STS \ Brent Cyber Security Strategy Update

NOVEMBER 29 **2021**

SharedTechnology.Services

1 Version Control

Version	*Summary*	*Date*	*Editor*
0.1	Initial Draft	21/10/2021	JC
0.2	Comments	15/10/2021	SE
0.3	Amended draft	19/11/2021	RD

2 Document Approval

Version	*Date*	*Approver*
1.0	19/11/2021	SE

Contents

3 Introduction

This report sets out where STS are working to help deliver on the Brent Cyber Strategy 2019-23. STS has developed a roadmap of technologies required to deliver on business priorities. The roadmap includes items that will improve the security of Brent Council in line with the Brent Cyber Security Strategy 2019-23. This report sets out progress in delivery of these improvements under three key themes:

- Defend
- Deter
- Develop

4 Implementation Plan

4.1 Defend

Firewalls

Firewalls are in place both externally and between zones. Work is on-going as part of Cyber Essentials to ensure all rules have a business case and are documented.

Health checks

Health checks are carried out annually as part of the submission for Public Sector Network (PSN) code of connection. Web check from the National Cyber Security Centre (NCSC) is configured and in use. We further use early warning from the NCSC, which allows us to receive notifications of malicious activity and help investigate attacks on network quickly.

Compliance

Brent currently meets the requirements of the three compliance regimes they are signed up to.

- PSN next submission due June 2022.
- NHS Data Security Protection Toolkit (DSPT) next submission due June 2022
- Payment Card Industry (PCI) Compliance next quarterly scan due December 2021

Working with partners

STS is an active member of the local warning advice and reporting (WARP), Information security for London (ISfL) and Information Governance for London (IGFL).
STS is currently engaging with the London Office of Technology and Innovation (LOTI) about the viability of a central security operations centre (SOC) that can be useful to all London councils, and is one of the first tranche of organisations to be involved in this initiative.

4.2 Deter

Governance

- Applying Government's Cyber Security Guidance.

- 10 Steps to Cyber Security - see section 6
- Cyber Essentials - see section 7

Technology and Information

Network Security:
All privileged users have separate standard user accounts for web browsing and reading email. Protected using the same web filtering and mail filtering software in place for all staff.

Multi Factor Authentication (MFA):
MFA is in place for all Office 365 access, using a risked based approach. All privileged access both to Office 365 and Azure admin services requires MFA to be used.

Privileged account passwords:
Default passwords on infrastructure are all changed to non-easily guessable passwords. The length and complexity requirements for privileged accounts is set such that they are more complex than standard accounts.

Malware prevention:
Anti-Virus is in use across the estate and pattern files are updated regularly. Both web filtering and mail filtering are in place for all staff.

Removable media controls:
In general staff do not have access to USB storage devices, other than mobile phones, for access to photographs. Staff in specific areas, cleared by the Information Governance team, have access to USB storage for specific purposes.

Secure Configuration:
All devices are built from standard configurations both end use compute and server estate. Group policy is applied to ensure common security standards. There are improvements which can be applied, these are covered in Appendix A

Training and educating users:
Phishing simulations have been taking place to increase user awareness of what phishing looks like. An opportunity to take further training is afforded to those who wish to take up the option. During the last year the Phish alarm button has been deployed to everyone to make it simpler to report potential Phishing emails.

4.3 Develop

Risk Register
A corporate risk register is held by Brent. STS have a general risk register that includes digital risk, this is shared with all partners of the shared service.

Cyber Threat Levels
Vigilance is maintained by reading the weekly NCSC cyber threat reports, further evidence and advice is sought from NHS cyber alerts and through engagement with the local WARP.

Penetration testing and incident response
IT health checks are carried out every year as part of the PSN submission. This year a more in depth penetration test was carried out by Dionach with funding from the Local Government Association (LGA).

Dionach will also be providing training to STS staff to carry out some of the testing methods they used. This will enable more regular checks in specific areas to take place.

A positive that came out of the penetration test was that the host based threat detection tools on the server estate picked up the activity of the testers. This demonstrates that if this had been an actual incident we would have been able to respond in a timely manner.

Introducing training for staff and elected members
As well as the yearly training mandated for staff, more work has taken place this year on providing phishing simulations to both staff and elected members. The phishing exercises and enhanced training were provided with funding through the LGA. Working

with the Information Governance team, STS will extend the use of the phishing simulation and enhanced cyber training.

Incident response and communications

Incident response playbooks have been developed and held for specific cyber events including unauthorised access, data breach, malicious code and Distributed Denial of Service (DDOS). Within the plans there are details of external parties and partners who can be contacted for help and advice. Including LGA, NCSC, Information Commissioners Office (ICO) and providers of cyber security tools.

5 Standards

5.1 Cyber Essentials

Significant work has been taking place over the last 12 months to get to a point where Cyber Essentials can be applied for.

1) Work on the iPad and iPhone estate, to remove legacy devices.
2) Work to remove legacy windows 2008 and windows 7 devices from the estate.
3) Documenting firewall rules to ensure they are aligned with business cases.

Once points 2 and 3 are completed, Brent will be in a position to apply for Cyber Essentials in early 2022.

5.2 ISO 27001

ISO 27001 is the accepted global benchmark for demonstrating your information security management systems. Some initial investigations have taken place. We will be looking to engage with a partner who has experience in obtaining ISO 27001. Further implementation and audit training will be required for the team undertaking the task of delivering ISO 27001. Funding will be required to deliver this project with STS.

6 NCSC 10 Steps to Cyber Security

Cyber security is central to the health and resilience of any organisation reliant on digital technology to function.

The NCSC has put together the 10 steps to Cyber Security help organisations manage their cyber security risks by breaking down the task of protecting the organisation into 10 components. Adopting security measures covered by the 10 Steps reduces the likelihood of cyber-attacks occurring, and minimises the impact to Brent Council when incidents do occur.

Brent Council are following the 10 step guidance and have the following in place:-

Risk Management Regime:
Current STS digital risks fed through to Brent's corporate risk register

Secure Configuration:
Currently all server and end user compute builds are created using a standard format. Tools and techniques to ensure that configurations are maintained over time are being investigated. This could be a 3rd party tool or using Microsoft features to ensure secure configuration and minimising the attack surface.

Network Security:
Firewalls, web proxies are in place, some segmentation of the network is configured creating secure zones. Traffic between zones has to traverse a firewall.

The new Hyper Converged Infrastructure, which is about to go out to tender, allows for more separation of services by creating extra zones adding to the overall security profile.

As part of the Respond & Recover area, STS has given importance to offline backups in the case of a ransomware incident. Rubrik (new backup solution) was procured and the installation and configuration has been completed.

Managing User Privileges:
All IT admin staff have standard user accounts for day to day use and are expected to elevate access when privilege is required. All default passwords on infrastructure are changed at time of install.

User Education and Awareness:
User education has been enhanced by the use of phishing simulations. Guidance has been published on the intranet to not only guide staff at work, but also provide advice on technology at home - such as the NCSC guidance on smart devices, SMS and email fraud.

Incident Management:
Run books have been developed with more to be created to address cyber incidents. Cases are managed through the current ITSM system.

Malware Prevention:
Web filtering, mail filtering and antivirus are all in place for all colleagues. Attack surface reduction rule are being deployed across the laptop estate.

Monitoring:
Various monitoring is used across the estate, STS are also engaging with LOTI which is in the initial stages of developing a centralised security operations centre (SOC) for all London councils similar to that in use by the NHS.

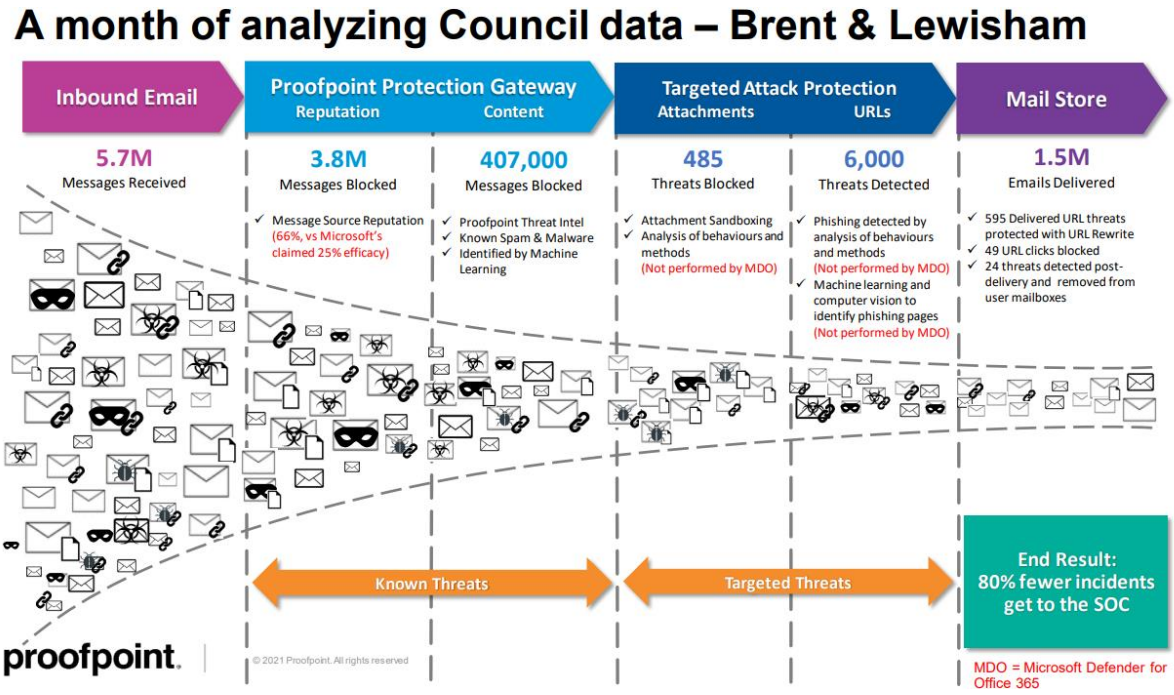
Removable Media Controls:
Most staff do not have the ability to used USB storage devices, those that do have been cleared by information governance and auto run is disabled as a security measure.

Home and Mobile Working:
Where VPN is in use and RDP, multi factor authentication is also used. The majority of staff working from home do so from securely configured Windows 10 laptops using direct access technology. The windows image used is checked as part of the annual IT health check.

7 Appendix A

Latest reports from Proofpoint and Forcepoint mail filtering and web filtering.

Proofpoint



Report covers both Brent and Lewisham for 1 month, of 5.7 Million messages sent to the council only 1.5 Million are delivered as safe.

There will still be instances of messages getting through that are not safe, this is where user vigilance and training comes in.

To assist staff in combating phishing and to make the reporting of emails a simpler process Phish Alarm a button inside exchange has been rolled out to everyone to simplify reporting.

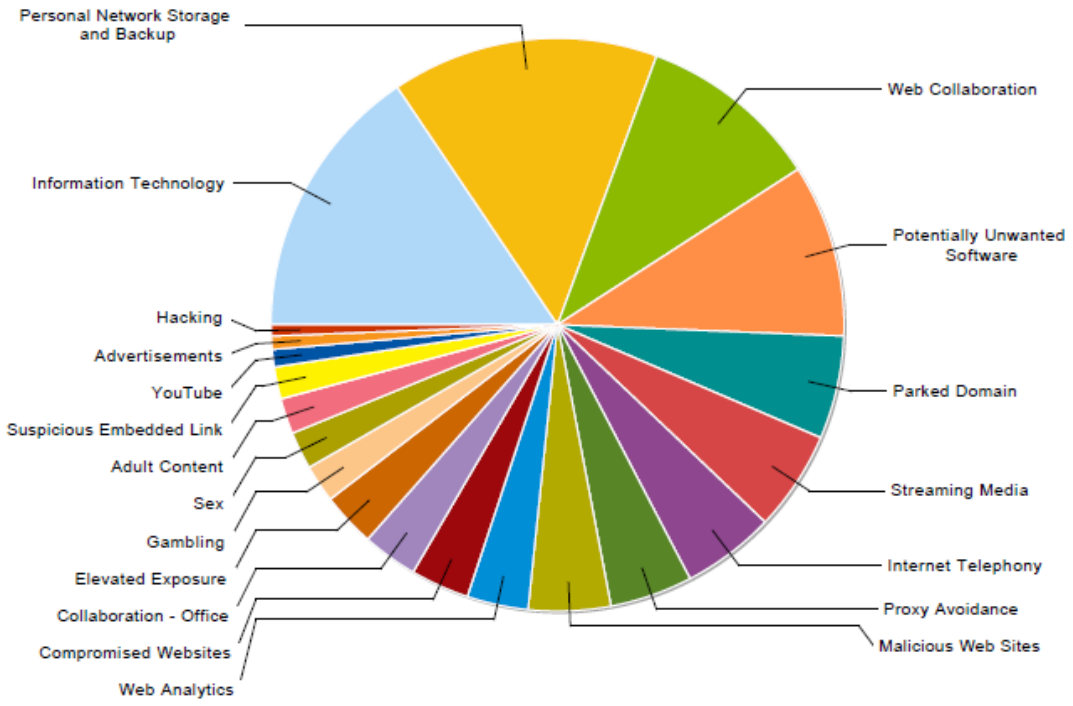
Web Filtering

FORCEPOINT
SECURITY PORTAL

Category Top 20

Date Range: **Last 1 month**

Action: *equals* **Blocked**



Forcepoint has been in place for over two years and STS a contract with them for another two years. The pie chart above shows the range of sites that are currently being blocked helping to protect the network.