South Somerset
District Council

SSDC's Cyber Security Strategy

South Somerset District Council

Contents

Foreword 02

Introduction 03

What is cyber security and why is it important? 03

Strategic context 04

Purpose 05

Scope of the strategy 05

The challenge we face as a council 05

Threats 06

Types of threats 06

Zero day threats 06

Physical threats 07

Terrorists 07

Espionage 07

Vulnerabilities 07

Risks 07

Our approach, principles and priorities 08

Implementation plan 09

Defend 09

Deter 09

Develop 10

Critical success factors 11

Cyber security governance roles and responsibilities 12

Appendix 1: Standards 13

Appendix 2: NCSC: 10 steps to cybe security 14

The Cyber Security Strategy

South Somerset District Council

Foreword

Information and data are vital to every part of South Somerset District Council's business. As we continue with a digital programme that is transforming the way we work and how local people access information and services, we need increasingly robust security measures to protect against cyber threats.

Across the globe, cyber attacks are growing in frequency and becoming more sophisticated. The increased use of the internet caused by Covid 19 pandemic means that cyber criminals have become more active, and our exposure has increased. When cyber attacks succeed the damage can be significant; with personal, economic and social consequences.

This Cyber Security Strategy sets out our approach for protecting our information systems and the data we hold to ensure the services we provide are secure and our residents, businesses and stakeholders can safely transact with us. This includes achieving a balance of embracing digital opportunities, including making information more widely available and accessible, whilst ensuring that right levels of protection are in place.

This strategy demonstrates our commitment and the key actions we will take to further establish a trusted digital environment for SSDC. We will strengthen and secure SSDC from cyber threats by increasing security awareness throughout our workforce, investing in our systems and infrastructure, deterring our adversaries, and developing a wide range of responses, from basic cyber hygiene to the most sophisticated defences.

Cyber-attacks will continue to evolve, which is why we will continue to work at pace to stay ahead of all threats.

This Cyber Security Strategy underpins and enables the SSDC Digital Strategy, which continues to ensure we harness the benefits of technology to improve the lives and life chances of all local people. The measures outlined in this strategy will safeguard trust and confidence in the way we operate and deliver our services, supporting SSDC to remain at the forefront of the digital revolution

Tony Lock

Portfolio Holder for Protecting Core Services

Introduction

This document sets out South Somerset District Council's application of information and cyber security standards to protect our information systems, the data held on them, and the services we provide, from unauthorised access, harm or misuse. It is our cyber security commitment both to the people we represent and the national interest; and emphasises the importance of cyber security in the role of all council staff.

What is cyber security and why is it important?

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

Attacks on Confidentiality – stealing or 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.

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 because, in order to effectively deliver services, South Somerset District Council collects, processes, and stores large amounts of data on computers and other devices. A significant portion of this data is sensitive information, including financial data, personal information, or other types of data for which unauthorised access or exposure could have negative consequences.

SSDC transmits 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.

Cyber security is crucial in ensuring our services are kept up and running. It is also vital in ensuring the public trusts the council with their information. A cyber-attack could have very serious consequences, both in terms of disrupting services – many of which serve our most vulnerable residents – and through damage to the council's reputation.

Strategic context

South Somerset District Council is One Team, Ambitious for South Somerset. We aim to be:

Great to work for
with agile and empowered staff, inspiring people and investing in developing our people.

Excellent to work with
Efficient and effective with a commercial mindset.

Leading the way
a modern and resilient council that is adaptable to change and technologically enabled.

Delivering for our communities
focused on outcomes and quality of life, data driven, and proactive.

The ongoing discussions over future models for local government in Somerset make this strategy no less important. Whatever model is adopted, digital ambition will be fundamental to delivering quality services to our communities, and as future structures exploit technology, cyber and information security will remain of the utmost importance.

The Covid 19 pandemic has impacted on all areas of public and private life. Amongst other things it has it has forced a great deal more of our routine professional and personal interactions on-line and many more of us now work predominantly from home. This has presented new and lucrative opportunities to cyber criminals. Whilst much will return to normal in due course, the extent to which we exploit cyberspace and many of our working practice will not return to the pre-pandemic norm. Cyber security has become, and will remain, a key responsibility for all of us – collectively and as individuals.

The SSDC Digital Strategy (2021-2026) will set out SSDC's ongoing digital ambition, including how technology will be used to progress the areas of focus and priority programs set out in the Council Plan. This Cyber Security Strategy supports delivery of the Digital Strategy and the Council Plan by providing a framework for SSDC to securely harness the benefits of digital technology for the benefit of all stakeholders. It is essential to the efficient running and evolution of the council.

This Cyber Security Strategy is supported by a suite of operational policies and procedures.

Purpose

The council seeks to deliver its digital strategy through transforming South Somerset into a digital place and a digital Council. The scale of transformation represents an unprecedented culture shift for the Council, residents, partners and businesses.

The Cyber Security Strategy is a new strategy, introduced in response to the increasing threat from cyber criminals and a number of successful and high profile cyber-attacks on public and private organisations. The purpose of the strategy is to give assurance to residents and other stakeholders of the council's commitment in 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.

Through delivery of this strategy, we will comply with and embed the principles of 'Cyber Essentials Plus'; a government-backed, industry-supported scheme to help organisations protect themselves against common online threats. We will also follow the "10 Steps to Cyber Security" framework published by the National Cyber Security Centre *(included as Appendix 2)*.

Scope of the strategy

This strategy is intended to cover all SSDC's information systems, the data held on them, and the services they help provide. It aims to increase cyber security for the benefit of all South Somerset residents, businesses, partners and stakeholders; helping to protect them from cyber threats and crime.

The challenge we face as a council

South Somerset District Council is using an increasing range of technology, from apps and the cloud, to different devices and gadgets. Much of our business is done online such as 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, the delivery of local public services, and ultimately has the potential to compromise national security.

Types of threats

Cybercriminals 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.

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.

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'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 updated its antivirus software.

Other types of threats

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 council 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 crucial that all employees have a fundamental awareness of cyber security and to support this.

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.

Our approach, principles and priorities

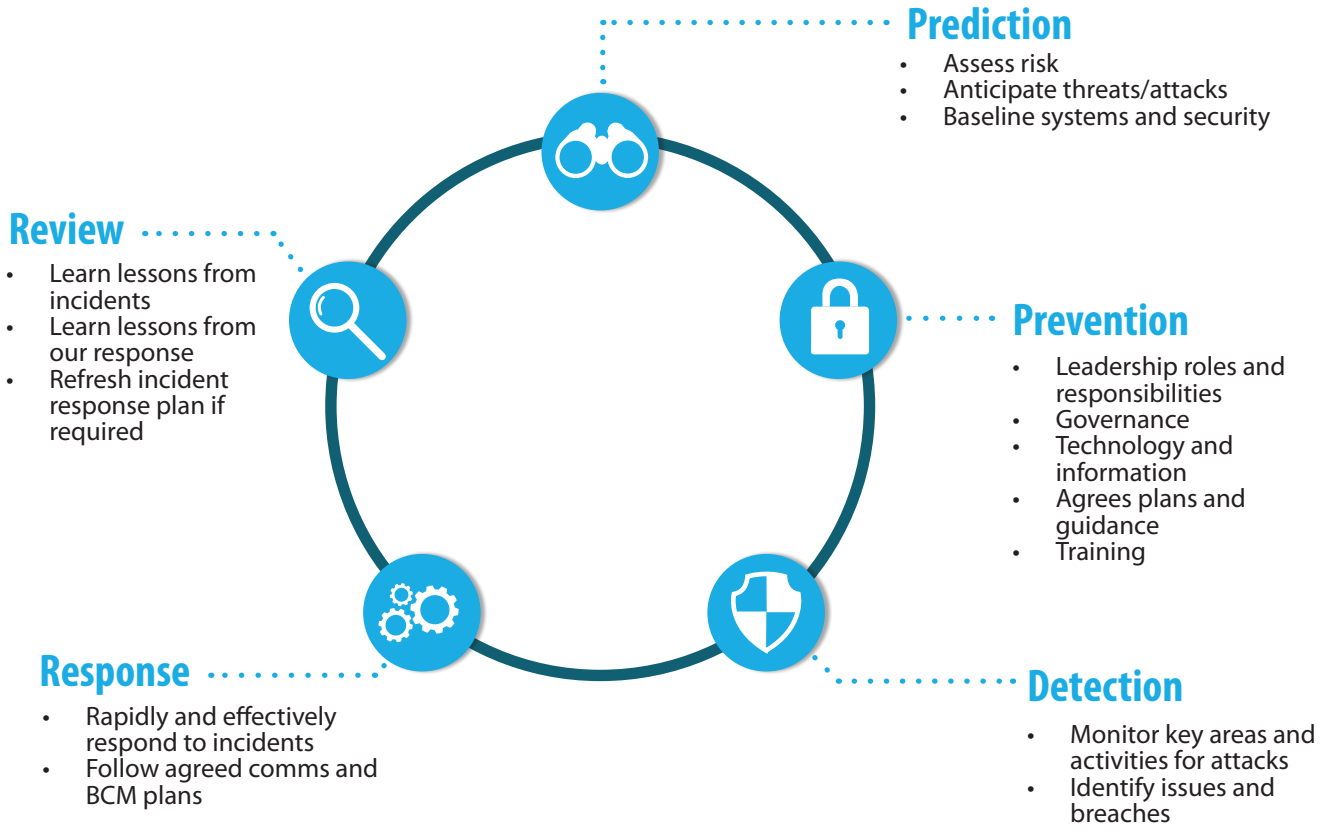
To mitigate the multiple threats we face and safeguard our interests in cyberspace, we need a strategic approach that underpins our collective and individual actions in the digital domain. This will include:

- A council wide risk management framework to help build a risk aware culture within the council, ensuring staff understand how to identify and manage risks.

- Cyber Awareness training to help mitigate insider threats, understand supply chain risks and ensure all staff understand the issues and their responsibilities.

- Applying the Cyber Essentials scheme controls and conforming to appropriate frameworks to ensure that the council will be able to identify, mitigate and protect against information security risks in a prioritised and resourceful fashion.

The diagram below shows the Cyber Security approach that SSDC will adopt.



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 SSDC and our residents' cyberspace, to deter our adversaries and to develop our capabilities.

Defend

The council 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:

- Implement firewalls and scanning services
- Carry out health checks penetration test and cyber resilience exercises to test systems and processes.
- Meet compliance regimes, which require good cyber hygiene, to connect to government private networks, e.g. Public Sector Network (PSN)
- Work with partners across the public sector through participation in the Cyber Security Information Sharing Partnership (CiSP), Warning, Advice and Reporting Point (WARP) and other networks.

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 us.

Actions:

Governance

- Applying government's cyber security guidance, e.g. 10 Steps to Cyber Security and Cyber Essentials Plus

Technology information

- 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 configuration

Agreed plans and guidance

Training and education so that all users can help detect, deter and defend against cyber threats

South Somerset District Council

Develop

The council will continually develop our innovative cyber security strategy to address the risks faced by our residents, businesses and community and voluntary sector.

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
- Put in place processes, 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
- Introduce 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 (not exhaustive)

Critical success factors

SSDC is 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 IT security, the council will:

- Develop appropriate cyber security governance processes.
- Adopt a council wide Cyber Risk Management Framework (Cyber Essentials Plus).
- Develop policies/procedures to review access on a regular basis.
- Create a cyber-specific Business Continuity Management Plan and review SSDC's Incident Plan to include emergency planning for cyber attack
- Maintain, rehearse and regularly review 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 playbooks to support test exercises on a regular basis; to ensure effective reaction to incidents when an incident occurs
- Create 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 SSDC has 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) requirements and the Payment Card Industry Data Security Standard (PCI DSS); 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.

Cyber security governance roles and responsibilities

Effective cyber security governance in SSDC is delivered through the following roles and functions.

Senior Information Risk Owner (SIRO)

The Council's nominated Senior Information Risk Owner (SIRO), is the Director of Strategy and Support. 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 GDPR.

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

District Executive

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

Senior Leadership Team (SLT)

SLT sponsor the Cyber Security Strategy and oversee the strategic framework through which the council governs its information resources.

Lead Specialist Digital Change

The Lead Specialists Digital Change is answerable to the SIRO for the cyber security health and readiness of SSDC. He/she will ensure that the Cyber Strategy is adequately resourced and that implementation work is appropriately prioritised.

Digital Specialist Security and Compliance

The Digital Specialist Security and Compliance is SSDC's IS and Cyber Security subject matter expert. He/she will give advice and guidance to other stakeholders, organise audits and health checks, and lead on cyber security incident response and DR.

Digital Specialist Strategy and Architecture will deputise if and when necessary.

Technical Design Authority (TDA)

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

Change Advisory Board (CAB)

The CAB reviews all proposed changes to existing services within the IT production arena to ensure that sufficient diligence has occurred to minimise the risk of adverse impact.

Data Protection Officer (DPO)

The DPO complements the activity of and supports the Digital Specialist Security and Compliance, leading on non-technical aspects of data protection and providing assurance.

Information Asset Owners (IAO)

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

All elected members and SSDC officers

It is the responsibility of all elected members and officers to comply with the standards set out in this Cyber Security Strategy.

South Somerset District Council

Appendix 1: Standards

Information Security Management with appropriate standards.

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.

The Government's Cyber Essentials provide security standards for the Internet (referred to as "Cyberspace" or "Cyber")

SSDC complies with PSN and PCI DSS.

Appendix 2: NCSC: 10 steps to cyber security

1. Risk management regime

Embed an appropriate risk management regime following the corporate standard 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.

2. 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.

3. 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.

4. 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'.

5. 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.

6. 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.

7. 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.

8. Monitoring

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.

South Somerset District Council

Appendix 2: NCSC: 10 steps to cyber security

9. 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.

10. Home and mobile working

Mobile working and remote system access have become the norm since Covid 19, but they expose 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.