| Brent | Resources and Public Realm Scrutiny Committee<br>19 July 2023<br>Report from Corporate Directors for Finance and Resources & Resident Services |
|---|---|

# Shared Service Performance & Cyber Security

| | |
|---|---|
| **Wards Affected:** | All |
| **Key or Non-Key Decision:** | N/A |
| **Open or Part/Fully Exempt:**<br>(If exempt, please highlight relevant paragraph of Part 1, Schedule 12A of 1972 Local Government Act) | Open |
| **No. of Appendices:** | Three:<br>Appendix A - Brent Cyber Security Strategy<br>Appendix B - Brent Cyber Security Strategy 2022-2026: Implementation Plan<br>Appendix C - STS Cyber Security Strategy (STSCSS) |
| **Background Papers:** | None |
| **Contact Officer(s):**<br>(Name, Title, Contact Details) | Fabio Negro<br>Managing Director of Shared Technology Services<br>Email: Fabio.Negro@sharedtechnology.services<br>Sadie East, Director of Transformation<br>Resident Services<br>Tel: 0208 937 1507<br>Email: Sadie.East@brent.gov.uk |

## 1.0 Purpose of the Report

1.1 This report provides an update on Shared Technology Services' (STS) operational performance and progress in implementing the Brent and STS cyber security strategies.

## 2.0 Shared Technology Services Operational Performance update

2.1 The ICT Shared Service was originally formed in partnership with Lewisham in April 2016 with Southwark joining the partnership a year later. The service provides the IT infrastructure (i.e. the datacentres, IT network & IT equipment) for the three Councils, on which the applications for council services and digital services can be developed and operated independently by each Council.

2.2 At the formation of the partnership, the three councils had differing IT infrastructures in various locations, and much of the early work of the shared service was to move these into the same datacentres (hosted in Brent and Croydon) and replace critical end-of-life IT hardware that often failed, resulting in IT service interruptions.

**2.3** Since the appointment of a new Managing Director in January 2020, when the

Shared Service ICT Strategy was agreed, **STS** was ready to shift focus to building a solid & stable platform, delivering value and quality service to the partner Councils **and** forging a lasting partnership between the organisations.

2.4 Delivering this original strategy required a commitment from Brent and the other partner Councils to a capital investment programme, replacing a variety of very old systems & hardware with fit-for-purpose, scalable and secure solutions, and the STS Technical Roadmap 2021-2026 was approved by Brent Cabinet in early 2021.

2.5 This investment programme is ongoing, but the progress made has benefited in significant improvements to the availability and stability of this underpinning infrastructure, resulting in far fewer issues experienced with the critical council applications that rely on a stable platform. For example, in January 2020 Brent Council was experiencing application interruptions (and therefore council service disruptions) more than 30 times on average. In the month June 2023, Brent experienced just 3 interruptions.

2.6 STS recognise that there is still more to do, including a replacement of the IT equipment issued to Brent council employees which is planned to commence later this financial year. This replacement will further improve the IT experience, stability and security by implementing modern technology.

2.7 The strong partnership with the three Councils remains, though has inevitably experienced the challenge of differing opinions. However, the model of what the shared IT service set out to provide - the foundational IT platform on which the councils can independently build on – has proven to be a lasting success, where other shared council service models have failed previously.

2.8 A new STS Strategy is being drafted in consultation with the partner Councils, which will reflect on the achievements we have made and recognise the work still to be completed. The strategy will also address our commitment to sustainability and the environment, as well as the well-being of the team.

## 3.0 Brent Cyber Security Strategy

3.0 A Cyber Security Strategy was first agreed by Cabinet in 2019 in response to high profile cyber-attacks on public and private organisations. The Brent Cyber Security Strategy 2022-2026 (BCSS) builds on this strategy and incorporates learning from cyber-attacks experienced by other local authorities (please see Appendix A & B). The central aim of this strategy is to significantly fortify the council's services against cyber-attacks, in line with the government's Cyber Security Strategy 2022-2030.

3.1 The threat of a Cyberattack on Brent Council is constant and ever-adapting, and we see attempts on a daily basis; for example, email attacks are still a primary source of concern but STS, in conjunction with our mail filtering partner, continues to be vigilant against potential malicious activity. In the period of the 90 days up to 8th of June for Brent and Lewisham councils, there were a total of 14.4 million inbound emails, of which only 5.3 million were allowed through. This work goes largely unseen, but it is critical to the protection of the Councils.

3.2 In recent months, Brent has experienced four more serious attacks, notably on the Brent website starting in December 2022 for a period of 5-6 weeks; we identified a coordinated effort to find weaknesses in the website that could have then been exploited. During this period we were able to monitor and take action to close down the threat.

3.3 So, our Cyber Security Strategy needs to be continually reviewed considering this evolving threat. For example, in 2023 we have seen a trend of attacking 3rd party suppliers to councils; four suppliers, including Capita and our IT Service system, Hornbill, have reported security breaches resulting in potential loss of data. These types of attacks potentially allow the attacker to access data pertaining to several organisations and potentially routes into our own IT systems.

3.4 In response to this new method of attack, Brent Council has instigated an internal cyber security Audit, originally scheduled for Q1 2024 but brought forward to start immediately. This audit will focus on our exposure to risk from 3rd party partners and suppliers, with the objective of evaluating the design of the Council’s security controls developed to prevent and detect security and data incidents in our supply chain, and not just on our own IT network.

3.5 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 2021.

3.6 Cyber Essentials accreditation was achieved in March 2022. The Council is working towards renewing this accreditation, with its more stringent requirements, in 2024.

3.7 Brent along with STS was selected by The Department for Leveling Up Housing and Communities (DLUHC) as a key authority to undertake a pilot for the Cyber Assessment Framework (CAF) in partnership with DLUHC and The National Cyber Security Centre (NCSC). The CAF is widely expected to become the national standard by which all public organisations are assessed.

3.8 Brent participated in the LGA’s Cyber 360 peer review, an initiative aimed at assessing and enhancing cybersecurity practices within local authorities. The council's involvement in this comprehensive review demonstrates its commitment to safeguarding sensitive data and protecting against cyber threats. The initial feedback received regarding Brent Council's cybersecurity measures has been overwhelmingly positive. The review highlighted the council's robust security protocols, proactive approach to risk management, and effective incident response procedures.

3.9 The BCSS was refreshed to align with Brent’s updated Digital Strategy 2022-2026 (the strategy was presented for Cabinet agreement on 6 December 2021), to reflect an ever-changing cyber threat landscape.

3.10 The BCSS will be refreshed in 2023 to ensure that it aligns with the Government’s new Cyber Security Strategy and will incorporate the Government’s Cyber Assessment Framework (CAF) once developed. The CAF (developed by the National Cyber Security Centre) describes 14 principles and KPI’s that organisations are expected to achieve during 2025-2030.

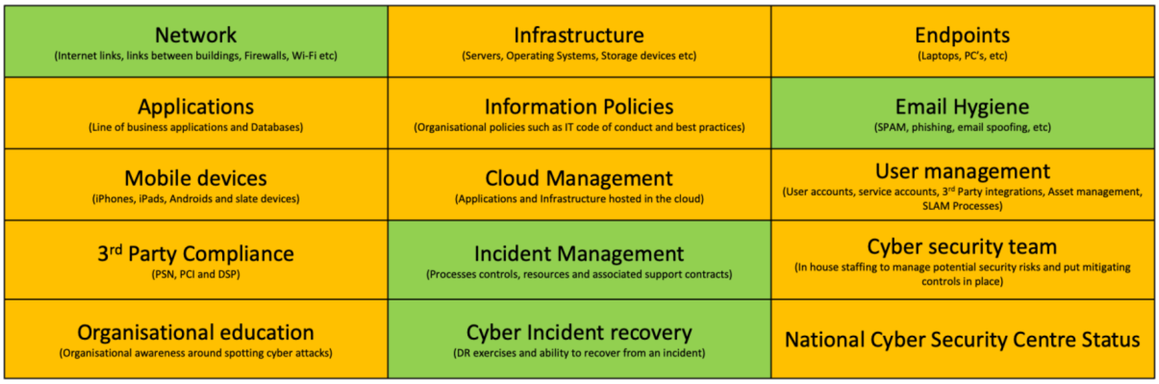
3.11 The refreshed BCSS will continue to build upon the progress made on the Cyber Security Work Programme, enabling Brent to comply with the latest security standards and successfully re-apply for Cyber Essentials certification by early 2024.

**Shared Technology Services Cyber Security Strategy**

3.12 The STS Cyber Security Strategy (STSCSS) (Appendix C) 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 partnership.

3.13 This report provides update on the work which STS is doing to support the implementation of the Brent and STS Cyber Security Strategies, which includes investment in infrastructure and cyber security included in the STS Technology Roadmap. STS are currently updating the Cyber Security Strategy to reference changes in the technical systems used by the STS Security team to identify and protect Brent from cyber-attack.

3.14 STS continues to assess our Cyber Security capabilities and posture, using a RAG status, as shown below:



| | | |
|---|---|---|
| 🟩 Network<br>(Internet links, links between buildings, Firewalls, Wi-Fi etc) | 🟨 Infrastructure<br>(Servers, Operating Systems, Storage devices etc) | 🟨 Endpoints<br>(Laptops, PC's, etc) |
| 🟨 Applications<br>(Line of business applications and Databases) | 🟨 Information Policies<br>(Organisational policies such as IT code of conduct and best practices) | 🟩 Email Hygiene<br>(SPAM, phishing, email spoofing, etc) |
| 🟨 Mobile devices<br>(iPhones, iPads, Androids and slate devices) | 🟨 Cloud Management<br>(Applications and Infrastructure hosted in the cloud) | 🟨 User management<br>(User accounts, service accounts, 3rd Party integrations, Asset management, SLAM Processes) |
| 🟨 3rd Party Compliance<br>(PSN, PCI and DSP) | 🟩 Incident Management<br>(Processes controls, resources and associated support contracts) | 🟨 Cyber security team<br>(In house staffing to manage potential security risks and put mitigating controls in place) |
| 🟨 Organisational education<br>(Organisational awareness around spotting cyber attacks) | 🟩 Cyber Incident recovery<br>(DR exercises and ability to recover from an incident) | 🟨 National Cyber Security Centre Status |

3.15 For User management, we regard this as an area we still need to improve on, and we are: The Starters, Movers and Leavers process is critical to robust user account management, and we are in the final stages of integrating HR data directly to the IT service management system, which is due to go live in August. This will ensure that we are notified of any new starters, or leavers so that accounts can be administered accordingly, and council IT assets recovered for redistribution.

3.16 In addition, we are fully enabling our hardware asset management module to record IT assets assigned to users and through the asset lifecycle.

3.17 We're also commencing a proof of value demonstration of 'just-in-time' privilege access management, whereby admin rights are only provided for a period, for the specific need. This greatly reduces the risk to the council from hacked administrator accounts.

3.18 As software exploits are discovered, suppliers release patches that need to be implemented across the applications, server and end-user device estate as quickly as possible. STS are creating a new, dedicated 'vulnerability management team who will implement these patches more rapidly, further increasing our resilience to attack.

3.19 Within the STS Cyber Security team, we have membership with LOTI's Information Governance Group for London (IGfL) and one of the team is the chair of Information Security for London (ISfL), which is London's first WARP (Warning, Advice and Reporting Point) designed to broker secure information sharing between the London boroughs.

3.20 The STS Joint Management Board will be participating in regular "table-top exercises" to run through some potential cyber incidents and our response to them, to ensure that we are prepared for this eventuality. These exercises, being coordinated with the councils' Emergency Planning teams are aimed to raise awareness and to test & learn from our ability to respond and recover from this type of event, running through the Cyber playbooks and Business Continuity plans.

## 4.0 Risk management and audit

Risk management:

4.1 The risk of cyber-attack is monitored as a key risk on Brent Council's strategic risk register. The risk is owned by the Managing Director of the Shared Technology Service and mitigations include the adoption of tools within Brent's recently procured Microsoft E5 licensing which includes endpoint protection and alert & event monitoring.

4.2 There are several other activities which mitigate the risk which include:

4.2.1. Brent has migrated to Microsoft 365 to embrace the security foundations of the product. M365 is a secure environment with robust security measures in place, like threat detection and anti-malware tools which mean security threats are identified and stopped immediately.

4.2.2. Anti-Virus is in use across STS estate and pattern files are updated regularly. Endpoint Protection on the Server estate has been recently upgraded to WithSecure's XDR (Extended Detection and Response) solution, providing a more comprehensive view of security issues on our estate.

4.2.3. Both web filtering and mail filtering are in place for all staff.

4.2.4. As well as the annual PSN/PSI scans, Brent took part in a three-month exercise with LOTI- London Office of Technology and Innovation and JumpSec to monitor and test our external attack service on the internet. This exercise highlighted issues with third parties who supply services to the council and assisted us in managing these risks.

4.2.5. Annual training is mandated for all staff and phishing simulations to both staff and elected members. To ensure transparency and informed decision-making, we present training performance updates to the corporate management team on a quarterly basis. Currently, we are in the final stages of preparing an options paper for a new Learning Management System (LMS) that will replace our existing IG training platform. This new LMS aims to enhance the learning experience for our employees, streamline training processes, improve the completion rate of all training modules and align with the evolving needs of our organisation.

4.2.6. Replacement of all end-of-life mobile phones to ensure that they continue to be in support of the vendor, thus receiving security updates.

4.2.7. Continual work is being conducted to reduce the vulnerabilities on our estate and we have been deploying tools to provide greater visibility into areas covering identity risk, data loss and phishing protection. Tools have been deployed to protect our external facing services such as Brent Website and other customer-facing services.

4.2.8. Over £330k of investment has so far been made in purchasing cyber monitoring and protection tools needed to keep our systems safe and a forward plan for the remaining three years has been built to ensure that we are able to respond to the ever-changing threat landscape.

4.2.9. We continue to learn from incidents impacting other organisations, such as Hackney Council's experience in 2020, which was subject to a ransomware attack. Brent Council, via the shared service, was one of the first London councils to invest in the implementation of an immutable backup solution which has now been in place for 2 years. This has significantly reduced the potential impact and improved our ability to recover from any similar attack.

4.2.10. 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.

4.2.11. STS monitors guidance released from the National Cyber Security Centre and implements those recommendations where applicable, such as a new password policy due to be communicated later in 2023.

4.2.12. 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 Brent Tech Week. The Councils Information Governance Team along with the STS Security team, rolled out a phishing simulator tool across the organisation.  The use of automated training has enabled us to raise awareness and vigilance across the council.

4.2.13. Brent's Data Ethics board plays a vital role in o protecting the privacy of individuals. It ensures that service areas apply the key ethical principles of fairness, privacy, transparency and accountability to Artificial Intelligence models and output can retain trust in how we as a council use data.

4.2.14. Brent Technical Design Authority governance and process is aimed at enabling early discussion with service areas to ensure that any new system requirement is secure by design. This includes the requirement for early DPIA assessments before any solution is designed.

4.2.15. Completion of a Risk flow analysis template is a prerequisite for all robotics automation processes before going live.

4.2.16. Regular yearly Penetration tests and audit checks of front-facing systems such as My Account Portal.

4.2.17. We have taken action to block some AI apps, such as ChatGPT, until such time as their security can be validated. However, Microsoft is embedding AI, branded as 'co-pilot', into Microsoft 365, which may provide real business benefits, and we will seek assurances on data security once this option has become available.

4.2.18. A refresh of the asset owner register is underway within Brent. On completion of this task all asset owners will attend mandatory training on roles and responsibilities. Brent aims to complete this action by December 2023.

4.3 Another mitigation that is being investigated is applying for Cyber Liability Insurance. Brent is now working towards obtaining a quote from insurers for this, if indeed they will quote, as the willingness of insurers to provide this type of protection has been reducing.

4.4 Brent is currently in the process of setting up a supplier security assurance framework. The framework aims to Conduct thorough due diligence with all third-party suppliers and conduct a comprehensive assessment of their security practices. Evaluate their security policies, procedures, and infrastructure. Request documentation, such as security certifications, audit reports, and vulnerability assessments, to validate their security claims.

4.5 The council conducts bespoke training sessions following data incidents to ensure that officers are well-informed about the risks and their individual responsibilities in safeguarding sensitive information. The aim of this training is to enhance officers' awareness of data security best practices, reinforce the importance of adhering to policies and procedures, and provide them with the necessary knowledge and tools to prevent future incidents. By prioritising ongoing training, the Information Governance Team are able to promote a culture of data protection awareness and accountability, ultimately reducing the likelihood of data incidents across the organisation.

4.6 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.

## 5.0 Financial Implications

5.1 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. To date, £330k has been invested in enhancing our cyber security protection and monitoring systems, with a further investment of ~£580k of investment in cyber security earmarked over the next 2-3 years.

## 6.0 Legal Implications

6.1 None.

## 7.0 Equality Implications

7.1 None.

## 8.0 Consultation with Ward Members and Stakeholders

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

***Report sign off:***

***PETER GADSDON***
Corporate Director, Resident Services

***MINESH PATEL***
Corporate Director, Finance and Resources