	Audit and Standards Advisory Committee 7 December 2021
	Report from Strategic Director Customer & Digital Services

Cyber Security strategy implementation udpate

Wards Affected:	All
Key or Non-Key Decision:	Not applicable
Open or Part/Fully Exempt: (If exempt, please highlight relevant paragraph of Part 1, Schedule 12A of 1972 Local Government Act)	Open
No. of Appendices:	3 1. STS/Brent Cyber Security Strategy Update 2. Brent Cyber Security Strategy 3. STS Cyber Security Strategy
Background Papers:	None
Contact Officer(s): (Name, Title, Contact Details)	Sadie East, Director of Transformation Customer and Digital Services Tel: 0208 937 1507 Email: Sadie.East@brent.gov.uk

1.0 Purpose of the Report

1.1 At the last meeting of the ASAC, it was agreed that a report be brought back to the next Committee regarding the actions that the Council are taking in relation to cyber security. The report at Appendix 1 provides an update on progress in implementing the Brent and Shared Technology Service (STS) cyber security Strategies.

2.0 Detail

Brent Cyber Security Strategy

2.1 The Brent Cyber Security Strategy (BCSS) was developed and agreed by Cabinet in 2019 in response to a number of successful and high profile cyber-attacks on public and private organisations. The BCSS was developed to strengthen Brent's IT network and support the delivery of the 2019-23 Digital Strategy.

2.2 A Cyber Security Work Programme was developed as the key framework for delivering on the BCSS. The Work Programme aims to comply with the principles of the government backed scheme - Cyber Essentials - and to follow the "10 Steps to Cyber Security" framework as published by the National Cyber Security Centre in 2012.

2.3 To date, a number of Cyber Essentials recommendations have been implemented. These include;

- Strict restrictions on the use of USB storage devices and auto run is disabled
- Removing / isolating non-compliant legacy servers and other devices from the Brent network
- Implementation of One Source, a vendor/application management system

2.4 Outside of Cyber Essentials, STS has also implemented a cloud based corporate back-up solution by Rubrik to counter ransomware attacks such as the high profile attack on Hackney Council's IT Network in 2020.

2.5 The BCSS (Appendix 2) is currently being refreshed to align with to Brent's updated Digital Strategy 2022-2026 (the strategy is being presented for Cabinet agreement on 6 December 2021), and to reflect an ever changing cyber threat landscape.

2.6 The refreshed BCSS will continue to build upon the progress made on the Cyber Security Work Programme, enabling Brent to comply with the latest security standards and achieve Cyber Essentials certification by early 2022.

Shared Technology Services Cyber Security Strategy

2.7 The Shared Technology Services (STS) is an IT shared service for the councils of Brent, Lewisham and Southwark with Brent council as the host borough for the service.

2.8 The STS Cyber Security Strategy (STSCSS) (Appendix 3) is aligned to Brent's CSS. The recommendations in the strategy are embedded in all areas of new and emerging technologies which STS implement for Brent and the other boroughs in the STS.

2.9 The report provided provides an update on the work which STS is doing to support implementation of the Brent and STS Cyber Security Strategies. This includes investment in infrastructure and cyber security included in the STS Technology Roadmap, which was agreed for Brent by Cabinet in June 2021.

3.0 Risk management and audit

Risk management:

3.1 The risk of cyber attack is monitored as a key risk on Brent Council's strategic risk register. The risk is owned the Managing Director of the Shared Technology Service and mitigations include the new Rubrik backup solution referred to above.

3.2 There are a number of other activities which mitigate the risk which include:

- Multi factor authentication (MFA) has been implemented for all Office 365 access.

- Anti-Virus is in use across STS estate and pattern files are updated regularly.
- Both web filtering and mail filtering are in place for all staff.
- As well as the yearly PCN/PSI, an in depth penetration test was carried out by Dionach, an external specialist
- Annual training is mandated for all staff and phishing simulations to both staff and elected members.
- Replacement of all end-of-life mobile phones to ensure that they continue to be in support from the vendor, thus receiving security updates.
- Continual work is being conducted in making sure that versions of Windows and the applications are supported and have the latest security updates.
- Significant investments have been made in purchasing the tools needed to keep our systems safe and a forward plan for the remaining four years has been built to ensure that are able to respond to the ever changing threat landscape.
- Brent and the partnering councils in STS have a 24x7 third party Security Operations Centre monitoring any unusual activity and will disable and remove any detected threats.
- STS monitors guidance released from the National Cyber Security Centre and implements those recommendations when possible, such as a new password policy due to be communicated Q1 2022.
- A range of internal communications campaigns have taken place to raise awareness of the threat of phishing and other risks. This included a presentation at the recent Brent Tech Week.

3.3 The number of improvements made in the past twelve months has seen a reduction in cyber investigations. Progress is monitored in the quarterly Shared Service Joint Committee.

Internal audit:

3.4 On 3 November 2020, Brent Council held a cyber security workshop facilitated by Internal Audit. This was a self-assessment review of the organisation's cyber security arrangements and the demands on its security functions managed by the Shared Services and within the Council. This was timed as the organisation aimed to advance its cyber security 'deter, defend, detect' strategy. The findings of this workshop have been collated and shared and are built the work outlined in this report.

3.5 A review has been planned as part of the 2021/22 audit plan, as agreed by the Council's Audit Committee, with the objective of evaluating the design of the Council's security controls developed to prevent and detect security and data incidents given the increased reliance on technology by Council staff when working from home and the potential for emerging opportunistic threats. This review will commence in January 2022.

4.0 Financial Implications

4.1 The STS Technology Roadmap was agreed by Cabinet in June 2021. This included £10m infrastructure investment over 4 years for Brent including activities to support cyber security. Cyber Protection is one of five key themes of the roadmap.

5.0 Legal Implications

5.1 None.

6.0 Equality Implications

6.1 None.

7.0 Consultation with Ward Members and Stakeholders

7.1 The Lead Cabinet member with responsibility for ICT (the Deputy Leader) has been informed and consulted during the development of the current and refreshed Cyber Security Strategies.

7.2 The refreshed Cyber Security Strategy for 2022-26 will be presented for Cabinet for agreement in early 2022.

8.0 Human Resources/Property Implications (if appropriate)

8.1 None

Report sign off:

Report sign off:

PETER GADSDON
Strategic Director, Customer and Digital Services