City of Westminster

Audit & Performance Committee Report

Committee	**Audit and Performance Committee**
Date:	**1st February 2018**
Classification:	**General Release (Appendix 3 not for publication)**
Title:	**Update on the mitigation measures to protect the Council from the risk of cybercrime.**
Wards Affected:	**All**
Key Decision:	**Not Applicable**
Financial Summary:	**Not Applicable**
Report of:	**Ben Goward CIO**

1. Summary

1.1. This report provides a briefing on current cyber security arrangements that are in place and which are further developing to protect the Council from and manage the impact of cybercrime.

1.2. The paper covers the following:

- IT Cyber Security currently employed by the council
- Information Security Strategy Initiatives
- Programmes in deployment
- Programmes scheduled
- Cyber Security Incidents

2. Recommendations

2.1 That Appendix 3 attached to this report be exempt from disclosure by virtue of the Local Government Act 1972 Schedule 12A, Part 1, paragraph 7 as amended, in that it contains information relating to any action taken or to be taken in connection with the prevention of crime.

2.2 That the report be noted.

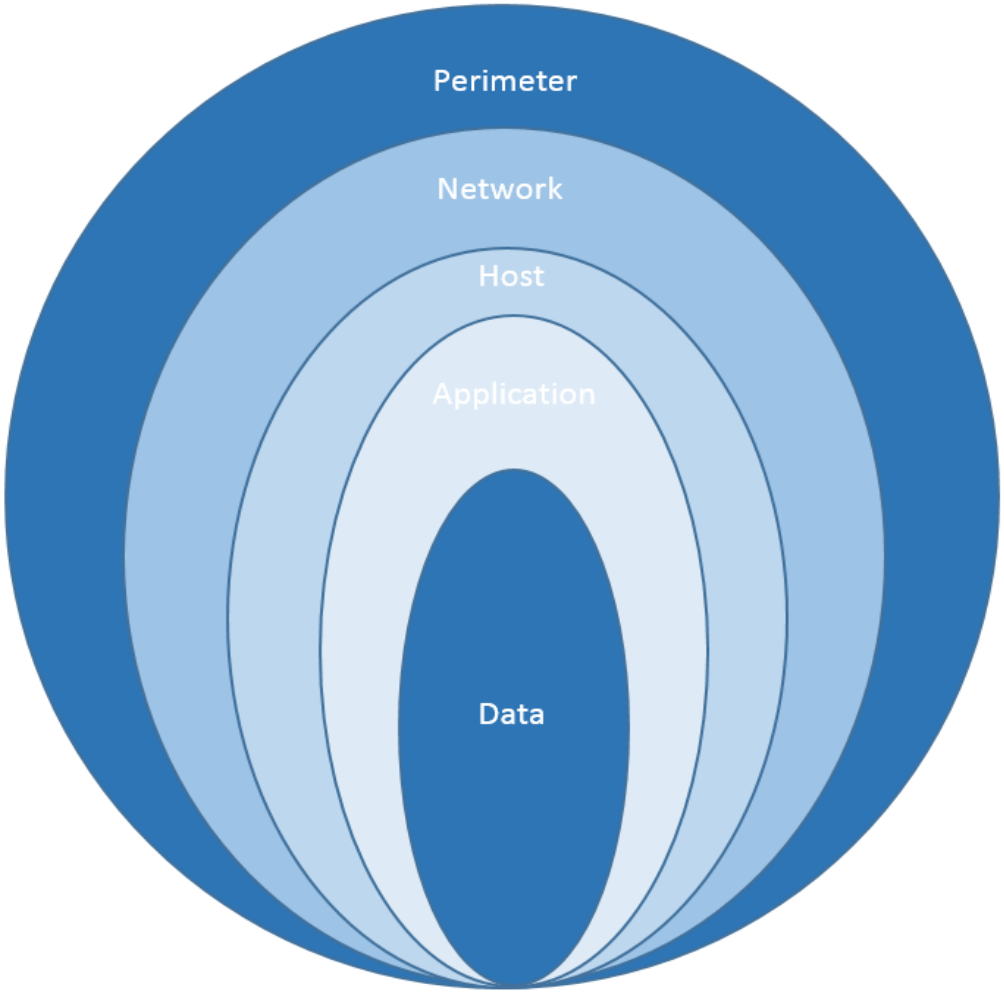
3. Cyber Security Currently employed

3.1 Cyber security for the council is provided through the implementation of security policies, technical controls and security education & awareness programs.

3.2 The Policies and technical controls support the council in achieving its compliance requirements for Legal & Regulatory obligations and in support of compliance with the PSN CoCo, NHS (Information Governance Toolkit) and Payment Card Industry – Data Security Standard (PCI-DSS).

3.3 Security policies are managed and maintained through the online tool Net Consent, which is configured for managing new starters and user re-compliance (auto notification management). Policy enforcement is configured and includes blocking access to network resources prior to acceptance by users, manages periodical renewals and provides notification to the councils Information security team (InfoSec) for all non-compliance.

3.4 The Council provide elements of defence in depth for IT services both internally and from their suppliers. Defence in depth is the principle of layering security mechanisms to increase security of the system as a whole. The following sections represent layered security (details of products currently employed can be found in Appendix 1).



Layers of Defence in Depth

Perimeter

3.5 The perimeter is the boundary between the private (council network) and public network, this is protected by security gateways (Firewalls) and services which control, inspect and prevent risks to the council's networks and services.

3.6 The Network is further protected through a demilitarized (DMZ), which sits just inside the perimeter and is segregated from both the public and internal networks and provides a controlled secure zone plus the second layer of security for the council.

Network

3.7 The council have a private site to site wide area network which provides connectivity to all their sites. The network is protected by its physical separation

from the public network. The Councils Local Area Networks sit within each site and are protected by the perimeter and DMZ.

Data Centre services and End User Compute

3.8 The data centres (DC) host infrastructure and services for the council. DC services employ defence in depth, vulnerability management and are governed by ISO 27001 certification. The ISO22301 certification assures Business Continuity & Disaster Recovery.

3.9 End user compute provides the user community's desktop, laptop and mobility requirements (iPads, iPhones and Android Phones). Desktop and laptop estates include; Anti-virus, full disk encryption, BIOS and domain login controls.

3.10 Mobility; Apple products (iPads, iPhones) by default employ encryption and have centralised control from a managed data manager (MDM). The MDM has the capability to remote data wipe plus remote lock device and SIM. The Samsung Android Phones are policy controlled by Microsoft Sync. Note: Android Phones are only permitted to handle OFFICIAL Data.

Web Services

3.11 The council's Microsoft O365 service is cloud based and connectivity to O365 is achieved across the public network. The information exchanged across the public network is secured by Network Layer Security/Secure Sockets Layer (TLS/SSL) certificates which provide encapsulation and encryption of all information. The councils web facing services are protected by controls employed by both Network and virtual cloud based Firewalls, and Web hosting is protected with defence in depth and governed by ISO27001 certification.

Other service suppliers

3.10 Agilisys provide service Desk and are ISO27001 certified.

4. Security Strategy Initiatives

4.1 The Information security strategy sets out the first strategic plan developed by the shared IT service and details the priorities for managing, control and protecting information assets. The strategy outlines the strategic objectives and mandates that future initiatives are based upon improving the council's security position.

4.2 A list of the 5 initiatives is provided here (more details can be found in Appendix 2).

1. Security Policy, Standard and Guidelines audit and update.
   Review, update and publish Security Policy, Standards and Guideline Framework.

2. IT Security Governance.

   Implement new IT Security Governance Programme.

3. Microsoft O365 Multi Factor Authentication Implementation
   Security oversight and signoff for improved Identity and Access Management (IDAM).

4. PSN re-certification.
   Drive ITHC, remediation and PSNA submission.

5. Information Security Awareness Training
   Develop and deliver a user education programme, linked with GDPR

5. Programs in deployment

5.1 The programs in this section have a relationship with the security strategy and form those programs which are already being actively implemented.

A list and summary of programs currently in deployment

1. Security Policy audit.
   Audit existing security policies against ISO27001 and industry best practice, report on status, list recommendations and requirements aligning with General Data Protection Regulation (GDPR) requirements (April 2018).

2. Security Governance
   Develop and implement Security Governance across IT Services (Jan 2018).

3. Microsoft O365 Multi Factor Authentication.
   Deploy Modern Authentication and implement Multi Factor Authentication (Feb 2018).

4. PSN Re-certification.
   Complete IT Health Check, plan and complete remediation's identified and submit application. (March 2018).

5. Information Security Awareness Training.
   Design and implement training including requirements addressing new policies and GDPR requirements (April 2018).

6. Programs scheduled

6.1 The programs in this section have yet to commence deployment and implementation the current date for completion within 2018.

Microsoft Win10

6.2 The program will see the deployment of Microsoft Windows 10 across both the WCC and RBKC EUC estates, this joint initiative is to realise the merging for management and security benefits WIN 10 enables, a security workshop at WCC is scheduled for the 9th Jan 2018.

Microsoft Intune

6.3 The program will see the deployment of Microsoft Intune which will eventually replace Airwatch again benefiting both councils, centralising management and control simplifying policy and security. Additional benefit this is a member of Microsoft cloud services family and will benefit from integration with Microsoft O365.

Microsoft SCCM

6.4 WCC already consume this service, however a new instance is required to realise the benefits of centralised management and security.

7. Cyber Security Incidents

7.1 The cyber security incidents experienced by the council are listed in appendix 3 due to the sensitive nature of this information and the risk it poses the information is a summary of each occurrence.

Appendix 1

Network & Perimeter security infrastructure services

Perimeter Firewalls; Palo Alto; a separate network for the management of Distributed Denial of Service (DDoS), Intrusion Prevention Service (IPS), URL Filtering and Logging.

DMZ Firewalls; Checkpoint; IPS, URL Filtering, Application Control and Logging, Private Site to site WAN network Multi-Protocol Label Switching (MPLS), (Virgin partner supplier; Intercity).

Data Centre Services and End User Compute (EUC)

Data Centre services provided BT who are ISO27001 and ISO22301 certified
Windows 7 Desktop and Laptop estate; Anti-virus, full disk encryption
Airwatch Mobile Data Manager (MDM); iPads, iPhones (OFFICIAL-SENSITIVE)
Apple employ encryption by default.

Microsoft Active Sync: Samsung Android (OFFICIAL) policy controlled.

Web Services

O365 connection from the Council utilises Transport Layer Security (TLS)/Secure Sockets Layer (SSL) certificates.

Code Enigma (ISO27001); Utilising Amazon Web services, Virtual Private Cloud (virtual FW), IPS, AV, Root Kit Hunter and TLS/SSL certificate management.
RBKC Web team manage payment services for WCC; these services are PCI-DSS compliance maintained, the team also provide TLS/SSL certificate management.
Web Hosting services are provided by Code Enigma Web who are (ISO27001 certified)

Appendix 2

Security Strategy Initiatives

1. Security Policy, Standard and Guidelines audit and update.
2. IT Security Governance.
3. Microsoft O365 Multi Factor Authentication Implementation
4. PSN re-certification.
5. Information Security Awareness Training

Initiative	Milestone	Due Date
1.	Review	
	ISO27001 policy audit	5th Jan 2018
	Report audit findings and recommendations.	12th Jan 2018
	Agree actions, identify owners	17th Jan 2018
	Update	
	Initiate program of work	22nd Jan 2018
	Reporting	Weekly
	Stake holder engagement	TBA
	Design review comms plan	TBA
	Execute Comms Plan	TBC
	Publish New Policies	April 2018
2.	Engage Stakeholders	
	Draft Security Forum Governance Terms of Reference (ToR)	12th Jan 2018
	Draft Forum Meeting Minutes Template	15th Jan 2018
	Implement Governance meetings	25th Jan 2018
3.	Complete Back out testing	12th Jan 2018
	Commence UAT	15th Jan 2018
	Complete UAT	19th Jan 2018 TBC
	Commence live deployment	5th -9th Feb 2018
4.	Commence ITHC review	10th Jan 2018
	Issue mitigations listing	17th Jan 2018
	Chair mitigations delivery workshop	19th Jan 2018
	Commence Mitigations implementation	22nd Jan 2018

	Draft PSN CoCo submission	2nd Feb 2018
	Complete Mitigations	2nd March 2018
	Collate artefacts for submission	28th Feb 2018
	Engage PSNA	TBC
	Submit application	28th March 2018
5.	Engage stakeholders	17th Jan 2018
	Review current training	26th Jan 2018
	Chair requirements workshop	5th Feb 2018
	Initiate program of work	26th Feb
	Create comms strategy	TBC
	Create implementation plan	TBA
	Complete program	April 2018

Ben Goward
Chief Information Officer

Background papers:

Email Security Incident v0.2
Unusual Account Activity Remediation process.docx **(Not for Publication)**

Contact officer: Ben Goward, CIO, Shared ICT Service, **Tel:** 02076415504, **E-mail:** bgoward@rbkc.gov.uk