Isle of Wight Council

Purpose: For Information

Agenda Item Introduction

Committee	**CORPORATE SCRUTINY COMMITTEE**
Date	**7 NOVEMBER 2023**
Topic	**CYBER SECURITY STRATEGY 2023-2030**

1. Background

1.1 The UK ‘Government Cyber Security Strategy 2022 – 2030’ was published last year which placed a requirement for “all government organisations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030”. It provided five advisable dimensions for consideration with regards to a public bodies’ cyber resilience.

1.2 The Cyber Security Strategy 2023-2030 will map out the dimensions providing the Isle of Wight Councils’ approach to each of these and meeting our responsibilities for resilience to cyber-attack.

1.3 The committee will review the draft strategy ahead of it being approved by the Cabinet Member for Regulatory Services, Community Protection, and ICT.

2. Focus for Scrutiny

2.1 The role of the committee is not to act as a ‘shadow Cabinet’. Its function is to ensure that the principles of decision making have been complied with:

- taking into account all relevant considerations and ignoring those which are irrelevant
- compliance with finance, contract and all other procedure rules
- due consultation and proper advice is taken, and alternative options considered before decisions are reached
- impartiality and an absence of bias or pre-determination
- any interests are properly declared
- decisions are properly recorded and published
- decisions are proportionate to the desired outcome
- respect for human rights and equality impacts
- a presumption in favour of transparency and openness
- clarity of aims and desired outcomes
- due consideration of all available options
- reasons are given for decisions

3. Outcome(s)

3.1 Does the committee support the proposed recommendations, or wish to report any comment to Cabinet?

4. Document(s) Attached

4.1 Report - Isle of Wight Council Cyber Security Strategy 2023-2030
4.2 Appendix 1 - Draft Isle of Wight Council Cyber Security Strategy 2023-2030 v0.3

Contact Point: Melanie White, Statutory Scrutiny Officer,
(01983) 821000 ext 8876, e-mail melanie.white@iow.gov.uk

Purpose: For Information

Scrutiny Committee Report

Committee	**CORPORATE SCRUTINY COMMITTEE**
Date	**7 NOVEMBER 2023**
Title	**ISLE OF WIGHT COUNCIL CYBER SECURITY STRATEGY 2023- 2030**
Report of	**CABINET MEMBER FOR REGULATORY SERVICES, COMMUNITY PROTECTION AND ICT**

5. Executive Summary

5.1 In 2022 the council approved its Digital Strategy which set out four priorities for digital improvement (Digital Island, Digital Citizen, Digital Council and Digital Intelligence). To enable these priorities to be achieved and the principles in it maintained and, to ensure that we appropriately protect the digital information we hold, it is crucial that the council has an appropriate approach to cyber security. The Digital Strategy also included the principle that the council will be "Secure by design" and this strategy expands on the statements made in that principle.

5.2 It is vital, that in this ever-changing landscape of cyber treats, the council considers all aspects in its protection of the information it holds and does this through appropriate risk-based investments in cyber security and the following of best practice governance and management processes.

5.3 In 2022 the UK government published the "Government Cyber Security Strategy 2022-2030" with all ambition that all government organisations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030, this strategy sets out how the Isle of Wight Council will approach this ambition.

6. Recommendation(s)

6.1 Scrutiny members are invited to make observations and any recommendations on the draft strategy prior to it being presented to the Cabinet Member for Regulatory Services, Community Protection, Waste and ICT for formal decision to adopt on the 19th December 2023.

7. Background

7.1 In 2022 the UK government published the “Government Cyber Security Strategy 2022-2030” with all ambition that all government organisations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030.

7.2 Since 2020 there has been a year on year global increase in Cyber Security attacks. With approximately 39% of all organisations registering an attack within 2022. This figure raises to 69% for large businesses. According to Cybersecurity Ventures, the global annual cost of cybercrime is predicted to reach $8 trillion USD in 2023. Compounding this is the rising cost of damages resulting from cybercrime, which is expected to reach $10.5 trillion by 2025.

7.3 Following consultation with the National Cyber Security Centre (NCSC), the Department for Levelling Up, Housing and Communities (DLUHC) Cyber Team and advice from the Local Government Association (LGA) Cyber Team the council has completed several cyber security based technical enhancements over the last three years. The council continues to invest in systems and solutions to close the technical gaps identified and reduce the attack surface of the organisation.

7.4 To focus resources, manage risk and achieve the national aim of being resilient to known vulnerabilities and attack methods no later than 2030, the council is basing its Cyber Security strategy on the same two complementary strategic pillars and five underlying objectives that were used by central government. Although these pillars and objectives are set by the government at a national level, they are still applicable to the council and its own cyber security at a local level.

7.5 The two Pillars are:

a) To build a strong foundation of organisational cyber security resilience; as an organisation sharing the responsibility, the council will use governance structures, mechanisms, tools, and support to manage our cyber security risks.

b) To ‘Defend as one;’ the council will work with partners and suppliers to ensure we can “present a defensive force disproportionately more powerful than the sum of its parts.”

7.6 The strategy will map out the Isle of Wight councils’ approach to each of these objectives five objectives:

a) Manage cyber security risk:
Effective cyber security risk management processes, governance and accountability enable the identification, assessment, and management of cyber security risks - at both the organisational and cross-government level.

b) Protect against cyber attack:
Understanding of cyber security risk informs the adoption of proportionate security measures with centrally developed capabilities enabling protection at scale.

c) Detect cyber security events:
Comprehensive monitoring of systems, networks and services enable cyber security events to be managed before they become incidents.

d) Minimise the impact of cyber security incidents:
Cyber security incidents are swiftly contained and assessed, enabling rapid response at scale.

e) Develop the right cyber security skills, knowledge, and culture:
Sufficient, skilled, and knowledgeable professionals fulfil all required cyber security needs - extending beyond technical cyber security experts to the breadth of professional functions that must incorporate cyber security into the services they provide - all underpinned by a cyber security culture that promotes sustainable change.

7.7 To assist in the delivery of the strategy a council wide programme board is to be established, led by Strategic Manager for ICT and Digital Services with the Cabinet Member for ICT included on the board membership. The board will take the responsibility for the development of the necessary action plan that will take forward and establish the business cases where necessary for each of the identified potential activities that underpin the five key objectives. This will result in the establishment of key projects that will form the basis of regular progress reporting.

8. Appendices Attached

8.1 Appendix 1 – Draft Isle of Wight Council Cyber Security Strategy 2023-2030 v0.3

9. Background Papers

9.1 Government Cyber Security Strategy: 2022 to 2030 - GOV.UK (www.gov.uk)
https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030

The Government Cyber Security Strategy sets out the government's approach to building a cyber resilient public sector. The strategy explains how the government will ensure that all public sector organisations will be resilient to cyber threats. The strategy's vision is to ensure that core government functions are resilient to cyber attack, strengthening the UK as a sovereign nation and cementing its authority as a democratic and responsible cyber power.

Contact Point: Roger Brown, Strategic Manager for ICT and Digital Services (SIRO), e-mail roger.brown@iow.gov.uk

Claire Shand
Strategic Director Corporate Services

Councillor Karen Lucioni
Cabinet Member for Regulatory Services, Community Protection, Waste and ICT