



Shared Technology
Services
Cyber Security
Strategy
2024-2026



Ciarán Weldon

Chief Information Security Officer

Shared Technology Services

I am the Chief Information Security Officer (CISO) for the shared service and have over 20 years of industry experience.

I have worked in public sector IT for over 20 years; while at Brent and subsequently in STS, I was responsible for developing the Messaging and Cloud Services for the councils. These roles provided me with insights into security from several areas and provided me with the skills to build upon my role as CISO.

As CISO for the past two years, I have sought to build and expand the service's capabilities to address the ever-evolving daily threats. I am motivated to achieve a culture of collaboration within the service and with our partners. Ensuring we provide the best security to our staff and residents.

This renewed Cyber Strategy reflects the development of our Cyber Security service under my leadership. It paves the path for continued growth in deploying controls and policies, aligning the service with the NCSC strategic tenants of Defend, Deter and Develop. The foundation of the strategy is that Cyber Security is everyone's responsibility, and we are working in partnership with the councils to adopt this awareness.

Since the conception of the shared service, I have noticed a significant change in the threat landscape, with attacks becoming more targeted and sophisticated. Adaption of navigating the compliance requirements and regulatory standards specific to the UK government and, more importantly, keeping data secure and protecting residents needs to be continuous. This Cyber Strategy reflects the change in STS cyber posture and gives us the vision to protect councils and data by being more agile and reactive to adversaries.

Cyber Security is everyone's responsibility.

1. Introduction

Shared Technology Services (STS) is an IT shared service for the Brent, Lewisham, and Southwark councils.

Brent Council is the host borough for the service. STS is governed by an Inter Authority Agreement between the three councils and a Joint Committee of two members from each council and the Executive Directors.

This document sets out the STS application of information and cyber security standards to protect our systems, the data held on them and the services we provide from unauthorised access, harm, or misuse.

Our cyber security commitment is to the residents of the three partner councils. It emphasises the importance of cyber security in the role of all staff.



2. The Challenge

Cybersecurity is a critical concern for local governments to protect sensitive information, critical infrastructure and essential services.

We have seen with increasing frequency how organisations can be impacted by cyber-attacks and the reputational damage that can follow.

For STS, the risk is threefold, as each council is subject to threat. Our original STS Cyber Security Strategy 2021-2024 outlined our approach of a continual cycle for protecting the councils and their customers from cyber-attacks, which remains our strategy for the next three years:

By implementing this revised, comprehensive cybersecurity strategy, STS can enhance cyber resilience, protect sensitive information and ensure the continued delivery of essential services to the community. Regular reviews and updates to the strategy ensure its effectiveness against evolving cyber threats.

The real challenge comes when an organisation needs to encourage more collaboration, access to information, and transformation. Very often, the rules around responsible data management stifle the ability to share. One of the most challenging jobs in this area is to balance and enable transformation effectively and continue the responsible use of data that we are accountable for.

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

This Cyber Security strategy outlines the focus STS shall be adopting for our councils and customers. It is imperative that the right controls are put in place to protect and react to cyber threats going forward. STS have a strong relationship with the National Cyber Security Centre and other private cyber agencies which will harness to help protect the data of both citizens and customers.

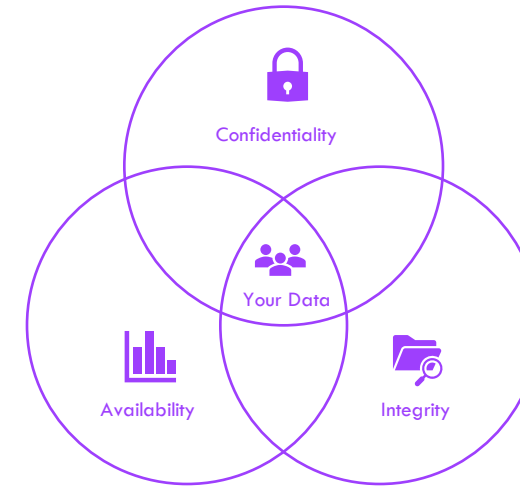
3. Why is cyber security important?

Cyber security is the practice of ensuring the confidentiality, integrity and availability (CIA) of information.

- **Attacks on Confidentiality** – stealing, or rather copying personal information.
- **Attacks on Integrity** – seeks to corrupt, damage or destroy information or systems and the people who rely on them.
- **Attacks on Availability** – denial of services, seen as ransomware.

Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorised access. Cyber security may also be referred to as information technology security.

Cyber security is important to effectively deliver services. Data is processed and stored in large amounts on computers and other devices. A significant portion of this data is sensitive information. It includes financial data, personal information and other types of data for which unauthorised access or exposure could have negative consequences.



Sensitive data is transmitted across networks and to other devices, whilst providing services or even just using the mobile to look at social media. Cyber security is the discipline dedicated to protecting this information and the systems used to process or store it. It is everyone's responsibility to ensure that we manage our data appropriately.

Cyber security is crucial in ensuring services are kept up and running. It is also vital in ensuring building and keeping the public's trust. A cyber-attack would have very serious consequences in terms of a disruption to services (many of which serve some of the most vulnerable residents), council's reputation and the impact to fiscal position.

4. Purpose and Scope

STS seeks to enable its partners to deliver its corporate and digital strategies; it is required that we allow our organisations to navigate cyber obstacles. The scale of transformation represents an unprecedented culture shift for staff, residents, partners and businesses. This in turn, creates risk.

The Cyber Security Strategy update introduces a response to several successful and high-profile cyber-attacks on public and private organisations. The purpose of the strategy is to give assurance to our councils and customers and to explain our commitment in delivering robust information security measures.

Through delivery of this strategy, STS will comply with and embed the principles of the Cyber Assessment Framework; a government-backed, industry-supported scheme to help organisations protect themselves against common online threats.

This strategy is intended to cover all partners and customers, with the data on the systems an STS responsibility, along with the services they help provide. The recommendations in this strategy will be embedded in all areas of new and emerging technologies which STS implement. It will also set out the best practices that will be rooted in business as usual.





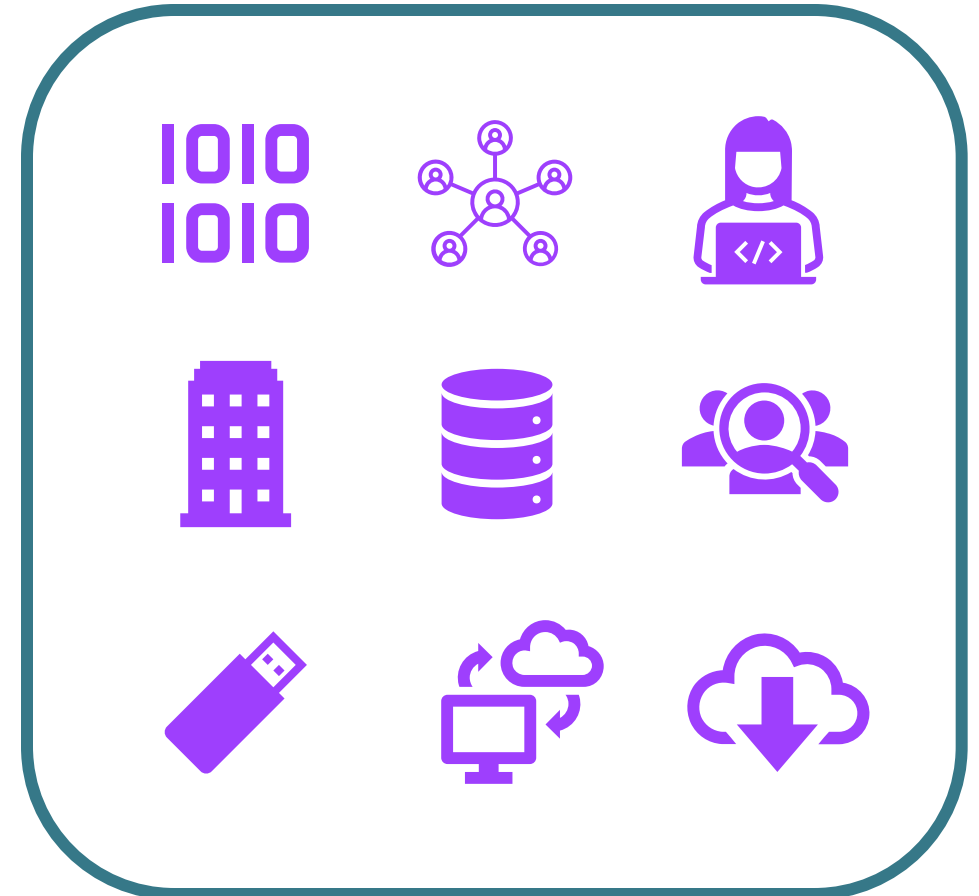
Figure 2 - The building blocks of Cyber Security

5. Assets

STS will regularly review the value of all assets across the partnership, ensure that political, social and economic values are considered to place the appropriate levels of protection around those digital and physical assets.

Our assets:

- Data
- Services
- Infrastructure

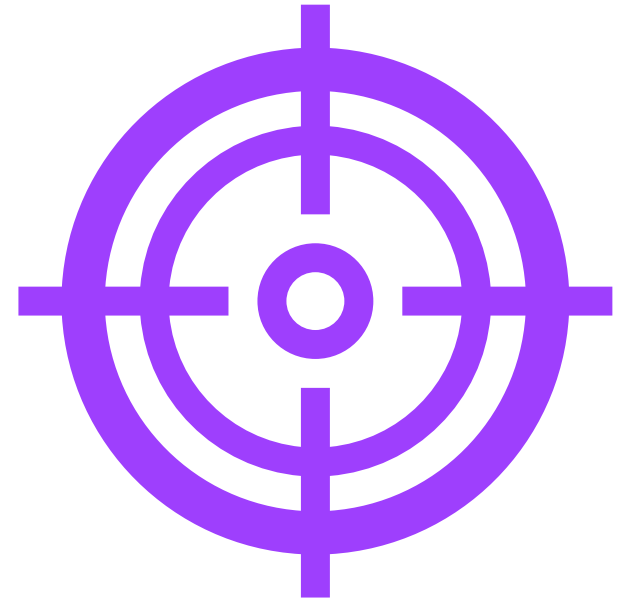


6. Vulnerabilities

Vulnerabilities are weaknesses or other conditions in an organisation that a threat actor, such as a hacker, nation-state, disgruntled employee, or other attacker, can exploit to affect data security adversely.

Cyber vulnerabilities typically include a subset of those weaknesses and focus on issues in an organisation's IT software, hardware, systems.

- **System Maintenance** – IT systems should be updated and checked regularly and effectively. It is essential that the systems are fully updated and appropriate fixes are applied. Poor setup, mismanagement or other issues in how an organisation installs and maintains its IT hardware and software components are threats.
- **Legacy Software** – To ensure that legacy systems have sufficient user and system authentication, data authenticity verification, or data integrity checking features that prevent uncontrolled system access.
- **Trend Analysis** - Monitoring organisational working patterns to identify unusual behaviour and respond accordingly.
- **Training and Skills** – It is paramount that all employees have a fundamental awareness of cyber security to support this.

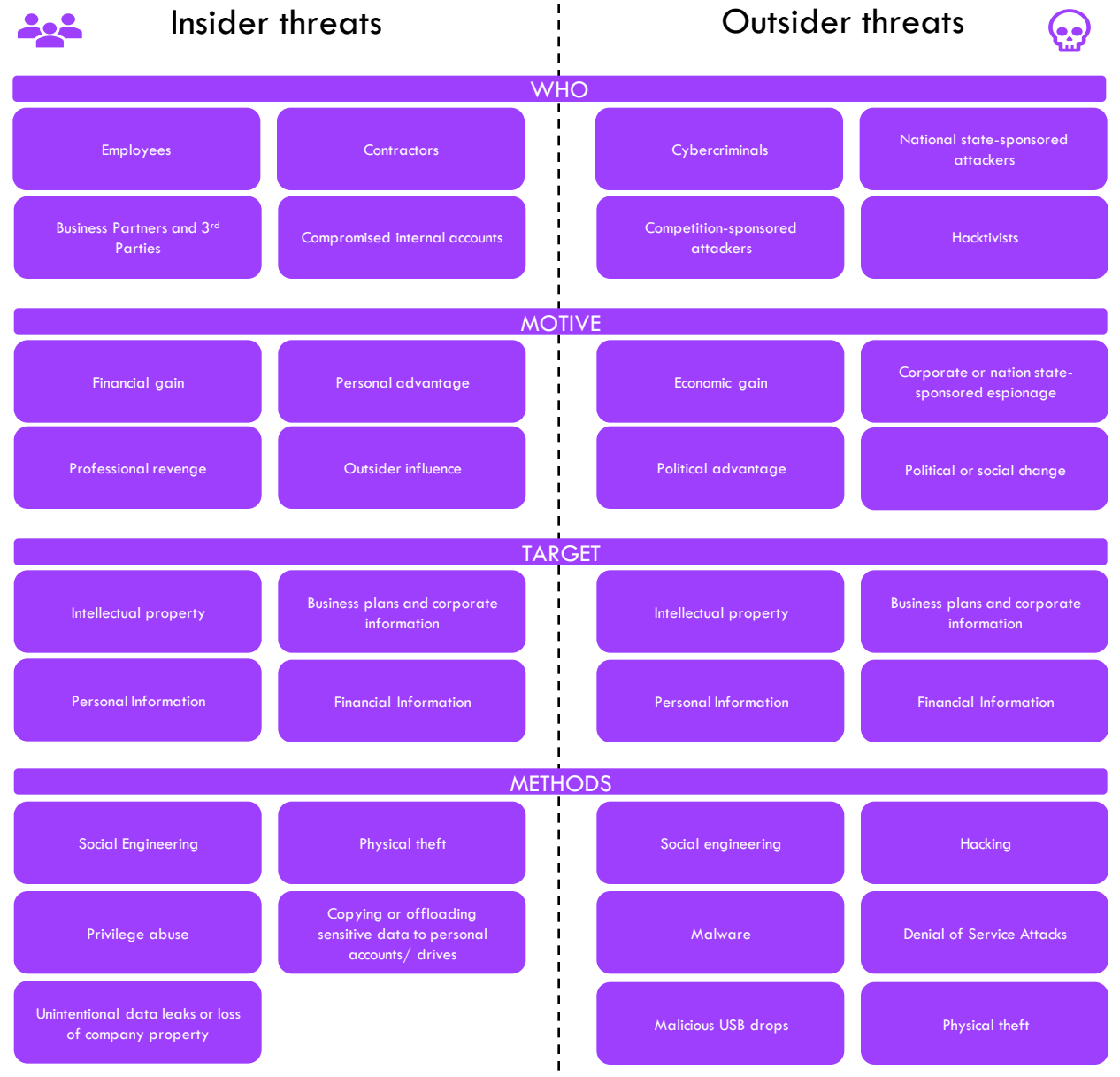


7. Threats

If left unchecked, a threat could disrupt the day-to-day operations and the delivery of local public services and ultimately have the potential to compromise national security.

Generally, there are two types of threats Insider Threats and Outsider Threats.

These threats are explained in detail in the chart to the right.



Cyber Criminals

Generally, cybercriminals are working for financial gain. Most commonly, for the purposes of fraud either by selling illegally gained information to a third party or using directly for criminal means.

Key tools and methods used by cybercriminals include:

- **Malware** – malicious software that includes viruses, Trojans, worms or any code or content that could have an adverse impact on organisations or individuals
- **Ransomware** – a kind of malware that locks victims out of their data or systems and only allows access once money is paid
- **Phishing** – emails purporting to come from a public agency to extract sensitive information from members of the public.

Hactivism

Hactivists will generally take over public websites or social media accounts to raise the profile of a particular cause.

When targeted against local government websites and networks, these attacks can cause local reputational damage. If cyber-attacks regularly disrupt online services, this could erode public confidence in such services.

Hactivist groups have successfully used distributed denial of service attacks to disrupt the websites of several councils to date. (DDoS attacks are when a system, service or network is burdened to such an extent by an electronic attack that it becomes unavailable).

Insiders

Staff may intentionally or unintentionally release sensitive information or data into the public domain. This could be for the purpose of sabotage or to sell to another party, but oftenly it is due to simple human error or a lack of awareness about the particular risks involved.

Malicious insider threats may include privileged administrative groups.

Zero Day Threats

A zero-day exploit is a cyber-attack that occurs on the same day or before software weaknesses are discovered. At that point, it's exploited before its creator makes a fix available. It is an attack that exploits a previously unknown security vulnerability.

This poses a risk to any computer or system that has not had the relevant patch applied or the relevant updates to its antivirus software.

Physical Threats

The increasing reliance on digital services increases vulnerability in the event of a fire, flood, power failure or other disaster (natural or otherwise).

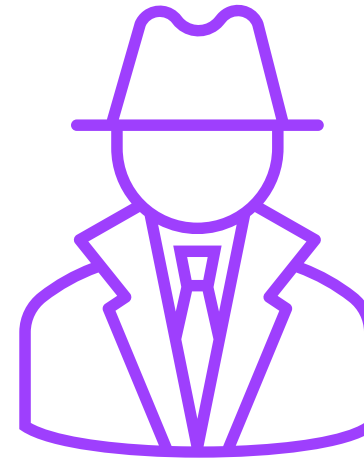
Terrorist

Some terrorist groups demonstrate intent to conduct cyber-attacks, but fortunately have limited technical capability.

Terrorist groups could obtain improved capability in several ways, namely through the sharing of expertise in online forums providing a significant opportunity for terrorists to escalate their capability.

Espionage

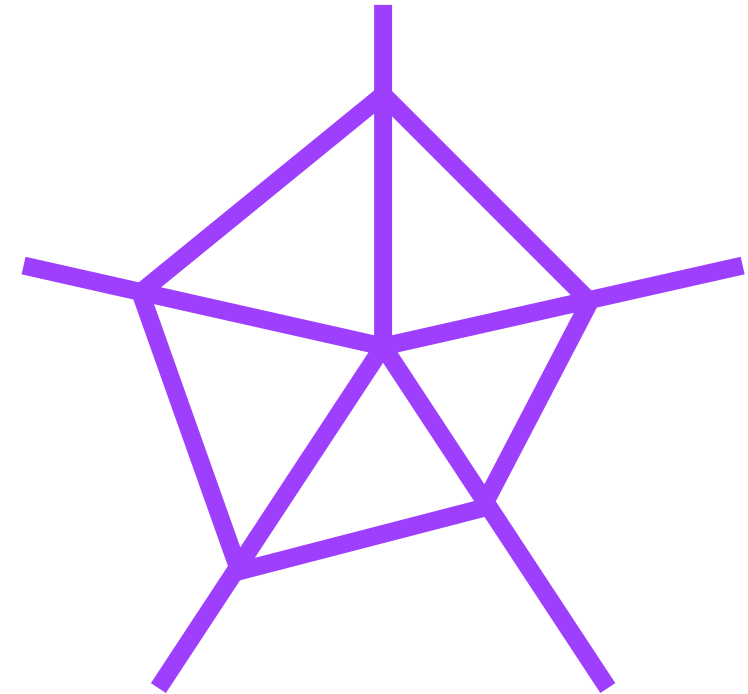
Several of the most sophisticated and hostile foreign intelligence agencies target UK government and public sector networks to steal sensitive information. This could ultimately disadvantage the UK in diplomatic, trade or military negotiations.



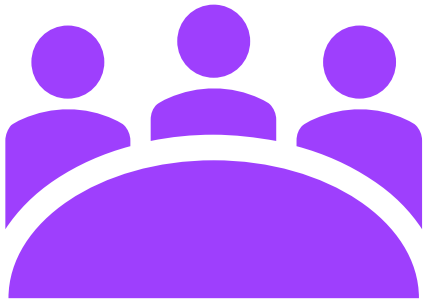
8. Risks

Cyber Risk Management is a fundamental part of the broader risk management to ensure cyber security challenges are fully identified across the councils and appropriate action is carried out to mitigate the risk but also develop effective recovery and containment procedures in the event of an incident.

A risk consists of a threat and a vulnerability of an asset. We conduct regular thorough risk assessments to identify potential vulnerabilities and threats specific to the local government's systems, networks and data. Regularly updating our assessments to stay current with evolving threats.



8. Our Approach



To mitigate the multiple threats, it is vital to face and safeguard interests, a strategic approach that underpins the collective and individual actions in the digital domain over the next three years is required. This will include:

- Collaborate with the other technical and governance teams in the councils to ensure there is a cohesive approach to cyber security.
- Foster a culture of empowerment, accountability, and continuous improvement.
- Prioritising information assets and processes with councils and customers, maintaining a register and conducting regular reviews including data retention policies.
- Ensuring adequate plans are in place to recover and quickly identify exposure.
- A council-wide risk management framework to help build a risk aware culture within each of the councils, ensuring staff understand how to identify and manage risks.
- Cyber Awareness training and principles to help mitigate insider threats, understand supply chain risks, and ensure all staff understand the issues and their responsibilities.

To further enhance the maturity and capability of the service STS have enhanced the Cyber Security team within the Shared Service to take on responsibility for patch management and remediation plans. STS's ability to rapidly and efficiently manage this will help to further reduce the risk to data; many of the more publicised incidents have been as a direct result of utilising where known weaknesses have not been patched in a timely manner.

The STS strategy also includes the initiation of a 24x7x365 Security Operations Centre service, via a 3rd party, to continuously detect and respond to attacks in real time; whilst having a limited service already for the server estate, the threat of attack is a global phenomenon, and therefore being always prepared and ready is a must.

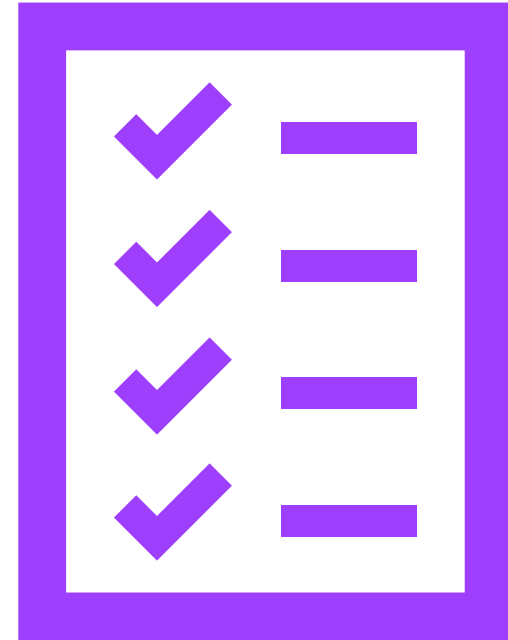
9. Plan

By aligning with the National Cyber Security Strategy's approach to defend our, residents, councils and customers and deter our adversaries and to develop our capabilities STS will adapt to the changing landscape and achieve our vision.

It was recognised that each partner and council will be at different levels of maturity and capacity therefore STS developed a 3-year (2024-2026) Technology Roadmap which has already resulted in investment in a significant number of cyber protections.

The 'Cyber RAG status' to assess our maturity in all areas has since been developed.

The STS implementation plan will recognise areas of improvement and put in place activities to address these, some of which will be a sovereign partner task, such as policy development. This will be an ongoing improvement plan.



10. Detect

The preemptive detection of potential cyber events is the foundation of the strategy. Through the following stages:

Asset Management: Identify all the assets within the network, including hardware, software, and data repositories.

Baseline Establishment: Establish a baseline for the regular activity on the network, systems and users by introducing agents to monitor the network to greater effect.

Threat Intelligence: Using threat intelligence feeds and courses to understand the threats to our network and prepare defenses.

Anomaly Detection: Deploying agents to understand and detect deviations from normal behavior and the capability to respond to these detections.

Continuous Monitoring: Automated monitoring tooling continuously monitors network alerts and suspicious behaviours.

Incident Response: Develop and implement incident response plans and carry out tabletop exercises to outline the process and procedures to contain, mitigate damage and return services to normal operations.

	2024				2025				2026			
	1st Q.	2nd Q.	3rd Q.	4th Q.	1st Q.	2nd Q.	3rd Q.	4th Q.	1st Q.	2nd Q.	3rd Q.	4th Q.
Vulnerability management	●	●	●	●	●	●	●	●	●	●	●	●
SOC Enrichment	●	●	●	●	●	●	●	●	●	●	●	●
Continuous Penetration scanning	●	●	●	●	●	●	●	●	●	●	●	●
Review of out-date or in support applications	●	●	●	●	●	●	●	●	●	●	●	●
Enhancing Endpoint protection	●	●	●	●	●	●	●	●	●	●	●	●
Results												

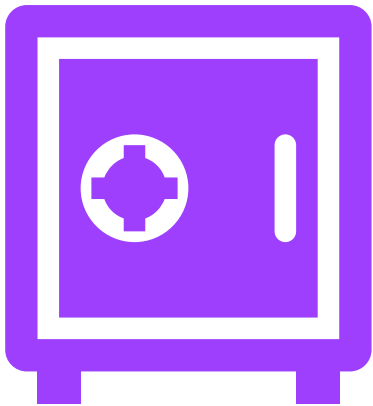
● Detect







11. Defend

STS will have the means to defend against evolving cyber threats, to respond effectively to incidents, and to 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.

Actions:

- Implementing daily firewalls and scanning services.
- Continue to monitor email hygiene for all partners and enable Attack Targeted Prevention.
- Improve threat correlation and reporting services.
- Ensure vulnerability and patch management is kept up to date.
- Ensuring that Cyber Security is considered in any procurement of solutions, to provide assurance on 3rd party supply chain risk.
- Work with councils and customers to ensure websites and line of business systems are kept secure.
- Enhance our 3rd party Security Operations Centre service with a partner to give us the assurance and protection of our systems, using dynamic and Artificial Intelligence (AI) from across the global to identify immediate threats.
- Carrying out health checks, penetration test and cyber resilience exercises to test their systems and processes.
- Identify an STS Red team to be able to respond to incidents and have relationships in place with government agencies and cyber specialists.
- Assuring our DR plan by carrying out regular backups and recovery exercises.
- Meeting compliance regimes, Code of Connection (CoCo) which require good cyber hygiene, to connect to government private networks, e.g. Public Sector Network (PSN) and the Health and Social Care Network.
- Working with partners across the public sector through participation in Cyber Security Information Sharing Partnership (CiSP), Warning, Advice and Reporting (WARPs) and participating in Cyber resilience exercises with LOTI.
- Work towards ISO27001



	2024				2025				2026			
	1st Q.	2nd Q.	3rd Q.	4th Q.	1st Q.	2nd Q.	3rd Q.	4th Q.	1st Q.	2nd Q.	3rd Q.	4th Q.
BCP and DR exercises												
Attack Surface Reduction												
Results												

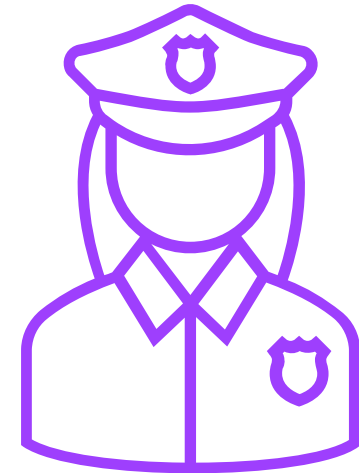
 Defend

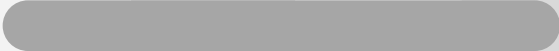
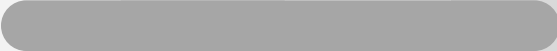
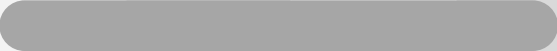
12. Deter

STS partner councils and customers will be a desirable target for all forms of aggression in cyberspace. This will involve detecting, understanding, investigating, and disrupting hostile action against us.

Actions:

- Applying government's cyber security guidance, e.g. 10 Steps to Cyber Security or Cyber Essentials.
- Users with wide ranging or extensive system privilege shall not use their highly privileged accounts for high-risk functions, in particular reading email and web browsing.
- Multi-factor authentication shall be used where technically possible, such as where administrative consoles provide access to manage cloud infrastructure, platforms or services. Multi - factor authentication shall be used for access to enterprise level social media accounts.
- Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and shall not be easy to guess. Passwords which would on their own grant extensive system access, should have high complexity and introduce multi-factor authentication.
- Use of Malware prevention and ensure air gaps or immutable storage.
- Ensure removable media is encrypted to the latest levels controls.
- Improve micro segmentation of the network to avoid attackers crossing the network.
- Secure configuration to avoid access to critical information and enabling attackers.
- Introduce cyber awareness and training for users to help detect, deter, and defend against the cyber threats.
- Enhancing our Security Operations Centre (SOC).



	2024				2025				2026			
	1 st Q.	2 nd Q.	3 rd Q.	4 th Q.	1 st Q.	2 nd Q.	3 rd Q.	4 th Q.	1 st Q.	2 nd Q.	3 rd Q.	4 th Q.
Resilience testing												
Enforce Security Policies												
Adoption of Cyber Framework												
Results												

 Deter

13. Develop

This includes developing a coordinated and tailored approach to risks and threats that we may encounter and mitigate potential vulnerabilities.










Actions:

- Develop and maintain risk management framework, internal control and governance for the prevention and detection of irregularities and fraud.
- Develop and enforce comprehensive cybersecurity policies and procedures that cover areas such as data handling, access control, incident response, remote work, and third-party vendor management. Ensure that employees and stakeholders are educated about these policies.
- Process, procedures, and controls to manage changes in cyber threat level and vulnerabilities.
- Managing vulnerabilities that may allow an attacker to gain access to critical systems.
- Operation of the council's penetration testing programme and Cyber-incident response
- Regularly train all staff and Councillors on cybersecurity best practices, social engineering awareness, and safe online behaviour. Conduct simulated phishing exercises to gauge the effectiveness of training and to identify areas for improvement.
- Regularly test and review our incident response and management plan, with clearly defined actions, roles, and responsibilities.
- Update our incident response and management plan to develop a detailed incident response plan that outlines the steps to be taken in the event of a cyber incident. This plan will cover identification, containment, eradication, recovery, and lessons learned. Regularly test and update the plan through simulated exercises.
- Develop a communication plan in the event of an incident which includes notifying (for example) the relevant supervisory body, senior accountable individuals, the Departmental press office, the National Cyber Security Centre (NCSC), Government Security Group (Cabinet Office), the Information Commissioner's Office (ICO) or law enforcement as applicable (not exhaustive)
- Assess the cybersecurity posture of third-party vendors and contractors that have access to the local government's systems and data. Ensure that they meet our cybersecurity standards and follow secure practices.
- Develop a network of sharing with other councils and customers, collaborate and learn from each other, harness networks such as London Office of Technology and Innovation, London CIO council, WARP, IGfL and ISfL.



	2024				2025				2026			
	1st Q.	2nd Q.	3rd Q.	4th Q.	1st Q.	2nd Q.	3rd Q.	4th Q.	1st Q.	2nd Q.	3rd Q.	4th Q.
Technical staff development	Develop				Develop				Develop			
Continuous Penetration scanning	Develop				Develop				Develop			
Introduction of security by design			Develop		Develop				Develop			
Process, Policy, Risk and Issues and RACI review		Develop		Develop		Develop		Develop		Develop		Develop
Results												

 Develop

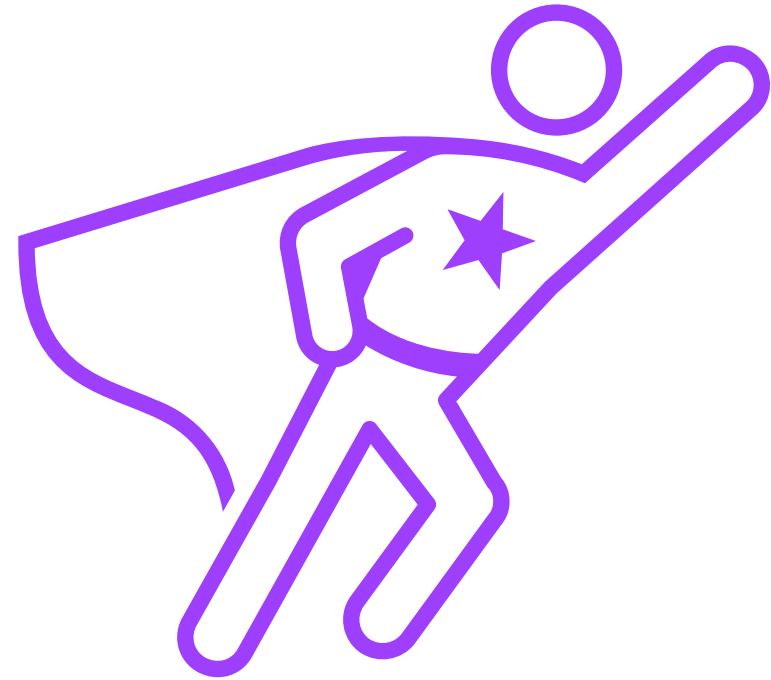
	2024				2025				2026			
	1st Q.	2nd Q.	3rd Q.	4th Q.	1st Q.	2nd Q.	3rd Q.	4th Q.	1st Q.	2nd Q.	3rd Q.	4th Q.
Review of infrastructure baselines												
Introduction of Software-Defined Network												
Win11 Laptop Refresh (NCSC Templates)												
Results												

 Develop

14. React

STS will ensure that sufficient controls are 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.

STS have third parties proactively monitoring our environment disabling any potential threats and locking down resources which are identified as a risk, which we will further enhance with a Security Operations Centre (SOC) service.



	2024				2025				2026			
	1st Q.	2nd Q.	3rd Q.	4th Q.	1st Q.	2nd Q.	3rd Q.	4th Q.	1st Q.	2nd Q.	3rd Q.	4th Q.
Cyber Insurance	[Bar]				[Bar]				[Bar]			
Cyber Assessment Framework April 24			[Bar]		[Bar]				[Bar]			
Public Services Network compliance	[Bar]				[Bar]				[Bar]			
Payment Card Industry compliance	[Bar]				[Bar]				[Bar]			
NHS DSPT Toolkit	[Bar]				[Bar]				[Bar]			
Results												

 React

1.5. Success Factors

Throughout this period of challenging transformation, the councils have committed to delivering robust information security measures to protect our data from misuse and cyber threats, and to safeguard their privacy through increasingly secure and modern information governance and data sharing arrangements both internally and with partners.

To continue to provide assurance on the effectiveness and robustness of STS's arrangements for IT security, we will:

- Develop appropriate cyber security governance processes.
- Develop a Cyber Risk Management Framework
- Develop policies/procedures to review access on a regular basis.
- Create a cyber-specific Business Continuity Management Plan and/or Incident Plan to include emergency planning for cyber-attack.
- Develop an incident response and management plan, with clearly defined actions, roles, and responsibilities. A copy of all incidents shall be recorded regardless of the need to report them.
- Set up a Playbook to have test incidents on a regular basis; to ensure reaction to incidents where an incident is triggered.
- Create standard test plans with security testing as a standard.
- Reconcile current systems in place and last times these were reviewed (build into Enterprise Architecture)
- Review vendor management – process of assessments of third parties
- Explore Active Cyber Defence tools and new technologies to ensure partners have the best solutions to match to threats.
- Apply the governments cyber security guidance – 10 Steps to Cyber Security
- Provide relevant cyber security training for staff and elected members.
- Apply a regular schedule of cyber exercises, within the wider cycle of multi-agency incident response and recovery exercises.
- Comply with the Governments Public Sector Network (PSN) Code of Connection and Payment Card Industry (PCI) standards; a minimum requirement for all systems used, audit trails, deletion of data etc.
- Protect enterprise technology by working with specialist partners to develop model architecture and review audit logs to reduce chances of threats.



16. Roles and Responsibilities

Information Governance and Policy will remain the councils' responsibility, and the Shared Service will work with those teams to ensure that shared understanding and collaboration is met. Effective cyber security governance in STS is delivered through the following roles and functions:

Senior Information Risk Owner (SIRO)

A nominated Senior Information Risk Owner (SIRO) is responsible for the governance of cyber security and information risk within the Council. This includes ensuring that information governance risk is managed in accordance with GDPR.

However, whilst the SIRO is the nominated officer, responsibility for safeguarding information and information systems is shared across the organisation with all staff having a role to play.

Joint Committee (JC)

The Joint Committee is made up of the lead councillors for IT. The Joint Committee will sponsor the Cyber Security Strategy and oversee the strategic framework through which the council governs its information resources and in turn agree and receive updates on implementation of the Cyber Security Strategy.

Joint Management Board (JMB)

The Joint Management Board is responsible for the strategic direction of the shared service and is made up of the executive directors from each council and the Managing Director of the shared service. This board is responsible for holding the shared service to account on the delivery of its obligations in turn the protection of its data and systems.

Operational Management Group (OMG)

The Operational Management Group is responsible for the day-to-day tracking of tasks and deliverables, this board will allocate resources and funds necessary to deliver the protection to the councils and its customers. The board is made up of Heads of IT from each council and the Senior Leadership Team of the shared service.

STS Security Forum

The STS Security Forum is comprised of Information Security leads from each of the councils and the STS CISO, where they will discuss all technical controls, policy and process.

Information Governance Group (IGG)

The IGG is comprised of senior representatives from each council area. The group are responsible for overseeing the delivery of the Cyber Security Strategy and monitoring its effectiveness.

Technical Design Authority (TDA)

The Technical Design Authority (TDA) make decisions regarding technical implementations for projects. This includes ensuring that cyber security implications are properly considered.

All council officers and Members

It is the responsibility of all officers and council Members to comply with the standards set out in this Cyber Security Strategy