE it is important that access control is preserved. IT Services consulted with the Directors for Adult and Children's services to agree this remediation action.

Windows 10 roll-out

4.13. IT Services is in the process of replacing all Windows 7 based devices in use at Hammersmith & Fulham with new Windows 10 laptops. (Windows 7 will cease to be safe to use after January 2020 when Microsoft will stop providing

security patches). The Windows 10 project has been a major piece of work, and information security requirements have been included from the start.

4.14. The prototype Windows 10 Enterprise laptop build was tested by an independent third-party security testing firm as part of the Council's 2019 Public Service Network certification process. The testers reported that the security configuration of the laptop build was good. Only one vulnerability was found, which has been corrected for the production build.

Public Service Network compliance

4.15. Hammersmith & Fulham received its last PSN Certificate of Compliance on 26th September 2018. PSN certification is required to enable on-going access to DWP data. In preparation for the renewal of the certification in September 2019, the Council was independently audited in April 2019.

Business continuity and resilience

4.16. The implementation of MFA and Office 365 upgrade is a significant improvement to meet the IT challenges that the council will face in the future, it is a critical tool in protecting identity theft. It will reduce risk and increase the resilience of the council's critical business data, and better able to meet the ever-increasing sophisticated forms of cyber-attacks.

4.17. The set of proposals will ensure that H&F's core data systems are continually hardened, effectively rendering our critical data impenetrable, even under the typical conditions of a constantly changing IT environment.

4.18. The measures proposed will greatly increase the resilience of services by ensuring their dependency on essential data meets the necessary confidentiality, integrity and availability standards.

Protection of social media accounts

4.19. Hammersmith and Fulham have Twitter, Facebook, YouTube, Flickr and Instagram accounts, and uses them to communicate with the public. All of these services are consumer orientated, though increasingly used by corporate bodies as part of their communications strategy.

4.20. As consumer orientated services, each uses login via a username and password as its primary method of authentication. Except for Flickr each service also offers a two-factor authentication option, where a challenge is sent to a nominated mobile phone number before the login is authorised.

4.21. The best security practice for protecting such accounts is to:

Use a strong password. This is 8 characters minimum, with a mix of numbers, punctuation, and letters in both uppercase and lowercase. This protects against dictionary (password guessing) attacks.

Not use the password on any other internet site. This protects against the other site being compromised and its passwords exposed.

Use two-factor authentication. Even if the password is exposed, an attacker will not be able to login.

If multiple users are allowed to login to the account, a staff member must be responsible for managing this multiple use. This is either by creating and removing administrative accounts, or changing the password on a shared account, as the team of staff who need administrative access changes. This protects against individuals who have left the organisation retaining access.

4.22. Hammersmith and Fulham's Communications Team have responsibility for operating social media accounts. They report they implement best practice as follows:

	Twitter	Facebook	YouTube	Flickr	Instagram
strong password	Y	Y	Y	Y	Y
unique password	Y	Y	Y	Y	Y
two factor authentication	Y	Y	Y	not available	Y
multi-use management	Y	Y	Y	Y	Y

Consequently, Hammersmith and Fulham's social media accounts are well protected against the risk of unauthorised access.

5. OPTIONS AND ANALYSIS OF OPTIONS

5.1. This report describes the outcome of cyber-security risk reduction actions implemented prior to this report. There are no relevant options for the matters discussed in this report.

6. CONSULTATION

6.1. As LBHF, RBKC and WCC share a single Office 365 tenancy, discussion and consultation has taken place with WCC and RBKC technical staff and their Senior Information Risk Officer when making the configuration changes to Office 365 described elsewhere in this report.

7. EQUALITY IMPLICATIONS

7.1. This report describes the outcome of cyber-security risk reduction actions implemented prior to this report. There are no equalities implications.

7.2. Implications verified by: Peter Smith, Head of Policy & Strategy, 020 8753 2206

8. LEGAL IMPLICATIONS

8.1. This report describes the outcome of cyber-security risk reduction actions implemented prior to this report. There are no legal implications.

8.2. Implications verified by: Rhian Davies, Assistant Director Legal, 020 8753 2729

9. FINANCIAL IMPLICATIONS

9.1. This report describes the outcome of cyber-security risk reduction actions implemented prior to this report. There are no financial implications.

9.2. Implications verified by: Emily Hill, Assistant Director, Corporate Finance, 020 8753 3145

10. IMPLICATIONS FOR BUSINESS

10.1. This report describes the outcome of cyber-security risk reduction actions implemented prior to this report. There are no implications for businesses in the borough.

10.2. Implications verified by Albena Karameros, Programme Manager, Earls Court, Governance & Coordination, 02079388583

11. COMMERCIAL IMPLICATIONS

11.1. This report describes the outcome of cyber-security risk reduction actions implemented prior to this report. There are no procurement implications.

11.2. Implications verified by: Andra Ulianov, Head of Procurement & Contracting, 07776672876

12. IT IMPLICATIONS

12.1. This report has been submitted by H&F's IT services. It describes the outcome of cyber-security risk reduction actions implemented prior to this report. There are no further IT implications.

12.2. IT services continues to monitor cyber risks.

12.3. Implications verified by: Veronica Barella, Chief Information Officer, 020 8753 2827

13. RISK MANAGEMENT

13.1. This report describes the outcome of cyber-security risk reduction actions implemented prior to this report. There are no new risk management implications

13.2. Implications verified by: Michael Sloniowski, Risk Manager, 020 8753 2587

14. OTHER IMPLICATION PARAGRAPHS

14.1. There are no property, business intelligence, health & wellbeing, Section 106 or PREVENT implications. Information security risks are discussed in the body of the report.

15. BACKGROUND PAPERS USED IN PREPARING THIS REPORT

None.