Item: 15

Statutory General Meeting of the Council: 16 May 2022.

Cyber Resilience.

Report by Corporate Director for Strategy, Performance and Business Solutions.

1. Purpose of Report

To appoint an elected member with specific responsibility for cyber resilience.

2. Recommendations

The Council is invited to note:

2.1.

That, in late 2015, the Scottish Government produced a generic Cyber Resilience Strategy for Scotland, with the aim of increasing awareness and focus on protection.

2.2.

That, in November 2017, the Public Sector Action Plan on Cyber Resilience for Scotland, developed jointly by the Scottish Government and the National Cyber Resilience Leaders' Board, was launched and represented a significant step towards establishing a wider culture of cyber resilience in Scotland.

2.3.

That, in March 2018, the Council resolved to appoint a named elected member in relation to the Cyber Resilience Strategy and Action Plan, with the member being Councillor Steven Heddle.

2.4.

The proposal that the Council appoint an elected member with specific responsibility for cyber resilience and that the appointment be for the term of office as councillor, namely for the period May 2022 to May 2027.

It is recommended:

2.5.

That a member be appointed with specific responsibility for cyber resilience.

3. Background

3.1.

Cyber resilience means being able to prepare for, withstand and rapidly recover and learn from, deliberate attacks or accidental events that have a disruptive effect on interconnected technologies. Cyber security is a key element of being resilient, but people and organisations must recognise that being safe online goes far beyond just technical measures. Building good understanding of cyber risks and threats helps organisations to take appropriate measures to stay safe and get the most from working online.

3.2.

In late 2015, the Scottish Government produced a generic Cyber Resilience Strategy for Scotland with the aim of increasing awareness and focus on protection.

3.3.

There have been several high-profile cyber-attacks on public sector bodies:

- The ‘wannacry’ ransomware attack which occurred in May 2017 and impacted (in the UK) the National Health Service. The response to this led to the launch of the Scottish Government’s Public Sector Action Plan.
- Redcar and Cleveland Council suffered a major ransomware attack in February 2020.
- Hackney Council suffered a cyberattack in October 2020 leading to confidential documents being posted on-line by hackers.
- Gloucester Council suffered an attack on its online revenue and benefits, planning and customer services systems in December 2021 and was linked to Russian hackers.
- Dundee and Angus College suffered a cyberattack in 2020 that wiped data from their systems.
- In December 2020, SEPA was subject to a significant cyber-attack affecting its contact centre, internal systems, processes and communications.
- On 19 April 2022, the Scottish Wide Area Network (SWAN) was targeted by a “denial of service” cyberattack, which disrupted Internet Access for Councils – including Orkney Islands Council – as a customer of SWAN.

3.4.

In November 2017, the Public Sector Action Plan on Cyber Resilience for Scotland, developed jointly by the Scottish Government and the National Cyber Resilience Leaders' Board, was launched. This document represented a significant step towards establishing a wider culture of cyber resilience in Scotland.

3.5.

The Public Sector Action Plan on Cyber Resilience for Scotland recognises that many Scottish public bodies already have sound standards of cyber security in place. However, the wider aim of the Action Plan is for the Scottish public sector to become an exemplar in this field over time, implementing a common approach to cyber resilience and offering greater assurance to those who use digital public services.

4. Appointment of Member

4.1.

On 20 February 2018, the Policy and Resources Committee considered the requirements of the Cyber Resilience Strategy for Scotland, noting that the Scottish Government had asked public bodies to achieve three key requirements to the timelines, as follows:

- Action 1 – Have in place minimum cyber risk governance arrangements by the end of June 2018.
- Action 2 – Ensure that public bodies that manage their own networks become active members of the National Cyber Security Centre's Cybersecurity Information Sharing Partnership, in order to promote sharing of cyber threat intelligence by the end of June 2018.
- Action 3 – Achieve Cyber Essentials / Plus cyber security certification on an appropriate basis by the end of October 2018. To support this, funding will be made available for all public bodies to undergo Cyber Essentials "pre-assessments" by the end of March 2018.

4.2.

Action 1 placed a requirement on all Scottish public bodies to have in place a Board-level commitment to manage the risks arising from the cyber threat. This is to recognise that the cyber threat is a business risk, one of many that need to be managed daily by all public bodies. Alongside the requirement for a named Board member, there is also the requirement for regular Board-level consideration of the cyber threat and the arrangements the organisation has in place to manage risks arising from it.

4.3.

The Corporate Director for Neighbourhood Services and Infrastructure is the nominated Senior Officer with lead responsibility to manage the risks arising from the cyber threat. The Information Services Programme Board, which meets quarterly, receives reports from the Corporate Director on cyber security and how any risks are being mitigated.

4.4.

A named elected member, who works with the lead officer to ensure there is good governance and oversight on this issue, was appointed, namely Councillor Steven Heddle.

4.5.

On 9 June 2020, the Information Services Programme Board agreed that, because the Council was continuing to meet the cyber security standards required to be part of the Public Service Network, it would not seek continued Cyber Essentials Plus accreditation. Regardless, the principle of having a named elected member who works with the lead officer to ensure there is good governance and oversight on this issue remains and therefore a nominee is sought.

4.6.

It is proposed that the Council appoint an elected member with specific responsibility for cyber resilience and that the appointment be for the term of office as councillor, namely for the period May 2022 to May 2027.

5. Corporate Governance

This report relates to the Council complying with governance and procedural issues and therefore does not directly support and contribute to improved outcomes for communities as outlined in the Council Plan and the Local Outcomes Improvement Plan.

6. Financial Implications

Although there are no direct financial implications arising from the recommendations of this report, cyber risks have become of greater significance to the Council as more services have an online presence for some part of the service. The risk of a cyber-attack impacting on Council Services has also increased as the number and sophistication of malicious software attacks has also increased.

7. Legal Aspects

There are no direct legal implications arising from the recommendations contained in this report.

8. Contact Officer

Karen Greaves, Corporate Director for Strategy, Performance and Business Solutions, extension 2202, Email karen.greaves@orkney.gov.uk