Isle of Wight Council

Purpose: For Decision

Delegated Decision Report

Date	**13 DECEMBER 2023**
Title	**ISLE OF WIGHT COUNCIL** **CYBER SECURITY STRATEGY 2023- 2030**
Report of	**STRATEGIC DIRECTOR OF CORPORATE SERVICES**

1. Executive Summary

1.1. 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.

1.2. 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.

1.3. 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.

2. Recommendation(s)

2.1. That the Cabinet Member for ICT approves the Isle of Wight Council Cyber Security Strategy 2023 – 2030 and the establishment of a programme board led by the Strategic Manager for ICT and Digital Services. That board will be responsible for the establishment of the associated strategy action plan in line with stated outcomes and provide the strategic oversight of business case developments and resulting project delivery.

3. Background

3.1. 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.

3.2. Since 2020 there has been a year on year global increase in Cyber Security attacks. With approximately 39 per cent of all organisations registering an attack within 2022. This figure raises to 69 per cent 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.

3.3. 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.

3.4. In June 2023, the council completed a Cyber 360 engagement with the LGA, and the report received included 39 recommendations across leadership and governance, risk, asset management, supply chain, policy and process, identity and access, data and systems, resilience, people management, response and recovery and learning and development. Those recommendations helped shape the strategy.

3.5. 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. 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.

3.6. 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."

3.7. The strategy will map out the Isle of Wight council's 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.

3.8. 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.

4. Corporate Priorities and Strategic Context

Responding to climate change and enhancing the biosphere

4.1. The council's climate change strategy is to achieve net zero emissions in its business and delivery of services by 2030; across the school estate by 2035; and an island by 2040. The use of digital technology means that the council can continue to make a significant contribution to the reduction of carbon emissions generated by our staff in the course of their work but also reduce the environmental impact in respect of power consumption, cooling and heat dissipation in our data centre with better and more efficient green solutions now available.

4.2. The Cyber Security Strategy will support the protection of the information stored in the digital solutions in the reduction of risk to the delivery of council services.

Economic Recovery and Reducing Poverty

4.3. While not affording specific strategy actions to securing improvements in the Island's economic status, the proposed strategy will support the economy by protecting the information that is held and processed by the council on behalf of the 3rd sector, partner business and our citizens. Cyber-attacks can be devastating to service delivery and have significant financial impact to all the organisations affected in the supply chain of those services.

Impact on Young People and Future Generations

4.4. The decisions the council makes now, not only affect current residents, but may have long term impacts, both positive and negative, on young people and future generations. These impacts may not immediately be apparent or may not emerge for many years or decades. Impacts will be interrelated across the various domains of young people's lives from housing, employment or training, health and the environment.

4.5. The United Nations Conventions on the Rights of the Child (UNCRC) in 1989, in particular Article 12, places a duty for children and young people to have an active voice in decision making on matters that affect them. We value the views of our young people. Incorporating coproduction and consultation with young people into our decision-making process is a robust way of ensuring young people's views are taken into consideration. Participation workers experienced in coproduction can support engagement with the Youth Council, our Island children and wider groups of young people to ensure the voice of young people is sought, heard and acted upon on important matters that will affect them.

4.6. As has been set out in this report, digital technology touches and impacts on all people in our everyday lives in some way. The protection of that digital technology through appropriate risk based cyber security is considered imperative. Cyber Security is also the responsibility of all that touch digital services so there will need to be engagement with and contribution by children and young people as the next generation of a digital society in the delivery of this strategy.

Corporate Aims

4.7. This strategy is fundamental to the delivery of the council's agreed corporate plan 2021 – 2025 and its stated priorities. With digital technology being an enabler of change and improvement, it has the potential to contribute to every part of the council's vision to work together openly and with our communities to support and sustain our economy, environment and people. Protecting the use of that technology and the information stored within its systems is critical to the delivery of all services.

5. Consultation and Engagement

5.1. This strategy is a document that has been constructed based on the council's vision and aspirations for digital services as agreed in the Digital Strategy 2022-2027. There is critical need to protect those services and the information held and processed by them. Internal engagement has been undertaken to inform its development with senior staff, corporate management team, services, internal managers and the portfolio holder for ICT.

5.2. The council engaged the Local Government Association (LGA) Cyber Team to complete a Cyber 360 Framework exercise. During this consultation a copy of the draft strategy was provided. The resulting report from the exercise contained 39 recommendations for improvements and enhancements. These recommendations have been integrated into the final version.

5.3. The strategy also affords ongoing opportunity for anyone who wishes to provide feedback or engage with the council on this strategy and its development.

6. Scrutiny Committee

6.1. Cyber Security was considered at a Corporate Scrutiny Committee informal review meeting on the 6th September 2023. The view of the panel was positive and supported the current direction of travel and the creation of this strategy.

6.2. The Cyber Security Strategy was considered at a Corporate Scrutiny Committee meeting on the 7th November 2023. The Cabinet Member for Regulatory Services, Community Protection, Waste and ICT invited all committee members to make observations and any recommendations on the draft strategy prior to it being presented for formal adoption.

7. Financial / Budget Implications

7.1. Each of the strategy pillars and objectives set out planned actions and activities that will underpin the delivery of the strategy aim and desired outcomes. Many of the activities can and will be established as work programmes within service planning that can be delivered within existing budgets and resources. Where projects require more detailed assessment for viability and additional resourcing, these will be subject to business case development in conjunction with budget accountants for consideration and decision-making purposes.

8. Legal Implications

8.1. There are no specific legal implications that need to be considered in the approval of the proposed Cyber Security Strategy although there will be many aspects of legislation that will need to be taken account of for compliance in its delivery. This will include the Data Protection Act 2018 in respect of the council's obligations for information security and governance of the information we are protecting.

9. Equality And Diversity

9.1. The council as a public body is required to meet its statutory obligations under the Equality Act 2010 to have due regard to eliminate unlawful discrimination, promote equal opportunities between people from different groups and to foster good relations between people who share a protected characteristic and people who do not share it. The protected characteristics are: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

9.2. It is recognised that it will be essential to assess equality impacts with any specific cyber security development projects that derive from the delivery of the strategy once approved. Engagement with representative groups will be a key factor for the consideration of any impact as will be the conducting of formal equality impact assessments as part of the business case developments.

10. Property Implications

10.1. There are no property implications in the approval and delivery of the strategy, the Isle of Wight council adopts an agile workforce and the development of the action plan will not impact on future property planning.

11. Options

11.1. Option 1: To approve the Isle of Wight Council Cyber Security Strategy 2023 – 2030 and establish a programme board led by the portfolio holder for ICT. That board will be responsible for the establishment of the associated strategy action plan in line with stated outcomes and provide the strategic oversight of business case developments and resulting project delivery.

11.2. Option 2: To refer the Isle of Wight Council Cyber Security Strategy 2023 – 2030 for further consideration.

12. Risk Management

12.1. The proposed strategy sets out a pair of pillars and five objectives and is driven to ensure that risk is managed based on known priorities for technology developments and improvements for cyber security delivery and in response to an ever-changing landscape of vulnerabilities and threat methods. It also acknowledges the need to remain flexible to allow for emerging developments and needs that arise and for active engagement with those affected by what we do as it is impossible to prescribe everything that needs to be done. The establishment of a programme board to oversee the delivery of the strategy and provide a clear steer to the priorities and projects required will significantly contribute to success.

12.2. There are capacity and financial risks associated with the approval of this strategy as much of the work programme required is yet to be determined. The preparation phase for any piece of new work cannot be underestimated. By taking a robust approach to the development of business cases where required to ascertain viability, funding and resource requirements balanced against risk to service delivery and the current threat level from the vulnerability being mitigated we can ensure that the limited resources are focused on risk mitigation in the correct areas.

12.3. The strategy lays out a requirement for continued engagement with external third-party experts these engagement activities will assist in establishing the current risk levels and potential changes required to systems, governance practices and management processes.

13. Evaluation

13.1. It is essential that the council continues to exploit available technologies to secure service improvements, efficiencies and ultimately the longer-term sustainability of public services for the Island. The proposed strategy sets out the key areas of action that will contribute to the risk reduction and protection of the council's stated priorities as set out within its corporate plan. It recognises that whilst digital technology plays an essential part of our everyday lives it is necessary to mitigate risk and be resilient to the known vulnerabilities and attack methods being used at any particular time.

13.2. The strategy also sets out a framework through which pillars and objectives will be at the heart of everything we do to make sure that when designing, deciding and delivering cyber security solutions, management process and governance frameworks, that they are fit for purpose and will stand us in good stead for the future.

13.3. With an ever-changing world of technology, the vulnerabilities and attack methods change with it. These continue to evolve at speed, this strategy therefore cannot be a definitive list or programme of work but instead sets out the known objectives and dimensions which must be considered when approaching the risk management of Cyber security. It is important to remember therefore that the strategy will remain flexible and adaptable to changing needs and priorities throughout its lifecycle, but which all will be based on evidence-based decision making through effective planning and full consideration of any investments required and active engagement with those affected by our work.

14. Appendices Attached

14.1. Appendix 1 – Isle of Wight Council Cyber Security Strategy 2023-2030

15. Background Papers

15.1. Government Cyber Security Strategy: 2022 to 2030 - GOV.UK (www.gov.uk)

15.2. 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