APPENDIX 1

Audit, Governance and Standards Committee of Southwark council

5 February 2023

Report of Chief Digital and Technology Officer

Cyber Security Update

Wards Affected:	N/A
Key or Non-Key Decision:	N/A
Open or Part/Fully Exempt: (If exempt, please highlight relevant paragraph of Part 1, Schedule 12A of 1972 Local Government Act)	N/A
No. of Appendices:	
Background Papers:	None
Contact Officer(s): (Name, Title, Contact Details)	Dionne Lowndes Chief Digital and Technology Officer Dionne.Lowndes@southwark.gov.uk Fabio Negro Managing Director Shared Technology Services Fabio.Negro@SharedTechnology.Services

1 Purpose of the Report

1.1 This report provides an update on the Cyber Security status, threats, and mitigations in Southwark Council.

2 Recommendation(s)

2.1 The Audit Governance and Standards Committee is asked to:

1. Note the actions being taken in this report;

3 Cyber Security Strategy

Introduction

We are committed to ensure we that our systems and data are secure, and that we maintain strong relationships with partners to achieve this.

Cyber Security forms a key aspect within the Technology and Digital Strategy. The Cyber Security strategy outlines the focus we shall be adopting for our councils and customers. It is imperative that we put the right controls in place to protect and react to cyber threats going forward. We have a strong relationship with National Cyber Security Centre and other private cyber agencies which we will harness to help us to protect the data of our citizens and our customers.

Cyber incidents are on the rise, especially within public sector. We know that the ramifications are serious and widespread, from personal to economic. Protection and remediation are service disrupting and of significant financial expense. The impact on people affected by their stolen information can be life altering in some cases.

It is critical for us to put in controls around how we use, store and process our data and for us to follow the guidance from experts to ensure that our systems are appropriately secure to keep potential attackers out of our systems.

We want to continue to use the benefits of technology to improve the lives of local people. This strategy will safeguard us all. It will build confidence in the way we operate and deliver our services and keep us at the forefront of the digital revolution.

3.1 The Shared Technology Service (STS) Cyber Security Strategy (2021-2024), detailed our approach to Cyber Security, which Southwark council adopted in 2021, a refreshed version has been drafted and is with members of the shared service Joint Management Board, the strategy outlines our plans to further develop our capabilities under the following key heading from the National Cyber Security Centre (NCSC):

- DEFEND – To have the means to defend against evolving cyber threats, respond effectively to incidents, and ensure networks, data and systems are protected and resilient. It includes helping our residents, businesses, and partners in gaining the knowledge and ability to defend themselves.

- DETER - Our council will be a desirable target for all forms of aggression in cyberspace. This will involve detecting, understanding, investigating, and disrupting hostile action against us.

- DEVELOP – Including developing a coordinated and tailored approach to risks and threats that we may encounter and mitigating potential vulnerabilities.

- REACT - Ensure that we have sufficient controls in place to respond to an attack and furthermore have the organisational channels and processes to make efficient decisions further protecting our data and limiting any scope of an attacker.

3.2 This report highlights, under each of these headings, the pertinent activities and events that appraise the Audit, Governance and Standards Committee of the current threats and our mitigating actions.

4 Defend

4.1 We have had the approval to implement a Vulnerability Management Team, initially financed to the end of the financial year but with a view to making this team permanent in 2024/2025.

4.2 This team was fully recruited in October 2023 and is responsible for ensuring our entire estate is as secure as possible by implementing the hundreds, sometimes thousands of patches we receive from vendors monthly.

4.3 These patches range from the relatively low-risk minor patches to small applications, up to ‘Zero Day’ threats which are new, known and already exploited serious vulnerabilities.

4.4 Following the successful three-month pilot in 2023, Southwark are engaging with Jumpsec through the London Office of Technology and Innovation (LOTI) to carry out a yearlong engagement for their Continuous Attack Surface Mapping/Management. This engagement will employ adversarial tactics to carry out activities to discover, identify threats and carry out regular threat hunting.

Continuous Attack Surface Mapping or Management (CASM) is a cybersecurity approach focused on dynamically and continuously identifying, monitoring, and managing an organisation's digital attack surface. The attack surface refers to all the points where an unauthorised user or malicious actor could potentially exploit vulnerabilities to compromise the security of Southwark’s systems.

4.5 Southwark gained Public Services Network certification for the first time on 3 October 2024 and will continue to go through the Cyber assessment on an annual basis going forward. The Public Services Network (PSN) certification ensures that government organisations in the UK adhere to a set of security standards, enabling them to securely share information and access shared services over a standardised network.

4.6 Security Awareness Training Programme: Further development of a cybersecurity training programme is to be rolled out for Southwark staff in 2024 to educate them on best practices, recognising phishing attempts and understanding their role in maintaining a secure digital environment.

4.7 Network Upgrades: Rolling programme to upgrade and fortify the council's network infrastructure with robust firewalls, intrusion prevention systems, and networking technology with regular security audits to identify and address vulnerabilities in the network architecture. Tooley Street has been completed, with other sites to be completed in 2024 including Queens Road.

4.8 Cybersecurity Awareness Campaigns: Technology and Digital Services will be conducting ongoing awareness campaigns throughout 2024 to keep staff informed about the latest cybersecurity threats, promoting a culture of vigilance, and encouraging reporting of any suspicious activities.

5 Deter

5.1 To protect and deter attacks against public facing websites, we have deployed several services to protect these instances, such as cloud Web Access Firewalls (WAF’s). These are a central defence against the numerous attacks we have been subjected to. These measures have also been adopted with services published from the STS infrastructure, by leveraging the WAF capabilities in the recently procured F5 load balancers. Southwark have migrated a significant amount of services to the Azure cloud which has security components designed to protect web applications from various cyber threats and attacks.

5.2 To protect user identity we have deployed Multi-Factor Authorisation for all privileged accounts, using services either external or on the internal network.

Whether you're accessing services outside of Southwark (external) or systems within the network (internal), Multi-Factor Authentication ensures that even if someone somehow learns your password, they still need that second piece of information to gain access such as a code sent to your phone.

5.3 To protect against escalation of privilege in our environment, we have trailed a proof of value in the Microsoft tool, Entra permissions manager. This cloud service, monitors and reports permissions assigned in a cloud environment, advising of the best practice to ensure the least privilege and lower the attack surface of breached accounts or identities.

5.4 Following guidance from Gartner we have engaged a supplier to explore an Extended Detection and Response service for the server estate which is due to be deployed by the end of February 2024. The Extended Detection and Response (XDR) service involves deploying a solution to detect, investigate, and respond to potential security threats across the servers within the IT infrastructure. This service enhances the ability to identify and address cyber threats targeting server systems, providing a more integrated and effective approach to safeguarding digital assets and sensitive data.

5.5 We are engaging with numerous security providers to explore a managed Security Operation Centre to augment the security team, to monitor and detect security events. The business case will be available to all three councils of the shared service in February 2024.

6 Develop

6.1 The development of the Cyber Security controls is currently being progressed in to two workstreams. The first is to issue formal Security policies that following the best practice published by the National Institute of Standards and Technology (NIST) Cyber Security Framework, and the National Cyber Security Centre (NCSC). This safeguards that the policies meet the requirements set out by central government and following industry best practices. The second workstream is the onboarding and development of the Vulnerability team. The team will seek to address of legacy vulnerabilities on the estate, and ensure the estate is line with standards such as Centre for Internet Security (CIS) and Microsoft.

Attack Surface Area	Previous RAG	Current RAG	Target RAG	Actions	Target date	LBS	STS
Network	G	G	G	Network Security Policy	Complete		■
Infrastructure	A	A	G	Windows Server 2012 Replacement	Nov-24	■	■
Endpoints	A	A	G	Removable Media Policy	Complete		■
				Remote Access Policy	TBC	■	
				Future Laptop Design	Apr-24	■	■
Applications				-			
Information Policies	A	A	G	Cyber Security Policy	TBC	■	
				Data Management Policy	TBC	■	
Email Hygiene	G	G	G	Add Phishing reporting to LBL and LBS	Mar-24	■	■
Mobile devices	A	A	G	Monitor mobile replacement project	TBC		
Cloud Management	A	A	G	Azure Secure Score Action Plan	TBC		■
User management	A	A	G	Password Management Policy	TBC	■	■
				Access Control Policy	Complete		■
Compliance	A	A	G	Cyber Insurance	Jan-24	■	
				Completion of PSN Actions	Complete		■
				Schedule PCI Scan for LBS	TBC	■	■
Incident Management	G	G	G	Incident Response Policy	Complete		■
				Playbook exercise Emergency Team	LBL done	■	■
Cyber Security Team	G	G	G	Server Security Application policy	Complete		■
Organisational education	A	A	G	Policy around lost or stolen equipment	TBC	■	
				Acceptable Use Policy	TBC	■	
				Security Awareness & Training Policy	TBC	■	
Cyber Incident recovery	G	G	G	DR Test	TBC		■
National Cyber Security Centre Status	A	A	A	-	-		
3rd Party Supply Chain	R	R	A	Jumpsec reporting and remediation	Complete	■	■
				LBB Audit completion	In progress		

6.2 There is no known overarching measure for all areas of Cyber, therefore the RAG Status is the Shared Technology Service’s assessment based on feedback from several external sources such as the Public Sector Network (PSN), National Cyber Security Centre (NCSC), and Common Assessment Framework (CAF), which is a set of guidelines and principles used for assessing and managing cybersecurity risks alongside previous and current audit exercises.

6.3 Third Party Supply Chain is flagged as Red due to a lack of controls which is currently under review, LBB the London Borough of Brent’s Internal Audit team have commissioned PWC to conduct an audit review shared service 3rd party review.

Third-party suppliers pose a cyber risk to Southwark Council (or any organisation) for several reasons:

Data Access and Handling: Third-party suppliers often have access to the organisation's systems and data. If these suppliers do not have robust cybersecurity measures in place, they may become targets for cyberattacks, and any vulnerabilities in their systems could be exploited to gain unauthorised access to sensitive information.

Lack of Security Standards: Third-party suppliers may not adhere to the same cybersecurity standards and practices as the organisation they are serving. Insufficient security measures on their part could lead to vulnerabilities that cybercriminals may exploit.

Insufficient Security Audits: Organisations may not conduct thorough security audits of their third-party suppliers, or these suppliers may not have adequate cybersecurity controls in place. This lack of oversight increases the risk of security incidents.

Data Sharing and Transmission: If third-party suppliers handle or transmit sensitive data on behalf of the council, there's a risk that this data could be intercepted or compromised during these processes if proper encryption and security measures are not in place.

Human Factor: The human factor is often a significant cybersecurity risk. If employees of third-party suppliers are not adequately trained on cybersecurity best practices, they may inadvertently contribute to security incidents, such as falling victim to phishing attacks.

Regulatory Compliance: If third-party suppliers fail to comply with relevant data protection and privacy regulations, the council could face legal and regulatory consequences for any data breaches or mishandling of sensitive information.

To mitigate these risks, the Shared Technology Service and Southwark Council, need to implement thorough vendor risk management practices, conduct regular security assessments of third-party suppliers, and establish clear cybersecurity requirements in their contracts with suppliers. Regular communication and collaboration on cybersecurity best practices can help create a more secure overall environment. This is being picked up as part of the audit.

7 React

7.1 During this last period we have not experienced any serious cyber security incidents. We are improving our defences daily and we have reduced the number of vulnerabilities across the infrastructure and will continue to do so daily.

There is a commitment to continue to develop and refine the incident response plan to effectively and promptly address any cybersecurity incidents, including a designated response team, communication protocols, and continuous improvement based on lessons learned.

In December 2023 a Cyber Security recovery exercise was conducted with Children's and Adults services to ensure the service understood their role in the event of a cyber-attack. The outcomes were valuable lessons learnt and we will be conducting other exercises in 2024.

8 Future Plans

8.1 Since the last Audit, Governance and Standards Committee, we have initiated a project to design our Future Laptop design. This project will implement a modern management platform for our PC and Laptop estate, as well as update the PCs and laptops to Windows 11 the enhanced security that Microsoft's latest Operating System offers.

8.2 We will improve user experience and at the same time enhance security by implementing "Windows Hello", which is Microsoft's biometric authentication method for logging into devices, negating the reliance on keying in passwords.

8.3 A new standard of user authentication will be implemented with advice from partners such as Microsoft, Apple, and Google that removes the need for passwords entirely. This standard is called "Passkeys" and utilises Windows Hello for logging into web applications, websites etc.

8.4 The newly established Vulnerability Management Team are actively working on protecting the council against known vulnerabilities and progress of this will be reported to the Audit, Governance and Standards Committee.

8.5 We are engaging with third parties to onboard a Security Operations Centre, to leverage the security investment the partners made in their Microsoft Licensing. This is a dedicated facility that monitors, detects, responds to, and mitigates potential cybersecurity threats and incidents in real time.

8.6 We are currently reviewing the number of administration and user accounts we have in the infrastructure and putting controls in place to automate removal where possible.

REPORT ENDS