NEWARK & SHERWOOD DISTRICT COUNCIL

Report to: Cabinet Meeting - 17 January 2023

Portfolio Holder: Councillor Keith Girling, Organisational Development & Governance

Director Lead: Sanjiv Kohli, Deputy Chief Executive / Director – Resources / S151 Officer

Lead Officer: Dave Richardson, Business Manager - ICT & Digital Services, Ext. 55405

Report Summary	
Type of Report	Open Report (with an exempt appendix), Non-Key Decision
Report Title	Cyber Security Strategy
Purpose of Report	To present Newark & Sherwood District Council's Cyber Security Strategy.
Recommendations	That Cabinet approve the adoption and wider communication of the Cyber Security Strategy.
Alternative Options Considered	Not to adopt a cyber security strategy, but this would be contrary to best practice.
Reason for Recommendations	To raise awareness of the Cyber Security agenda and obtain buy-in to the implementation plan, providing assurance to our residents, businesses, and external stakeholders.

1.0 Background

1.1 Cyber Security Updates have been a regular item on the Senior Leadership Team's (SLT) agenda with many an update providing an overview of the organisation's posture and resilience. This has included implementation of a cyber incident response plan and setting the scene for a proposed Cyber360 pilot review by the Local Government Association (LGA).

1.2 SLT have been made aware of emerging risks and actions plan to mitigate and control these risks, this is all part of the cyber security lenses and culture that we aim to promote further in order to protect stakeholders data and information assets from a range of threats.

1.3 The national strategy, LGA and the Cyber Security Centre (NCSC) acknowledge board level responsibility in the event of Cyber Incident, which our SLT have recognised with the further acceptance that a pilot Cyber360 review by the LGA would be beneficial.

1.4 During a Cyber360 pilot review of another Local Authority, ICT & Digital Services Business Manager participated and acknowledged that Newark & Sherwood District Council had a gap in the suite of strategies, albeit assurance that controls and actions are being implemented.

1.5 Since the recent update to SLT, ICT & Digital Services have developed a Cyber Security Strategy and implementation plan that aligns to the National Strategy and yet is appropriate for our employees, elected members and partners that utilise the Council's infrastructure.

1.6 The Strategy outlines key themes and is presented in the separate document Cyber Security Strategy 2022 to 2026:

- Purpose
- Scope
- The Challenge we face
- Threats
- Vulnerabilities
- Risk
- Approach, Principles and priorities
- Implementation Plan
- Critical Success Factors
- Roles and Responsibilities

1.7 This strategy should provide a level of assurance to our stakeholders that the Council takes Cyber Security, data protection and information security seriously, notwithstanding acknowledge the challenging and changing global threat landscape.

2.0 Proposal/Details of Options Considered

2.1 The acceptance and implementation of the strategy will ensure that we deliver a vision and plan to managing cyber security threats whilst reducing risk, protecting residents and stakeholder data from misuse and cyber threats.

2.2 Therefore, the proposal is that the Council adopt the Cyber Security Strategy.

2.3 Once adopted, ICT & Digital Services will communicate important messages and actions from the Strategy to key stakeholders including elected members and employees across the Council, Active4Today and Arkwood Developments Ltd.

2.4 This includes but is not limited to: cyber awareness training for colleagues and councillors, supply chain due diligence and awareness of the Cyber Incident Response Plan.

2.5 ICT & Digital Services will also support residents and local business by liaising with Corporate Communications to provide information about cyber security practice, and by offering signposting support in response to incidents and queries.

2.6 The Cyber Security Strategy implementation plan is not a public facing document due to the sensitive nature of information contained within it, which would create a risk to the Council's security if published. It is therefore included in a separate **exempt appendix** on this agenda. However, the strategy without the implementation plan is high level enough to be a public facing document and is attached to this report at the **appendix**.

3.0 Implications

In writing this report and in putting forward recommendations, Officers have considered the following implications; Data Protection, Digital and Cyber Security, Equality and Diversity, Financial, Human Resources, Human Rights, Legal, Safeguarding, Sustainability, and Crime and Disorder and where appropriate they have made reference to these implications and added suitable expert comment where appropriate.

Background Papers and Published Documents

None.

APPENDIX

NEWARK & SHERWOOD DISTRICT COUNCIL

Cyber Security Strategy 2022-26

"Protecting residents and stakeholders data from misuse and cyber threats"

ICT & Digital Solutions

Introduction

This document sets out Newark and Sherwood 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 security commitment to both internal and external stakeholders; and emphasises the importance of security in their role.

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** – Accessing Information without authorisation
- **Attacks on Integrity** – Altering data or systems with the aim of corrupting, damaging, or destroying information
- **Attacks on Availability** – Limiting or preventing access to data and/or services

In this document we will refer specifically to Cyber security, however this will represent both cyber and information security in a wider scope.

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 commonly be referred to as information technology security.

Cyber security is important because to effectively deliver services, Newark and Sherwood 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.

NSDC transmits sensitive data across networks and to other devices while providing services. Cyber security is the discipline dedicated to protecting this information and the systems used to process or store it.

Purpose

The NSDC Digital Strategy (2021-2024) sets out NSDC's ongoing digital ambition, including how technology will be used to progress the areas of focus and priority programs set out in the Community Plan.

The council seeks to deliver its digital strategy through transforming Newark and Sherwood into a digital place, digital community, and a digital Council. The scale of transformation represents an unprecedented culture shift for the stakeholders. With this digital transformation comes an element of risk and therefore the introduction of the cyber security strategy.

Furthermore, the Cyber Security Strategy is a new strategy, introduced in response to the increasing threat from cyber criminals and several successful and high-profile cyber-attacks on public and private organisations, alongside the ambitious digital strategy.

This Strategy underpins the delivery of the Digital Strategy and the Community Plan by providing a framework for NSDC 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.

The purpose of the strategy is to give assurance to 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 our partners.

Through delivery of this strategy, we will align our ways of working with industry standards, best practices, and audit requirements, including, but not limited to, Cyber Essentials and ISO27001.

Scope of the Strategy

This strategy is intended to cover all of NSDC's information systems, assets and supply chain, the data held on them, and the services they help provide. It aims to increase cyber security for the benefit of all stakeholders; helping to protect them from cyber threats and crime.

Asset Types

The primary aim of Cyber Security is to protect the organisation's ICT and digital assets, which can be categorised as following.

Data – Any form of information stored in a digital system. Data may be stored in the council's internal systems, or by 3rd parties. The data falling under the council's remit could include resident's personal information, staff records and IT system passwords.

Software – Systems, tools and programs used by council employees, members, and residents to carry out specific tasks. These could be programs installed on devices, (Microsoft Word and Outlook), systems running on our servers (Housing Management, Printer Management), or cloud-based tools (HR/Payroll System, Council Website).

Hardware – Physical equipment used by the council to deliver digital services, including user phones and laptops, communication and audio visual devices, and server room equipment.

People – NSDC's operations are made possible by people, and their knowledge, skills and behaviours are valued as we would with more tangible assets.

Stakeholders

This strategy applies to all stakeholders for the Council's Cyber Security: Employees, Councillors, Residents, Service Users, Businesses, Partners, Suppliers.

The challenge we face as a council

Newark and Sherwood District Council is using an increasing range of technology, from endpoints to complex digital services. 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.

Horizon scanning suggests that we have multiple big issues to consider that affect Cyber Security, these include, but are not limited to:

- Global warming
- Pandemics
- Economic instability
- Political elections
- Insurrections
- Civil unrest
- Armed conflict

These global scale issues can increase the Cyber Security risk as the number of threat actors seeking political or financial gain increases. As a local authority, we can expect to see patterns in these behaviours reflected in our own experiences. For instance, local authorities have been targeted in recent years by ransomware, with the aim of extorting money from them.

Technology horizon scanning has identified emerging digital trends which should be considered in relation to Cyber Security:

- Cloud computing
- Software Defined Networking
- Zero-Trust Networks
- Internet of Things
- Artificial Intelligence
- Smart Cities
- Digital Ethics

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

The council faces several types of threat as a UK public authority; each has different behaviours, aims, likelihood and potential impact.

These threats are considered and assessed in all stages of our Cyber Security actions to ensure we are reacting appropriately to the current threat landscape.

Cyber Crime – Malicious digital activity carried out primarily for financial gain; common attacks such as phishing and ransomware are usually attributed to Cyber Crime activities

Insider Threats – The risk posed by council employees, through both intentional and unintentional acts causing loss, manipulation, or exposure of data

Physical – Digital assets are at risk of damage or loss through physical threats such as fire, flood, and power loss

Hacktivism – Politically motivated activity aimed at causing reputational damage or promoting a cause

Terrorism – Terrorist groups are increasingly carrying out cyber activities in their operations, causing major disruption to critical systems and/or enabling physical attacks

Espionage – UK government organisations are subject to intelligence gathering by foreign governments

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 are typically in the IT software, hardware, systems, and processes an organisation uses or has its data held within.

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.

Zero Days – Previously unknown technological threats and weaknesses which could be exploited by attackers and could be missed by anti-virus and monitoring tools due to never being seen before.

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.

Supply Chain – Third party products and services may be exposed or attacked, outside of the control of the organisation. The system maintenance, software updates and training is the joint responsibility of both the organisation and supplier.

Risks

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

The Council's response to Cyber Risk has seen the creation of a Cyber Incident Response Plan (CIRP).

A CIRP is formulated by an enterprise to respond to potentially catastrophic, computer-related incidents, such as viruses or hacker attacks. The CIRP includes steps to determine whether the incident originated from a malicious source — and, if so, to contain the threat and isolate the enterprise from the attacker.

Cyber risk is governed within the realm of the Corporate Information Governance Group, which assess operational risk on a 6 weekly basis and strategic risk on a quarterly basis.

Our approach, principles, and priorities

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

- Maintaining the Cyber Essentials scheme, working towards ISO27001 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.

- Utilising available technical resources to maintain and improve our Cyber Security capabilities. This could include keeping existing systems up to date with vulnerability fixes, implementing new software tools, and enrolling in training courses and materials

- Maintaining a council wide risk management framework to help preserve 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 employees and elected members understand the issues and their responsibilities.

Glossary

NSDC – Newark and Sherwood District Council

NCSC – National Cyber Security Centre. The NCSC acts as a bridge between industry and government, providing a unified source of advice, guidance, and support on cyber security, including the management of cyber security incidents.

Cyber Essentials – A self-assessed UK government scheme that helps organisations protect themselves against common cyber attacks by defining security controls and standards which should be implemented.

ISMS – Information Security Management Systems. The implementation of security controls and risk management across an organisation's operations.

ISO27001 – An industry standard for Information Security Management Systems, recognised worldwide used by organisations to protect information from security attacks. Recognised worldwide, with certification giving confidence to 3rd parties in our Cyber Security standards.