Brent Cyber Security Strategy

2022 to 2026

Brent

Contents

Brent Cyber Security Strategy
2022 to 2026

Foreword

With an increasing reliance on information and digital solutions, Brent Council, like other public organisations, faces a higher risk from potential cyber threats. The council's Cyber Security Strategy works alongside its Digital Strategy 2022-26, to support the council, meet the borough's objectives and safeguard our residents' and stakeholders' information.

This Cyber Security Strategy 2022-26 demonstrates Brent's commitment to continually develop, improve and strengthen our digital technology and services.

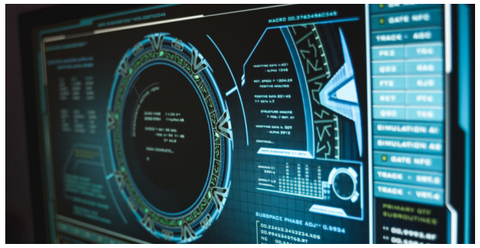
Our reputation for security has become even more significant in this growing digital age. With the increasing use of our online services during the pandemic and a sharp increase in remote working and use of devices, we have continued to plan, adapt and support our service users accordingly. As demand for digital services increases, we need to ensure that Brent continues to transform and adapt its services into ever more efficient, digital ways of working. This is a key aim of our new Digital Strategy.

This strategy sets out how Brent will mitigate against, and respond to, online risks including phishing, malware and ransomware. We know that cyber attacks will continue to evolve, which is why the public and private sectors must continue to work at pace to deliver real-world innovations and outcomes to reduce the threat to Brent's critical services and to deter would-be attackers.

We must ensure that our digital services to businesses and the public are as safe, secure and reliable as possible, and this strategy will help Brent to achieve this.

Councillor Margaret McLennan, Deputy Leader of the Council and Lead Member for Resources and interim lead for Children's Safeguarding, Early Help and Social Care

Introduction



This document sets out the council's strategy for cyber security, to significantly strengthen our services against cyber attack, in line with the Government Cyber Security Strategy 2022-2030.

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 in the form of ransomware.

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

Cyber security is important because Brent Council collects, processes, and stores significant amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorised access or exposure could have negative consequences.

Brent Council transmits sensitive data across networks and to other devices in the course of doing businesses. This Cyber Security Strategy describes the discipline dedicated to protecting that information and the systems used to process or store it.

A robust cyber security strategy is crucial for ensuring services are kept up and running, and also for maintaining public trust in the council's ability to safeguard their information and provide them with the confidence to transact with the council online. A cyber attack could have very serious consequences for the council. This could include disruption to vital services (many of which serve the most vulnerable), and a significant financial impact, as well as damaging the council's reputation.

Brent Council's overarching vision in the Brent Borough Plan – Building a Better Brent 2019-2023 "is to make Brent a borough of culture, empathy, and shared prosperity." Achieving our vision will therefore require innovation, continued and deeper partnership, and careful planning based on sound evidence. This strategy complements this, as we are at the forefront of a digital revolution, which is transforming how people interact and their expectations for accessing information and services. With the increasing volumes of personal data being processed, there is a greater need to protect it. Therefore, this Cyber Security Strategy is key to the efficient and productive running of Brent Council.

Brent Cyber Security Strategy 2022 to 2026

Purpose

The council seeks to deliver its Digital Strategy through transforming Brent into a digital place and a digital council. The scale of transformation set out in the Digital Strategy represents an unprecedented culture shift for the council, residents, partners and businesses.

The new Cyber Security Strategy builds upon the work of the previous 2019-23 strategy and also incorporates lessons learnt from high profile cyber incidents experienced by other local authorities. The purpose of the updated strategy is to give assurance to residents, and other stakeholders, that the council is committed in delivering robust information security measures to protect residents' and stakeholders' data from misuse and cyber threats and to safeguard their privacy through increasingly secure and innovative information governance and data sharing arrangements both internally and with partners.

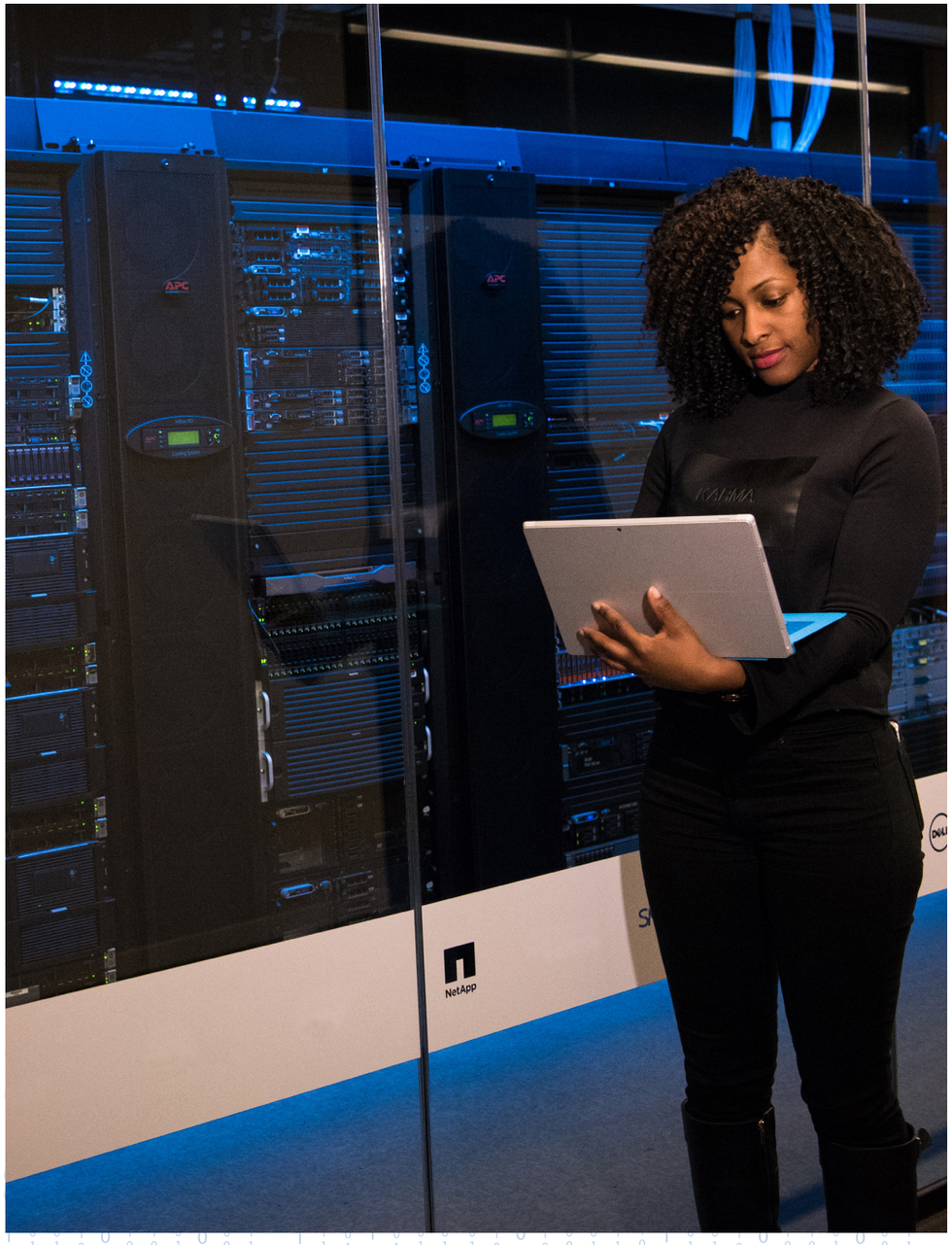
The Cyber Security Strategy sits alongside the Digital Strategy 2022-26, Shared Technology Services (STS) Roadmap, STS Cyber Security Strategy and Data Management Strategy, supported by a suite of operational policies (Information Security Policy, Information Risk Policy and Access to Information Rule Book).

Since the launch of the previous Cyber Security Strategy, the council has been working towards achieving compliance with the principles of the government backed scheme - Cyber Essentials. We achieved Cyber Essentials accreditation in February 2022.

It is the council's intention to follow the "10 Steps to Cyber Security" as published by the National Cyber Security Centre in 2012 and most recently updated in 2021 (set out within this document – see Appendix 2 - 10 Steps to Cyber Security). Brent's Cyber Security Strategy 2022-2026 is aligned 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. The CAF is an assessment framework that provides a systematic and comprehensive approach to assessing the extent to which risks to essential functions are being managed by organisations. Aligning with this framework will enable the council to establish and maintain appropriate and proportionate cyber security, and embed security by design.

Scope of the strategy

In order to protect council systems and information from internet based (cyber) threats, and crime.



Brent
Cyber
Security
Strategy
2022
to
2026

The challenge we face as a council

Brent Council employs a wide range of technological and digital solutions, which have also been developed to incorporate learning from high-profile cyber attacks experienced by other local authorities, and taking into consideration potential cyber risks given the current globally challenging political landscape. As the number of applications and cloud based services used across the organisation increases, the potential vulnerabilities and risks also increase. These need to be managed effectively to mitigate and prevent potential cyber threats.

Threats

A threat if left unchecked, could disrupt the day-to-day operations of the council, the delivery of local public services and ultimately has the potential to compromise national security.

TYPES OF THREATS

- **Zero day threats**
  A zero day exploit is a cyber attack that occurs on the same day a weakness is discovered in software. At that point, it is exploited before a fix becomes available from its creator. 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 updated its antivirus software.

- **Cybercriminals and cybercrime**
  Cybercriminals are generally working for financial gain. Most commonly, for the purposes of fraud: either 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.

- **Hacktivism**
  Hacktivists 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 reputational damage locally. If online services are regularly disrupted by cyber-attacks this could lead to the erosion of public confidence in using such services.

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

- **Insiders**
  Staff may intentionally or unintentionally release sensitive information or data into the public domain. This may be for the purpose of sabotage or to sell to another party, but more often than not is due to simple human error or a lack of awareness about the particular risks involved.

- **Other threats include**:
  - **Physical threats**
    The increasing reliance on digital services brings with it an increased vulnerability in the event of a fire, flood, power cut or other disaster natural or otherwise that impact upon the council's IT systems.

  - **Terrorists**
    Some terrorist groups demonstrate intent to conduct cyber attacks, but fortunately have limited technical capability. Terrorist groups could obtain improved capability in a number of 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 or trade negotiations, or militarily.

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 adversely affect data security.

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

- **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 the way an organisation installs and maintains its IT hardware and software components is a threat.

- **Legacy Software**
  To ensure that legacy systems have sufficient user and system authentication, data authenticity verification, or data integrity checking features that prevent uncontrolled access to systems.

- **Training and Skills**
  It is fundamental that all employees have a fundamental awareness of cyber security and to support this.

Brent
Cyber
Security
Strategy
2022
to
2026

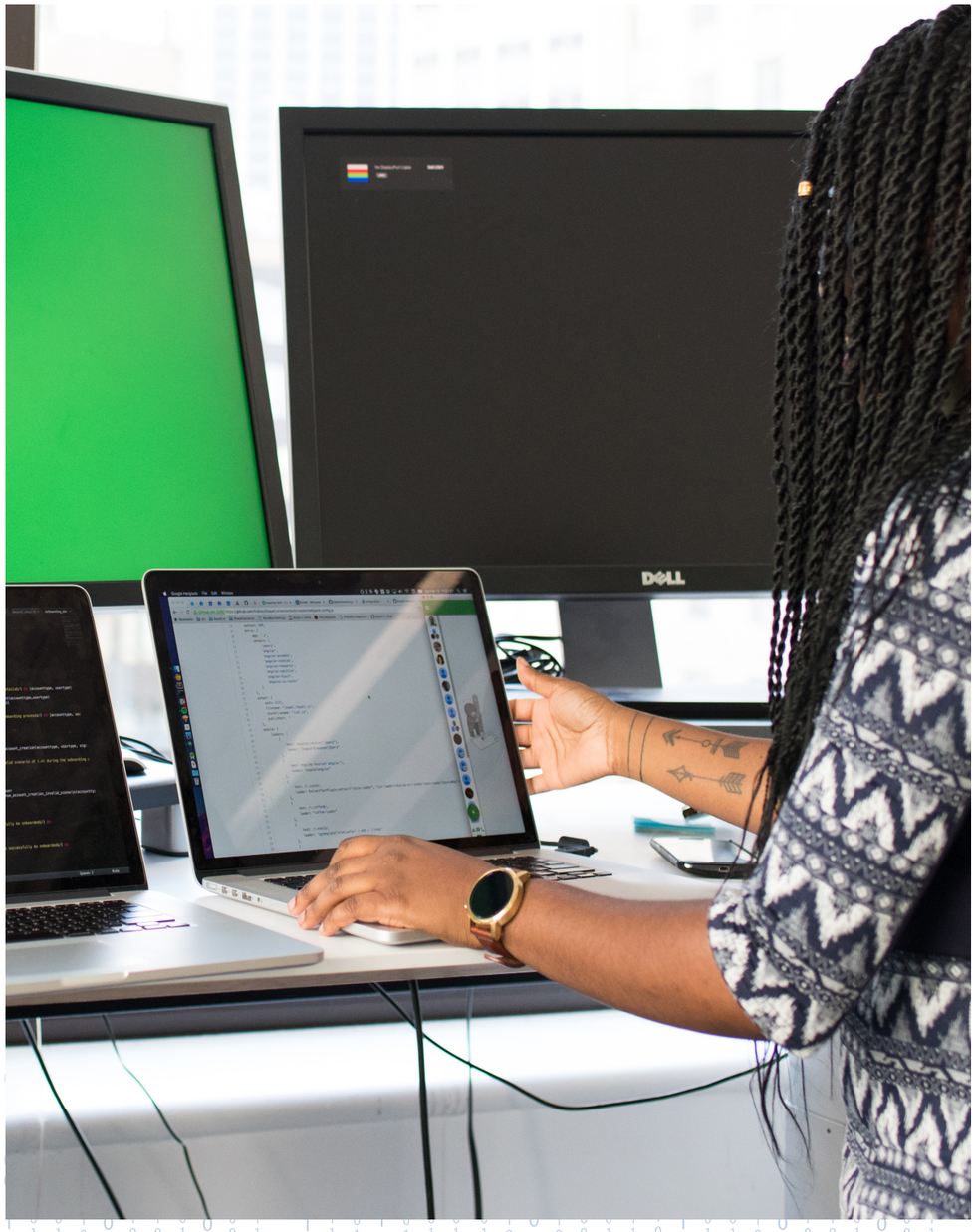
Data

Data is a business's most valuable and most risky asset, but to secure it you must know what you have got, so it is imperative to be able to find and reveal both structured and unstructured data across the organisation's assets.

Once a business knows its data, it can protect and power the organisation and the people it serves by both mitigating the risks in the data and using it in positive and proactive ways to drive the business forward.

Risks

Cyber risk management is a fundamental part of the broader risk management to ensure cyber security challenges are fully identified across the council and appropriate action is carried out to mitigate the risk.



Brent
Cyber
Security
Strategy
2022
to
2026

Our principles, goals and objectives

To mitigate the multiple threats, we face and safeguard our interests in cyberspace, we need a strategic approach that underpins all our collective and individual actions in the digital domain over the next four years.

This section sets out our vision, high level objectives, principles and priorities that will guide Brent Council in addressing cyber security.

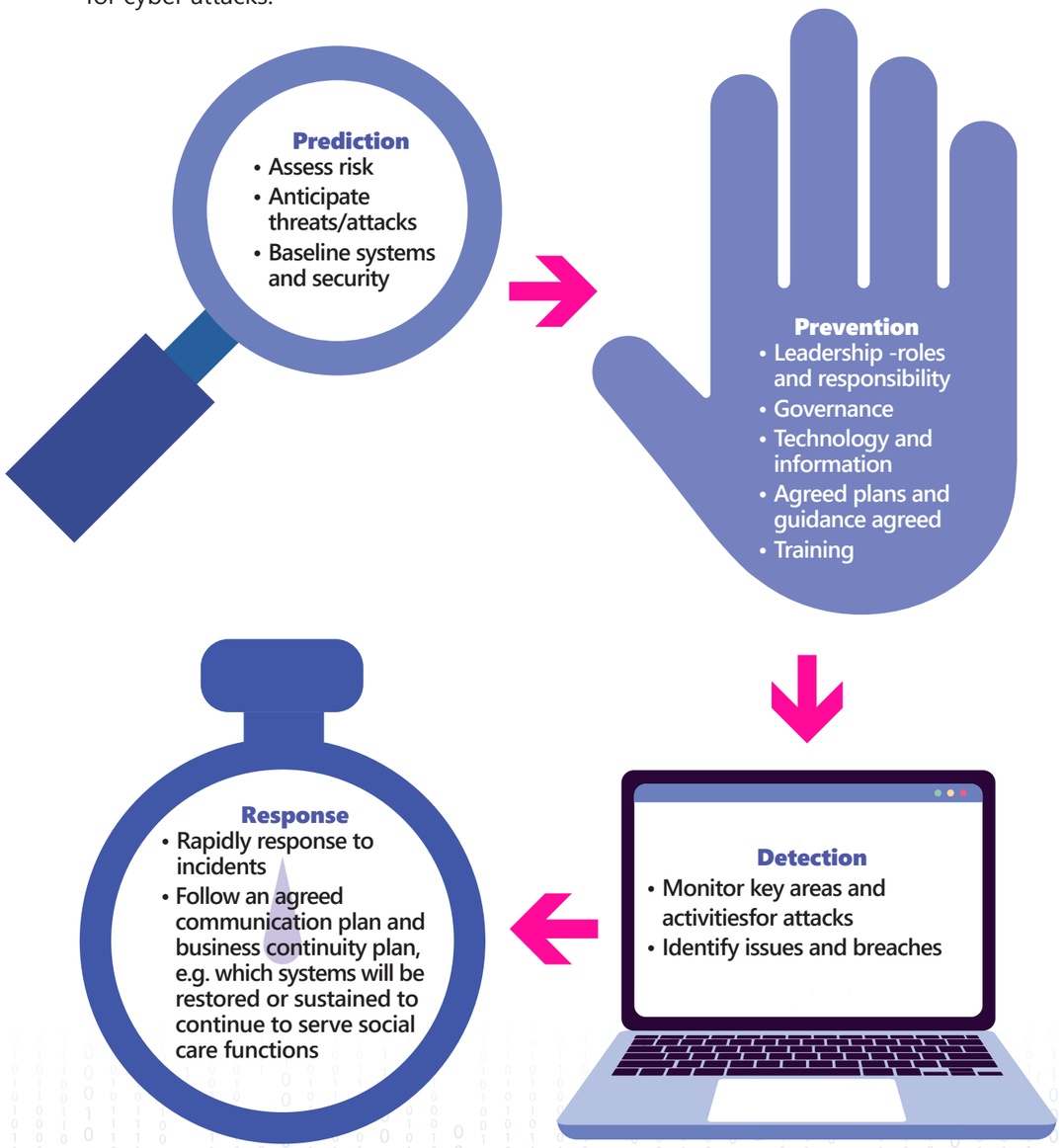
A council wide risk management framework is necessary for building a risk aware culture within the council, ensuring staff understand how to identify and manage risks.

The council is working towards achieving compliance with the Cyber Essentials standards by April 2022. The Cyber Essentials standards were developed by the UK Government in partnership with information security industry experts to assist organisations to mitigate and reduce the risks of common cyber threats. The council will also align itself with other standards including the Government Cyber Security Strategy 2022-2030, common assessment framework and other standards including ISO 27001. This will enable the council to continue to predict, prevent, detect and respond to information security risks.

Cyber awareness training is vital, from mitigating against an insider threat, understanding the supply chain risks or ensuring executive management understand the issues and responsibilities.

High level approach

The diagram below shows the roadmap for preparing the council and its contractors for cyber attacks.



Brent Cyber Security Strategy 2022 to 2026

Implementation plan

To deal with the changing landscape and to achieve our vision we will align with the National Cyber Security Strategy's (NCSC's) approach to **defend** Brent Council and our residents' cyberspace, to **deter** our adversaries and to **develop** our capabilities.

1. Defend

To have the means to defend the council against evolving cyber threats, to respond effectively to incidents, to ensure networks, data and systems are protected and resilient. Citizens and businesses have the knowledge and ability to defend themselves.

Actions:

a) Implementing firewalls and scanning services.

b) Carrying out health checks, penetration test and cyber resilience exercises to test their systems and processes, e.g. Web Check – a website configuration and vulnerability scanning service, developed with a number of public sector organisations including councils. This is free to use and available to all public sector organisations.

c) Meet compliance regimes, Code of Connection (CoCo) which require good cyber hygiene, to connect to government private networks, e.g. Public Services Network (PSN) and the Health and Social Care Network.

d) Work with partners across the public sector through participation in Cyber Security Information Sharing Partnership (CiSP), Warning, Advice and Reporting.

2. Deter

The council will be a hard target for all forms of aggression in cyberspace. This will involve detecting, understanding, investigating and disrupting hostile action.

Actions:

a) Apply government's cyber security guidance, e.g. 10 Steps to Cyber Security and Cyber Essentials and when developed the Government's common assessment framework

b) Use multi - factor authentication where technically possible, such as where administrative consoles provide access to manage cloud based infrastructure, platforms or services. Multi - factor authentication shall be used for access to enterprise level social media accounts

c) Establish an incident response and disaster recovery capability. Test incident management plans

d) Develop a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks

e) Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices

f) Train and or educate users to help detect, deter and defend against the cyber threats.

3. Develop

To have an innovative cyber security strategy to address the risks faced by residents, businesses and those in the voluntary sectors.

To develop a co-ordinated and tailored approach to risks and threats that we may encounter and mitigate potential vulnerabilities.

Actions:

a) Continue to develop and maintain risk management framework, internal control and governance for the prevention and detection of irregularities and fraud

b) Establish and implement process, procedures and controls to manage changes in cyber threat level and vulnerabilities

c) Operate the council's penetration testing programme; and cyber incident response

Brent
Cyber
Security
Strategy
2022
to
2026

d) Ensure continued training for staff and elected members

e) Develop an incident response and management plan, with clearly defined actions, roles and responsibilities. Develop an approach towards effective information security that puts data at the heart of the strategy by following five key steps:

1) Documented data policies and processes: set out the intentions for how the organisation will deal with its data to lay the bedrock for successful data security and governance

2) Employee awareness, training and culture: support data security and governance being so ingrained in people's thinking that it sits front and centre in their minds every day

3) Information discovery and classification: identify what data lies within the estate so appropriate actions can be taken to secure it, extract value from it and manage its complexity

4) Adding enforcement technologies: document encryption, data loss prevention, access control, data remediation, content management – taking a blended approach to enforcement means opening up APIs and integrating systems

5) Operational process and record keeping: use KPIs to enable the business to monitor and better understand its data to identify areas for continuous improvement.

f) Develop a communication plan in the event of an incident which includes notifying (for example) the relevant supervisory body, senior accountable individuals, the National Cyber Security Centre (NCSC), Government Security Group (Cabinet Office), the Information Commissioner's Office (ICO) or law enforcement as applicable (not exhaustive).

Critical success factors

Throughout the period of challenging transformation, the council will deliver robust information security measures to protect residents and stakeholder 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 the council's arrangements for IT security, the council will aim to:

- Build appropriate cyber security governance processes
- Maintain a council wide Cyber Risk Management Framework
- Maintain policies/procedures to review accesses on a regular basis.
- Create a cyber specific Business Continuity Management Plan and/or review Brent's Incident Plan to include emergency planning for cyber attacks
- 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 Brent has the best solutions to match to threats
- Continue to apply government's cyber security guidance – 10 Steps to Cyber Security
- Align with the Government's Cyber Assessment Framework once developed
- Provide relevant cyber security training for staff and elected members
- A regular schedule of cyber exercises, within the wider cycle of multi-agency incident response and recovery exercises
- Comply with the Government's 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.

Brent
Cyber
Security
Strategy
2022
to
2026

Cyber security governance / roles and responsibilities

An overview of the stakeholders tasked with improving cyber security and their respective roles and responsibilities.

Senior Information Risk Owner (SIRO)

The council's nominated Senior Information Risk Owner (SIRO) is the Director of Legal HR Audit and Investigations for Brent Council and who holds responsibility for the governance of cyber security and information risk within the council.

The SIRO is ultimately responsible for managing the risk to information and for ensuring that responsibility for information governance has been sufficiently organised to manage the risks, in accordance with the Data Protection Act 2018.

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.

The Cabinet

The Cabinet is made up of the Leader of the Council and other senior councillors (Cabinet members). Cabinet will agree and receive updates on implementation of the Cyber Security Strategy.

Council Management Team (CMT)

CMT sponsors the Cyber Security Strategy

and will oversee the strategic framework through which the council governs its information resources.

Information Governance Group (IGG)
CMT sponsors the Cyber Security Strategy and will oversee the strategic framework through which the council governs its information resources.

Information Governance Team (IGT)
The Information Governance Team will oversee the council's compliance with The Data Protection Act 2018 and promote information governance (IG) best practice, including cyber security, across the organisation. The Information Governance Lead will work closely with the Senior Information Risk Owner (SIRO) and the Data Protection Officer to provide effective advice and oversight of information compliance across the council.

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

Customer & Digital Board
The Customer and Digital Board oversees implementation of the council's Digital Strategy. The board will ensure that risks, issues and dependencies are proactively managed and make decisions in relation to any risks and issues that have been escalated in relation to the digital programme.

Shared Technology Services (STS)
Shared Technology Services oversees the delivery of the Shared IT Service for Brent, Lewisham and Southwark.

Information Asset Owners (IAO)
Information Asset Owners are responsible for all processing of personal data within their business area.

It is the responsibility of all staff to comply with the Standard.

Brent
Cyber
Security
Strategy
2022
to
2026

Appendix 1-Standards

Information Security Management within Brent Council will comply with the British Standard: BS ISO/IEC 27001:2013

This standard specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system (ISMS) within the context of the council's overall business risks. It specifies requirements for the implementation of security controls customised to the needs of the council. ISO27032 and The Government's Cyber Essentials provide security standards for the Internet (referred to as "Cyberspace" or "Cyber").

Currently, Brent has PSN, DSP toolkit and follows PCI.

Appendix 2 - Ten steps to cyber security

Risk management regime
Embed an appropriate risk management regime following the ISO27k standards, across the organisation. This should be supported by an empowered governance structure, which is actively supported by the board and senior managers. Clearly communicate your approach to risk management with the development of applicable policies and practices. These should aim to ensure that all employees, contractors and suppliers are aware of the approach, how decisions are made, and any applicable risk boundaries.

Secure configuration
Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems. You should develop a strategy to remove or disable unnecessary functionality from systems, and to quickly fix known vulnerabilities, usually via patching. Failure to do so is likely to result in increased risk of compromise of systems and information.

Network security
The connections from your networks to the Internet, and other partner networks, expose your systems and technologies to attack. By creating and implementing some simple policies and appropriate architectural and technical responses, you can reduce the chances of these attacks succeeding (or causing harm to your organisation). Your organisation's networks almost certainly span many sites and the use of mobile or remote working, and cloud services, makes defining a fixed network boundary difficult. Rather than focusing purely on physical connections, think about where your data is stored and processed, and where an attacker would have the opportunity to interfere with it.

Managing user privileges
If users are provided with unnecessary system privileges or data access rights, then the impact of misuse or compromise of that users account will be more severe than it need be. All users should be provided with a reasonable (but minimal) level of system privileges and rights needed for their role. The granting of highly elevated system privileges should be carefully controlled and managed. This principle is sometimes referred to as 'least privilege'.

User education and awareness
Users have a critical role to play in their organisation's security and so it's important that security rules and the technology provided enable users to do their job as well as help keep the organisation secure. This can be supported by a systematic delivery of awareness programmes and training that deliver security expertise as well as helping to establish a security-conscious culture.

Incident management
All organisations will experience security incidents at some point. Investment in establishing effective incident management policies and processes will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact. You should identify recognised sources (internal or external) of specialist incident management expertise.

Malware prevention
Malicious software, or malware is an umbrella term to cover any code or content that could have a malicious, undesirable impact on systems. Any exchange of information carries with it a degree of risk that malware might be exchanged, which could seriously impact your systems and services. The risk may be reduced by developing and implementing appropriate anti-malware policies as part of an overall 'defence in depth' approach.

Monitoring
System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements.

Removable media controls
Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. You should be clear about the business need to use removable media and apply appropriate security controls to its use.

Home and mobile working
Mobile working and remote system access offers great benefits, but exposes new risks that need to be managed. You should establish risk based policies and procedures that support mobile working or remote access to systems that are applicable to users, as well as service providers. Train users on the secure use of their mobile devices in the environments they are likely to be working in.

Appendix 3 - Brent's cyber security work program

Ref#	Priority	Action	Owner	Details	Due Date
1-a	DEFEND	Implementing firewalls and scanning services	Chief Security Officer	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.	Apr-22
1-b	DEFEND	Carrying out health checks, penetration test and cyber resilience exercises to test their systems and processes	Chief Security Officer/ Information Governance Lead	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.	Annually
1-c	DEFEND	Meeting compliance regimes, e.g. PSN, PSI and the Health and Social Care Network	Chief Security Officer/ Information Governance Lead	• 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 March 2022	Annually (June 2022)
1-d	DEFEND	Working with partners across the public sector through participation in Cyber Security Information Sharing Partnership (CiSP), Warning, Advice and Reporting	Chief Security Officer	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	Nov-22
2-a	DETER	Network Security - Protect the networks from attack, Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.	Chief Security Officer/ Information Governance Lead	• Applying Government's Cyber Security Guidance • 10 Steps to Cyber Security • Cyber Essentials	Apr-22
2-b	DETER	Multi - factor authentication shall be used where technically possible, such as where administrative consoles provide access to manage cloud based infrastructure, platforms or services. Multi - factor authentication shall be used for access to enterprise level social media accounts.	STS	Where VPN and Remote Desktop Proxy (RDP) are in use, Multi Factor Authentication (MFA) 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. Data A Protection Impact Assessmnt (DPIA) to be carried out on al new systems/tools.	Sep-22

Brent Cyber Security Strategy 2022 to 2026

Appendix 3 - Brent's cyber security work program continued

Ref#	Priority	Action	Owner	Details	Due Date
2-c	DETER	Incident management - Establish an incident response and disaster recovery capability. Test your incident management plans.	Chief Security Officer/ Information Governance Lead	Run books have been developed with more to be created to address cyber incidents. Cases are managed through the current ITSM system.	Sep-22
2-d	DETER	Monitoring - Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks.	Chief Security Officer	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.	Sep-22
2-e	DETER	Secure configuration - Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.	Chief Security Officer	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.	Oct-22
2-f	DETER	User education and awareness - Produce user security policies covering acceptable and secure use of your systems. Include in staff training.	Chief Security Officer/ Information Governance Lead	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.	Annually
3-a	DEVELOP	Develop and maintain risk management framework, internal control and governance for the prevention and detection of irregularities and fraud	STS/Brent IG	Current STS digital risks fed through to Brent's corporate risk register	Annually
3-b	DEVELOP	Process, procedures and controls to manage changes in cyber threat level and vulnerabilities	Chief Security Officer	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.	Annually
3-c	DEVELOP	Operation of the council's penetration testing programme; and Cyber-incident response	Chief Security Officer/ Information Governance Lead	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).	Annually
3-d	DEVELOP	Introducing training for staff and elected members	Chief Security Officer/ Information Governance Lead	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.	Annually

Appendix 3 - Brent's cyber security work program continued

Ref#	Priority	Action	Owner	Details	Due Date
3-e	DEVELOP	Develop an incident response and management plan, with clearly defined actions, roles and responsibilities	Chief Security Officer/ Information Governance Lead	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).	Sep-22
3-f	DEVELOP	Develop a communication plan in the event of an incident	Chief Security Officer/ Information Governance Lead	Relevant Internal roles and responsibilities have been identified. The Information Governance team are working with STS to develop the plan within the incident response playbook excercises.	Sep-22

Brent Cyber Security Strategy
2022 to 2026

Brent