Cabinet

15 June 2022

Cyber Security Strategy

Report of Corporate Management Team

Paul Darby, Corporate Director of Resources

Councillor Susan McDonnell, Cabinet Portfolio Holder for Digital, Customer Service and Procurement.

Electoral division(s) affected:

Countywide

Purpose of the Report

1 To highlight the importance and provide an overview of the Councils cyber security arrangements and to adopt a new corporate cyber security strategy for Durham County Council.

Executive summary

2 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. It is the practice of ensuring the confidentiality, integrity, and availability (CIA) of information.

3 Across the globe, cyber-attacks are growing in frequency and becoming more sophisticated. The increased use of the internet, furthered by the 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.

4 Information and data are vital to every part of Durham County Council's business. As we continue to deliver 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.

5 A successful cyber-attack would considerably interrupt the Councils ability to deliver services - many of which serve our most vulnerable

residents - as well as incurring large recovery costs and significant damage to our reputation.

6 To mitigate the multiple threats faced and to safeguard our interests in cyberspace, the Council needs a clearly defined and strategic approach to underpin collective and individual actions in the digital domain.

7 The Cyber Security Strategy is a new strategy, proposed in response to the increasing threats from cyber criminals and several successful and high-profile cyber-attacks on other public and private organisations.

8 The strategy aligns to the recently published Government cyber security strategy, the central aim of which is for government's critical functions to be significantly hardened to cyber-attack by 2025, with all government organisations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030.

9 It is critical that the council sets out a clear and defined approach for protecting its information systems and the data it holds to ensure the services it provides are secure and its 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.

10 It is intended that the strategy, as well as signalling a clear direction of travel, demonstrates the Councils firm commitment and the actions we will take to further establish a trusted digital environment for the organisation, our residents, and other stakeholders.

11 The strategy and the actions contained within will further strengthen and secure the Council from cyber threats by increasing security awareness throughout our workforce, investing in our systems and digital infrastructure, deterring our adversaries, and developing a wide range of responses, from basic cyber hygiene to the most sophisticated defences.

12 Cyber-attacks will continue to evolve, which is why we will continue to work at pace to stay ahead of all threats. The Cyber Security Strategy underpins and enables the Digital Strategy, which continues to ensure we will place the customer at the heart of everything we do in a changing technological landscape.

13 The new strategy has been designed to be a presented and consumed primarily as digital document and although hard copies will be available on request, this will be by exception.

14 The full document is included in Appendix 2.

Recommendation(s)

15 Cabinet is recommended to:

(a) Note the content of the report and agree the adoption of the Cyber Security Strategy

Background

16 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.

17 It is the practice of ensuring the confidentiality, integrity, and availability (CIA) of information. Attacks on confidentiality include stealing or copying personal information. Attacks on integrity seek to corrupt, damage, or destroy information or systems and the people who rely on them. Attacks on availability focus on denial of services.

18 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.

19 To deliver services, Durham County Council collects, processes, transmits, and stores large amounts of personal and sensitive data and transmits sensitive data across networks to other devices.

20 A successful cyber-attack would considerably interrupt the Councils ability to deliver services - many of which serve our most vulnerable residents - as well as incurring large recovery costs and significant damage to our reputation.

21 The time to recover can be significant. Information from known cyber-attacks show that Copeland Borough Council took over 2 years to recover services from an attack in 2017 and whilst Hackney Council's ICT services were restored after 13 months from an attack in 2020, the processing of transaction backlogs remain an issue today, two years later.

22 A robust cyber security approach enables us to protect information, the systems that are used to process or store it, ensures our services are kept up and running, and is vital in ensuring the public trusts the council with their information.

23 As we deliver 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.

24 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.

Why do we need a cyber security strategy for Durham County Council?

25 The Cyber Security Strategy is a new strategy, proposed in response to the increasing threats from cyber criminals and several successful and high-profile cyber-attacks on public and private organisations.

26 The strategy aligns to the recently published Government cyber security strategy, the central aim of which is for government's critical functions to be significantly hardened to cyber-attack by 2025, with all government organisations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030.

27 To support the achievement of this aim it is critical that the council sets out a clear and defined 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.

28 It is intended that the strategy, as well as signalling a clear direction of travel, demonstrates the Councils firm commitment and the actions we will take to further establish a trusted digital environment for the organisation, our residents, and our stakeholders.

29 We will strengthen and secure the Council 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.

30 The establishment of a Digital Security Team (DST) and partnership working both regionally and nationally shows that cyber security is taken seriously within the Council.

31 Investment in staff training has recently supported two members of the team in gaining MSc in Cyber Security, and a Cyber Security Apprentice post is part of the structure.

32 Successful bidding for available funding has allowed the deployment of a Cyber Vault, which securely holds copies of the authority's important datasets. This development was funded with £350,000 from MHCLG.

33 Cyber-attacks will continue to evolve, which is why we will continue to work at pace to stay ahead of all threats. The Cyber Security Strategy underpins and enables the Councils Digital Strategy, which continues to

ensure we will place the customer at the heart of everything we do in a changing technological landscape.

34 Through delivery of the strategy, the council 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. The council will also follow the “10 Steps to Cyber Security” framework published by the National Cyber Security Centre

35 The scope of the strategy includes all DCC’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 residents, businesses, partners, and stakeholders; helping to protect them from cyber threats and crime.

Future approach

36 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.

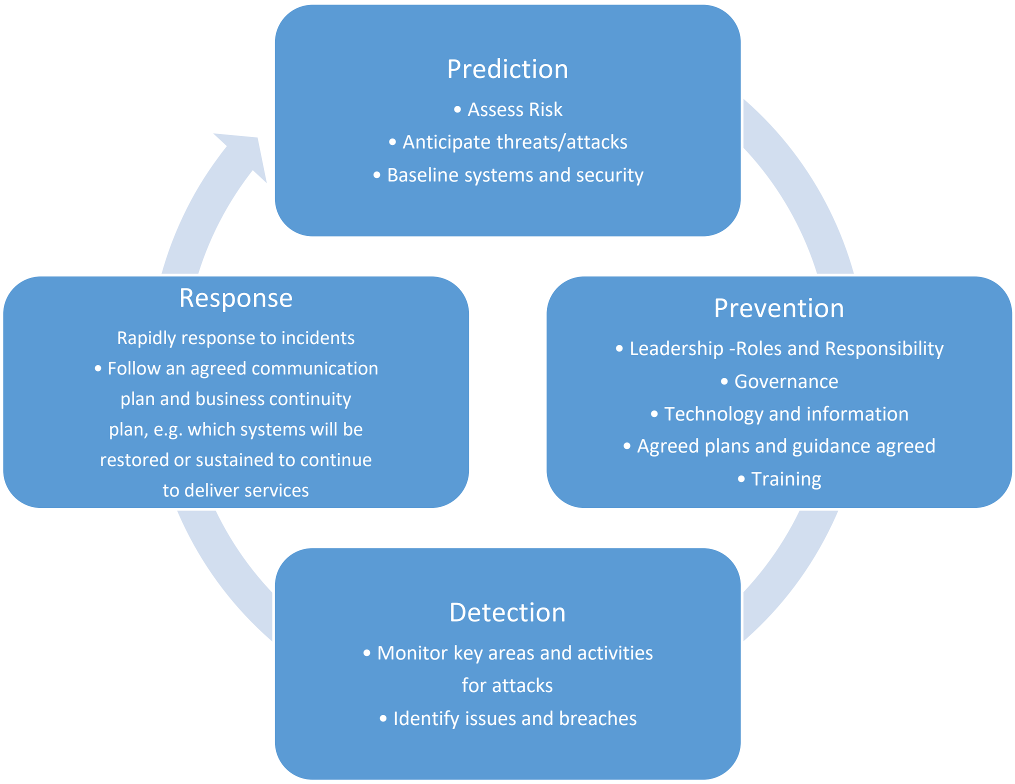
37 This will include:

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.

38 The diagram below the key steps for protecting the council and its stakeholders from cyber-attacks.



Prediction

- Assess Risk
- Anticipate threats/attacks
- Baseline systems and security

Prevention

- Leadership -Roles and Responsibility
- Governance
- Technology and information
- Agreed plans and guidance agreed
- Training

Detection

- Monitor key areas and activities for attacks
- Identify issues and breaches

Response

Rapidly response to incidents

- Follow an agreed communication plan and business continuity plan, e.g. which systems will be restored or sustained to continue to deliver services

Implementation Plan

39 To adapt to the changing landscape and achieve our strategy aims we will align with the National Cyber Security Strategy's approach to defend the Council and our residents' cyberspace, to deter our adversaries and to develop our capabilities.

40 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. This includes helping our residents, businesses, and partners in gaining the knowledge and ability to defend themselves.

41 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.

42 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 coordinated and tailored approach to risks and threats that we may encounter and mitigation of potential vulnerabilities.

43 Additionally, and to provide assurance, a range of critical success factors are outlined within the strategy.

Cyber Security Strategy Document

44 The new cyber security strategy has been designed to be viewed and consumed primarily as digital document and although hard copies will be available on request, this will be by exception. A draft of the full document is presented in Appendix 2 of this report.

45 The more detailed implementation planning documents should not be shared with other organisations and should be withheld from disclosure to Freedom of Information requests, as it may provide an advantage to cyber criminals.

Conclusion

46 The proposed cyber security strategy sets out an 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.

47 This strategy demonstrates our commitment and the key actions we will take to further establish a trusted digital environment for the Council. We will strengthen and secure the Council 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.

48 Cyber-attacks will continue to evolve, which is why we will continue to work at pace to stay ahead of all threats. The Cyber Security Strategy underpins and enables the Digital Strategy, which continues to ensure we will place the customer at the heart of everything we do in a changing technological landscape.

49 The measures outlined in this strategy will safeguard trust and confidence in the way we operate and deliver our services, supporting DCC to remain at the forefront of digital leadership.

50 The adoption of the strategy will provide a framework within which these ambitions can be delivered, and will align to the council vision, council plan and digital strategy.

Background papers

- NCSC National Cyber Security Strategy

- NCSC 10 Steps to Cyber Security
- Cyber Essentials Plus

Other useful documents

- None

Contact:	Steve Hodgson	Tel: 03000 260019

Appendix 1: Implications

Legal Implications

The Cyber Security Strategy sets out a framework for the delivery of the Council's digital security ambitions. Delivery within this framework will be managed within a range of project and programme environments, each with individual legal, contractual, and regulatory positions.

Finance

The Cyber Security Strategy sets out a framework for the delivery of the Council's digital security ambitions. Delivery within this framework will be managed within a range of project and programme environments, each with individual financing provision, monitoring, and control.

Consultation

Not applicable

Equality and Diversity / Public Sector Equality Duty

NA

Human Rights

Not applicable

Crime and Disorder

Not applicable

Staffing

Programme activity will be delivered within existing resources.

Accommodation

Not applicable

Risk

The management of cyber security is, in large part, the management of risk. The Council has robust processes in place to manage risk at various levels within the organisation.

Procurement

The Cyber Security Strategy sets out a framework for the delivery of the Council's digital security ambitions. Delivery within this framework will be managed within a range of project and programme environments, each with individual procurement provision, monitoring, and control.

Appendix 2: Cyber Security strategy document

Document is attached as Digital Services Cyber Security Strategy 2022-2025.PDF