BARNSLEY METROPOLITAN BOROUGH COUNCIL

This matter is not a Key Decision within the Council's definition and has not been included in the relevant Forward Plan

Report of the
Executive Director of Core

CYBER SECURITY STRATEGY 2020 - 2021

1. Purpose of report

The purpose of this report is to provide Cabinet with an update on achievements made and to approve the Cyber Security Strategy.

2. Recommendations

It is recommended that Cabinet:

2.1 **The report is noted, and the Cyber Security Strategy approved.**

3. Introduction

3.1 The Security team have made significant progress over the last three years specifically in changing the way that cyber security is considered. The Council has changed from a reactive approach to a proactive perspective.

3.2 IT Services analyse thousands of phishing e-mails each year, taking actions where possible to protect not just individual users but the Council as a whole. They have run various phishing campaigns to challenge users and provided specific advice and support to those affected.

3.3 They utilise online services to proactively monitor the dark web looking for new data breaches which contain the details of any Council user; as soon as these are identified then specific advice is provided to those individuals, helping to protect them and indeed the wider Council.

3.4 IT Services have changed the way they procure goods and services by incorporating security into all their tenders and updated the Data Protection Impact Assessment process to ensure these important requirements are included in all system designs and builds - rather than trying to retrospectively apply security after the commissioning activity.

3.5 The Security team have run awareness events for both users and partners, keeping them fully informed of security changes that have been applied or are planned, and provided support for using new functionality.

3.6 IT Services proactively scan the network for vulnerabilities, trying to find issues before they are exploited or result in an accreditation failure. They have processes in place to proactively plan for end of life

hardware/software before it has expired; rather than waiting on health checks and subsequently fail security certifications.

3.7 IT Services now have a state-of-the-art machine learning based anti-virus system that has seen no major incidents affect users, which is a fantastic achievement.

3.8 The Security team are active members of both Government based Cyber Security Working Groups such as the WARP, MHCLG and NCSC, as well as participants in a cluster group based in Barnsley.

4. Proposal and justification

4.1 The following Cyber Security Strategy (Appendix A) was drafted to build on the existing work that has been completed and looks ahead after horizon scanning and taking advice from Central Government and Industry peers.

5. Consideration of alternative approaches

5.1 The strategy is not able to formulate an exact plan of the work required due to the ever-changing nature of Cyber Security risks to the Council. It is a vision on where IT Services sees itself and the activities envisaged based on their understanding of National security risks.

6. Implications for local people / service users

6.1 The recommendations within this report would provide the public with the reassurance that the Council's infrastructure is adequately protected with a view to sustain Council business without interruption of service.

7. Financial implications

7.1 Consultations have taken place with representatives of the Director of Finance (S151 Officer).

There are no direct financial implications associated with this report, as the purpose of the report is to update Cabinet on the achievements made and to obtain Cabinet approval to adopt the Cyber Security Strategy.

8. Employee implications

8.1 None.

9. Communications implications

9.1 To continue to communicate through Business Relationship Managers and in addition via Straight Talk and the Intranet.

10. Consultations

10.1 The Information Governance Board approved the strategy on 20th January 2020.

10.2 The Council's Senior Management Team approved this report during their meeting on 25th February 2020.

10.3 Cllr Gardiner, Cabinet Spokesperson for Core was briefed by the Head of IT (Service Management) on 6th April 2020.

11. Promoting equality, diversity, and social inclusion

11.1 A full Equalities Impact Assessment is not required.

12. Tackling the Impact of Poverty

12.1 N/A.

13. Tackling health inequalities

13.1 N/A.

14. Reduction of crime and disorder

14.1 This strategy will contribute towards the reduction in cyber crime.

15. Risk management issues

15.1 A recent LGA report stated that *"The UK cyber security threat landscape presents high risks for 'UK PLC', government, businesses and councils, requiring all actors to adopt and implement up-to-date protection in line with best practices".*

16. Health, safety, and emergency resilience issues

16.1 The Security team have undertaken several cyber security events jointly with colleagues in Emergency Planning. The Information Governance Board and IT specialists were invited to participate in several scenarios last year; these were all based around cyber attacks that could happen. These sessions acknowledged the preparedness of the Council, should such an event affect us in the future.

17. Compatibility with the European Convention on Human Rights

17.1 The proposal is fully compliant with the European Convention on Human Rights.

18. Conservation of biodiversity

18.1 N/A.

21. Background papers

21.1 Appendix A – Cyber Security Strategy

Financial Implications/Consultation

Avanda Mitchell (11.03.2020)

……..

(To be signed by the senior Financial Services officer where there are no financial implications)

APPENDIX A – CYBER SECURITY STRATEGY

Customer, Information and Digital Service

BARNSLEY
Metropolitan Borough Council

Cyber Security Strategy
2020 - 2021

Document Control

Organisation	Barnsley Metropolitan Borough Council
Title	Cyber Security Strategy – 2020 - 2021
Author	ICT Technical Security Lead
Owner	Head of IT (Service Management) Customer, Information and Digital Services
Commencement Date	February 2020
Applicable to	All users
Information/Action	For information and appropriate action
Review Date	To be reviewed 1 year from approval or earlier should changes be made to legislation or best practice guidance
Review Responsibility	Information Governance Board and SMT

Revision History

Date	Version	Author	Comments
20/12/2019	0.1	Simon Marshall	First Draft
24/12/2019	0.2	Sara Hydon	Final Draft
20/01/2020	1.0	Simon Marshall	Approved at Information Governance Board
25/02/2020	1.0	Simon Marshall	Approved at SMT

Document Distribution

This document will be distributed to the following for review and feedback prior to approval:

Name
Information Governance Board

Strategy Governance

The following table identifies who within BMBC is Accountable, Responsible, Informed or Consulted with regards to this strategy. The following definitions apply:

- **Responsible** – The person(s) responsible for developing and introducing the strategy
- **Accountable** – The person who has ultimate accountability and authority for the strategy
- **Consulted** – The person(s) or groups to be consulted prior to final strategy implementation or amendment
- **Informed** – The person(s) or groups to be informed after strategy implementation or amendment.

Responsible	Information Secuity Team Lead
Accountable	Service Director - Customer, Information and Digital Services
Consulted	Head of ICT - Service Management, Information Governance Board, SMT
Informed	All users

Introduction

This strategy sets out Barnsley Metropolitan Borough Council's plan of actions for its information and cyber security standards to protect their information systems, the data held within them, and the services they provide; from unauthorised access, harm or misuse. It is the Council's cyber security commitment to the people they represent and emphasises the importance of cyber security in the role of all Council employees, partner organisations and those whom process data on behalf of the Council.

What is Cyber Security

Cyber security is the practice of ensuring the confidentiality, integrity and availability of information and refers to the technologies, processes, and practices designed to protect the network, devices, applications and data from attack, damage, or unauthorised access.

It protects the technologies, data and information that we use in our everyday lives.

Context

The overarching vision of the Council is "to work together for a brighter future, a better Barnsley, with a thriving and vibrant economy, strong resilient communities, and citizens who achieve their potential." Achieving this vison will require innovation, continued and deeper partnership working, and careful planning based on sound evidence.

This Cyber Security Strategy supports delivery of the #DigitalFirst Programme by providing a framework for the Council to securely harness the benefits of the digital revolution for the benefit of all stakeholders. It is essential to the efficient running and evolution of a future Barnsley.

The strategy sits alongside the Council's Digital strategy and is supported by a suite of operational policies; including but not limited to (Information Security and Computer Usage Policy, System Access Control Policy and Network Security Policy).

Purpose

The Council seeks to deliver its digital strategy through transforming Barnsley into a digital place and a Digital Council, #DigitalFirst is leading on this transformational change programme. The scale and speed of transformation represents an unprecedented culture shift for the Council, residents, partners and businesses.

The Cyber Security Strategy is new, introduced in response to several successful and high-profile cyber attacks on both public and private organisations. The purpose of the strategy is to provide assurance to all stakeholders of the Council's commitment in delivering robust information security measures to protect customer and stakeholder data from misuse and cyber threats, and to safeguard privacy through increasingly secure and modern information governance and data sharing arrangements both internally and with partners.

The strategy covers all Council information systems, the data held on them, and the services they help provide, whether these systems are hosted by the Council or stored in the Cloud. It aims to increase cyber security awareness for the benefit of not just the Council but our residents, businesses, partners and stakeholders; helping to protect their data from cyber threats and crime.

The Challenge

The Council is using an increasing range of technology, from agile working with mobile phones and portable laptop / tablet devices, on premise hosting of applications, cloud-based applications and mobile apps. Much of their business is online: corresponding with residents and local partners, carrying out agile working, and Councillors 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 wider local public services such as the Hospital and ultimately has the potential to compromise National Government security. For these reasons, this strategy will align with the advice of the National Cyber Security Centre (NCSC) part of GCHQ.

The Approach

To mitigate the multiple threats faced and safeguard interests within cyberspace, the Council require a strategic approach that underpins their collective and individual actions in the digital domain over this coming year.

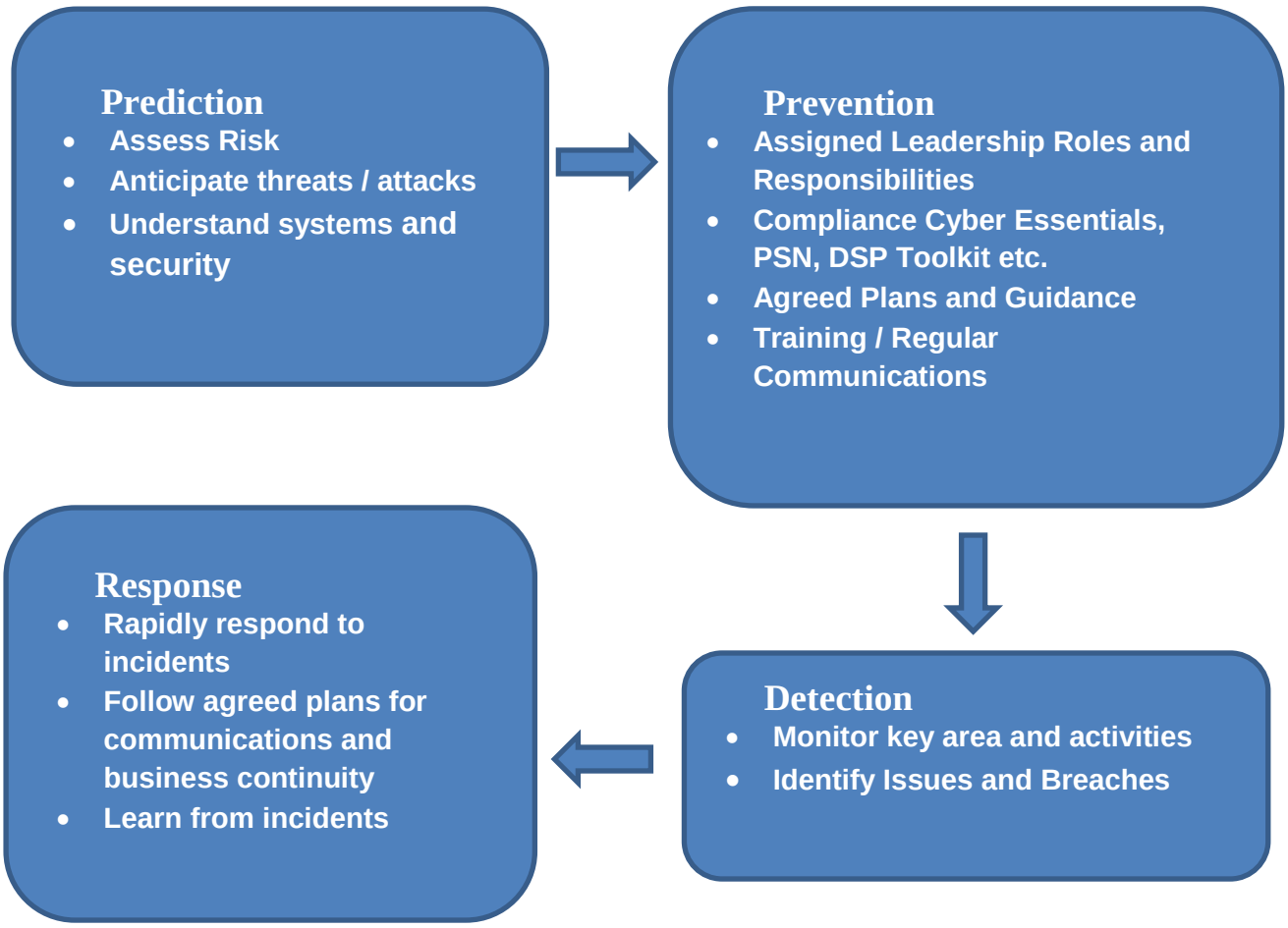
This will include:

A Cyber risk management framework to help build a risk aware culture within the Council, ensuring users understand how to identify and manage risks.

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

Applying the Cyber Essentials Plus, NCSC controls and complying with frameworks and industry good practice schemes including ISO27001 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 key steps for protecting the Council and its contractors from cyber attacks:



Success Factors

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

- ✓ Develop a defined cyber security governance process.
- ✓ Develop a specific Cyber Risk Management Framework which feeds into the IT and Corporate Risk Registers.
- ✓ Develop policies/procedures to review access on a regular basis.
- ✓ Create a cyber specific Business Continuity Management Plan and/or Incident Plan to include emergency planning for various cyber attacks.
- ✓ 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 beyond the Council.
- ✓ Develop a communication plan in the event of an incident which includes notifying internal and external stakeholders and partners.
- ✓ Set up a Playbook to have test incidents on a regular basis, to ensure reaction to the event where an incident is triggered.
- ✓ Create standard test plans with security testing as a standard.
- ✓ Reconcile current systems that are in place and last times these were reviewed (build into Enterprise Architecture principles).
- ✓ Review supplier management, assurance process of assessments of third parties.
- ✓ Explore Active Cyber Defence tools and new technologies to ensure the Council has best solutions to match the threat landscape.
- ✓ Apply the governments cyber security guidance – 10 Steps to Cyber Security.
- ✓ Provide relevant cyber security training for users and elected members.
- ✓ Apply a regular schedule of cyber exercises, within the wider cycle of multi-agency incident response and recovery exercises.
- ✓ Comply with Cyber Essentials Plus, Government Public Sector Network (PSN) Code of Connection and Payment Card Industry (PCI) standards compliance; define a clear minimum requirement for all systems used, audit trails, deletion of data etc.

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 Executive Director of Core Services. 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 officer, responsibility for safeguarding information and information systems is shared across the organisation with all users having a role to play.

The deputy is the Service Director of Customer, Information and Digital Services.

Senior Management Team (SMT)

SMT should take an overview of the Cyber Security Strategy via regular updates from the SIRO who sits on SMT, where progress and risks are reported.

Information Governance Board

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

Data Protection Officer

The DPO leads on overseeing the Council's implementation of GDPR. 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.

The deputy is the Head of IT (Service Management) within Customer, Information and Digital Services.

Security 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 Asset Owners

Information Asset Owners are responsible for all processing of personal data within their business unit. They are identified as part of the DPIA process undertaken by both Information Governance and Information Security teams.

All Council users and Elected Members

It is the responsibility of all 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 Information Security and Computer Usage Policy.

Ten Steps to Cyber Security (December 2019)

NCSC Tens Steps to Cyber Security is referenced several times throughout this strategy, here is the current executive summary of this piece of guidance supplied by the NCSC part of GCHQ.

Executive summary

This guidance is designed for organisations looking to protect themselves in cyberspace. The 10 Steps to Cyber Security was originally published in 2012 and is now used by a majority of the FTSE350. It sets out what a common cyber attack looks like and how attackers typically undertake them. Understanding the cyber environment and adopting an approach aligned with the 10 Steps is an effective means to help protect organisations from attacks.

An effective approach to cyber security starts with establishing an effective organisational risk management regime (shown at the centre of the following diagram).

This regime and the 9 steps that surround it are described below.

[Download the NCSC 10 Steps To Cyber Security infographic (PDF)]