Cyngor Castell-nedd Port Talbot
Neath Port Talbot Council

NPTCBC

Cyber Security Strategy

Version: 2.0
Publish Date: December 2021
Review Date: December 2022
Next Review: December 2023
Owner: Chief Digital Officer

Cyngor Castell-nedd Port Talbot
Neath Port Talbot Council

Table of contents

1. Introduction

We live in a world characterised by interconnecting data, constantly evolving and empowering us to make better informed decisions. Information and data are vital to every part of the work of a Local Authority. As we deliver against the objectives in our Smart & Connected Digital Strategy, we are transforming the way we work and how our residents, business and wider stakeholders access information and services. As a result, we need increasingly robust security measures to protect against cyber threats.

Across the world, cyber-attacks are growing more frequent and sophisticated. Public sector organisations are not immune to the rise in cyber incidents and when they succeed, the damage can be life-altering, with severe personal, economic and social consequences.

This Cyber Security Strategy sets out Neath Port Talbot County Borough Council's approach to protecting our information systems, the data held within them, and the services they provide from unauthorised access, harm or misuse. This ensures the services we provide are secure and our residents, businesses and wider stakeholders can safely interact with us. It requires a balance of embracing digital opportunities, including making information more widely available and accessible, whilst ensuring that the right levels of protection are in place.

In order to obtain strong cyber security, the Council must ensure it promotes a comprehensive risk-based approach to cyber security, which is integrated across personnel, technical security, information assurance and physical security which strategically encompasses Information Security, Assurance, Resilience and Governance.

This approach is in line with the HMG Cyber Security standard, the Public Services Network (PSN) code of connection and National Cyber Security Strategy of 'Defend, Deter, Develop'.

2. Purpose and scope of the strategy

The purpose of this strategy is to give assurance to residents, businesses and other stakeholders of the Council's commitment to delivering robust information security measures to protect resident 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. The strategy supports delivery of the wider Digital Strategy by providing a framework for the Council to securely harness the benefits of digital services for the benefit of all stakeholders.

Through delivery of this strategy, we will comply with and embed the principles of 'Cyber Essentials'; 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, the data on the systems we are responsible for and the services they help provide. The recommendations in this strategy will be embedded in all areas of new and emerging technologies which we implement. It will also set out the best practices that will be rooted in our business as usual.

The strategy will sit alongside other Council strategies such as the Information Governance Strategy and is supported by a suite of operational policies (Acceptable usage policy, Information Security Policy, IT Security Policy, Removable Media Policy, Mobile Device Policy and Information Security Breach Policy) and Incident Response Playbooks (Denial of Service, Phishing, Malware etc.)

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 unauthorised copying of 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 unauthorised access. Cyber security may also be referred to as information technology security.

It is important because, in order to effectively deliver services, we all process and store large amounts of data on computers and other devices, with a significant portion of this data being classified as sensitive information. It will also include financial, personal and other types of information, for which unauthorised access or exposure could have negative consequences.

We transmit sensitive data across networks and to other devices in the course of providing services. 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 also crucial in ensuring our services continue to operate. It is a core element of building and keeping our stakeholders trust. A cyber-attack would potentially have very serious consequences in terms of disruption to our services (many of which serve some of our most vulnerable residents), the Council's reputation and impact to our financial position.

4. The challenge we face as a Council

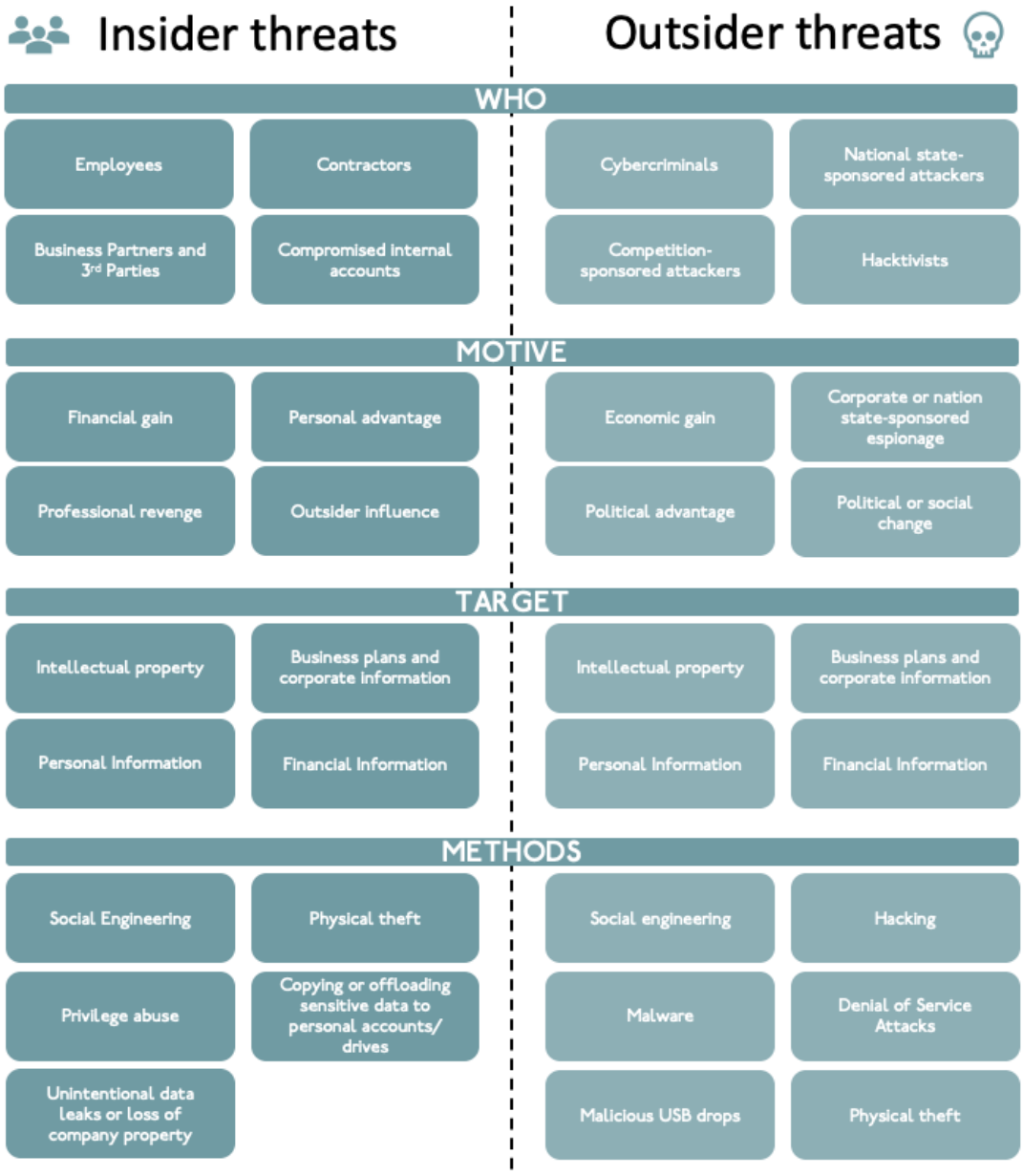
We are using an increasing range of technology, from 'apps' and 'the cloud', to different devices and 'gadgets'. Much of our business is online - corresponding with residents and local businesses, carrying out case work, and reviewing reports and papers for Council meetings.

This direction of travel is expected to continue and accelerate; making effective cyber security ever more crucial in protecting against new types of threats, risks and vulnerabilities.

Threats - A threat if left unchecked, could disrupt the day-to-day operations of the Council, and the delivery of local public services.

Types of Threats

Generally, there are two types of threats. Insider Threats or Outsider Threats they are explained in detail in the diagram below:



Cyber Criminals and Cyber Crime

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.

We have already developed Cyber Incident Playbooks for each of these situations.

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

Hacktivist groups have successfully used distributed denial of service (DDoS) attacks to disrupt the websites of a number of Councils already. (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 in order to sell to another party, but more often than not 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 a weakness has been discovered in software. At that point, it's 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 the relevant updates to its antivirus software.

Physical Threats

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

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, trade or military negotiations.

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

We must 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 crucial that all employees have a fundamental awareness of cyber security. Accountable managers are responsible for ensuring all their employees have completed the appropriate training.

Assets

We regularly review the value of all assets across the Council in line with legislative requirements, to ensure that the appropriate levels of protection are placed around those digital and physical assets. Our assets include:

- Data
- Services
- Infrastructure

Risks

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

5. Our approach, principles and priorities

To mitigate the multiple threats we face and to safeguard our interests, we need a strategic approach that underpins our collective and individual actions in the digital domain over the coming years. This will include:

- Fostering a culture of empowerment, accountability and continuous improvement.
- Prioritising information assets and processes, maintaining appropriate records and policies and conducting regular reviews including data retention policies.
- Ensuring adequate procedures and plans are in place to recover and quickly identify exposure.
- Embedding a Council wide risk management framework to help build a risk aware culture, ensuring staff understand how to identify and manage risks.
- Delivering Information Security Awareness training and principles to help mitigate insider threats, understand supply chain risks and ensure all staff understand the issues and their responsibilities.

The diagram below shows the continual cycle for protecting the Council and its service users from cyber-attacks:

Identify

- Identify and catalogue sensitive information and key operational services.
- Understand and manage user access to key operational services.
- Review through Information and Cyber Security Governance Processes.

Protect

- Access to sensitive information and key operational services shall only be provided to identified, authenticated and authorised users or systems.
- Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities.
- High privileged accounts shall not be vulnerable to common cyber-attacks.

Detect

- Steps are taken to detect cyber-attacks.
- Monitor key areas and activities.

Respond

- A rapid response to incidents.
- A defined, planned and tested response to security incidents that impact personal, sensitive or confidential information, leveraging a multi-disciplinary response team.

Recover

- Identification and testing of contingency mechanisms to ensure critical service delivery continues.
- Restoration of services to normal operation.
- Lessons learned fed back into the process.

6. Implementation Plan

To adapt to the changing landscape and achieve our vision we will align with the National Cyber Security Strategy's approach to defend the Council, residents, businesses and wider stakeholders, deterring potential threats and developing our capabilities – Defend, Deter and Develop.

Defend

The Council will further develop 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:

- Maintaining firewalls and scanning services.
- Continue to develop end-point protection (Anti-Virus, USB Encryption and MDM).
- 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.
- Meeting compliance regimes, Code of Connection (CoCo) which require good cyber hygiene, to connect to government private networks, e.g. Public Sector Network (PSN).
- Working with partners across the public sector through participation in Cyber Security Information Sharing Partnership (CiSP), Warning, Advice and Reporting.

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 against the Council.

Actions:

- **Governance**
    - Applying government's cyber security guidance, e.g. 10 Steps to Cyber Security or Cyber Essentials.
    - Review (update where appropriate) policies and procedures.

- **Technology and information**
    - Ongoing review of network security.
    - 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 based 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.
    - Malware prevention.
    - Removable media controls.
    - Secure by design configuration.
- Review and update plans and guidance.
- Training or educating users to help detect, deter and defend against the cyber threats.

Develop

The Council will continually develop this innovative cyber security strategy to address the risks faced by our residents, businesses and wider stakeholders.

This includes developing a co-ordinated 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.
- 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.
- Training for staff and elected members.
- Develop an incident response and management plan, with clearly defined actions, roles and responsibilities.
- 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.
- Develop a network of sharing with other Councils, collaborate and learn from each other, harness networks such as, WARP and CiSP.

7. Critical Success Factors

Throughout this period of challenging transformation, the Council has committed to delivering 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 information security, the Council will:

- Develop appropriate cyber security governance processes.
- Develop a Council wide Cyber Risk Management Framework.
- Develop policies/procedures to review access on a regular basis.
- Create a cyber-specific Business Continuity Management Plan and/or review our 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 we have the best solutions to match to threats.
- Apply the Government's 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.

8. Cyber Security Governance – Roles and Responsibilities

Effective cyber security governance at the Council is delivered through the following roles and functions.

Senior Information Risk Owner (SIRO)

The Council's nominated Senior Information Risk Owner (SIRO), is the Chief Digital Officer. The 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 legal requirements.

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

Corporate Director's Group (CDG)
CDG will take an overview of the Cyber Security Strategy via regular updates from the SIRO, where progress and risks are reported.

Corporate Governance Group

The Corporate Governance Group will have reporting and monitoring oversight of Cyber Security threats that have been experienced across the Council. They will also deal with any Cyber Security escalation matters.

Information Security Group (ISG)
The group is comprised of senior representatives from each service area. The group are responsible for overseeing the delivery of the Information, Cyber Security and related Strategies and monitoring their effectiveness.

Data Protection Officer (DPO)
The Council's Data Protection Office (DPO), is the Head of Legal and Democratic Services. The DPO leads on overseeing the Council's implementation of data protection legislation (UK GDPR and the Data Protection Act 2018). They take an assurance view that progress is being made in adoption and implementation of the Cyber Security Strategy, and commission the undertaking of Audits of Information Security as appropriate.

Security and Operations Team
The Security team will lead on the implementation of the Cyber Security Strategy, preparing regular feedback and updates not only on progress regarding implementation of the tasks identified but also provide an informed view of the threat landscape overall.

Information Governance Team
The Information Governance team will lead on information security incident investigations that are not serious cyber security incidents which are dealt with under the cyber incidence response plan and hold the corporate information security incident register.

The team will be part of all initiatives to provide information security, data protection and information management advice and recommendations ensuring that potential issues are identified and escalated to the relevant area.

Information Asset Owners
Information Asset Owners are responsible for all processing of personal data within their business unit/service area. They are identified by the Information Governance team.

All Council staff / users and Elected Members
It is the responsibility of all staff / users and Elected Members to comply with the standards set out in this Cyber Security Strategy and within supporting Policies, such as, but not limited to Members ICT Scheme, Information Security and Acceptable Usage Policy.

Appendix A: Standards

Information Security Management within Neath Port Talbot County Borough Council will comply with appropriate standards. These include the Governments' Cyber Essentials certification for Cyber Security, the Public Services Network Code of Connection and PCI DSS.

The 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.

Appendix B: NCSC: 10 Steps to Cyber Security

Risk Management Regime

Embed an appropriate risk management regime following 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.