Item: 9

Policy and Resources Committee: 20 February 2018.

Cyber Resilience Strategy for Scotland.

Report by Executive Director of Corporate Services.

1. Purpose of Report

To explain the requirements of the Cyber Resilience Strategy for Scotland, and to seek the appointment of an elected member lead for this Strategy and the Orkney Islands Council response.

2. Recommendations

The Committee 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 represents a significant step towards establishing a wider culture of cyber resilience in Scotland.

2.3.

The requirements of the Cyber Resilience Strategy and Action Plan and the cyber risk governance arrangements, as outlined in section 5 of this report.

It is recommended:

2.4.

That an elected member be appointed as the named elected member in relation to the Cyber Resilience Strategy and Action Plan.

3. Policy Aspects

The proposals in this report support the undernoted Council values:

- Promoting Survival – to support our communities.
- Working Together – to overcome issues more effectively through partnership working.

- Working to Provide Better Services – to improve the planning and delivery of services.

4. Background

4.1.

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 cyber resilient people and organisations recognise that being safe online goes far beyond just technical measures. By building understanding of cyber risks and threats, they take the appropriate measures to stay safe and get the most from working online.

4.2.

In late 2015, the Scottish Government produced a generic Cyber Resilience Strategy for Scotland with the aim of increasing awareness and focus on protection. The report is available here http://www.gov.scot/Resource/0048/00489206.pdf. There have also, since that date, been several high profile cyber-attacks, the most recent being the 'wannacry' ransomware attack in May 2017 which was a worldwide attack, and identified a high level of vulnerability especially within the National Health Service.

4.3.

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 is available here http://www.gov.scot/Resource/0052/00527399.pdf and represents a significant step towards establishing a wider culture of cyber resilience in Scotland.

4.4.

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. Delivery of the Action Plan will be coordinated and led by the Scottish Government's Cyber Resilience Unit, working in partnership with the National Cyber Resilience Leaders' Board and Scottish public bodies.

5. Key Actions and Local Response

5.1.

The Scottish Government has asked public bodies to achieve the following three key requirements to the following timelines. The Council's response to each is noted below each action.

5.2.

Action 1 – Have in place minimum cyber risk governance arrangements by the end of June 2018.

5.2.1.

This places 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.

5.2.2.

To meet this requirement, the Executive Director of Corporate Services is the nominated Senior Officer with lead responsibility to manage the risks arising from the cyber threat. The existing Information Services Programme Board, which meets quarterly, will receive reports from the Executive Director of Corporate Services on progress being made against the Public Sector Action Plan and how any risks are being mitigated.

5.2.3.

In addition to the officer lead, it is recommended there be a named elected member for this matter, who will work with the Executive Director for Corporate Services to ensure there is good governance and oversight on this issue. Where appropriate, reports will be brought to elected members through the Asset Management Sub-committee. Councillor Steven Heddle has been approached, as a member of the Asset Management Sub-committee and due to his experience in this area, including being the Convention of Scottish Local Authorities' spokesperson for the environment and economy, and has confirmed that he is willing to be considered.

5.3.

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.

5.3.1.

This is already complete as the Council has been an active and participating member of the Cybersecurity Information Sharing Partnership since 2015.

5.4.

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.

5.4.1.

Work is already underway within the IT team to compete this action within the designated timescale. Initially the submission will be for the Cyber Essentials certification, with Cyber Plus to follow in 2019.

5.4.2.

The first step is an IT Health Check. The results from this will assist with completion of the pre-assessment stage, and the external contractor who will carry this out has been identified. The Health Check was carried out on 6 February 2018 and the results are awaited. The submission for certification is on track to be submitted by the end of March 2018.

5.4.3.

Grant funding of £1,000 has been made available to carry out the pre-assessment stage, and an application for this is underway.

6. Financial Implications

6.1.

The Convention of Scottish Local Authorities has identified that the assessment regarding the achievement of Cyber Essentials certification may well identify further actions which will require additional funding. Unavoidable pressures have been identified through discussions at the Senior Management Team and information provided that these will be clarified in due course.

6.2.

In terms of staffing resource, at this time the amount of additional work required to meet the actions above is being considered. The IT team has one officer who has a lead on Information Security and it is thought unlikely that this certification work can be absorbed within their current work programme. If this is the case then a temporary resource would be required to support this work, which would have to be progressed in line with the usual Human Resources procedures and guidance and if adequate budget for the certification work referred to at 6.1 above can be identified.

6.3.

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 Officers

Gillian Morrison, Executive Director of Corporate Services, extension 2103, Email gillian.morrison@orkney.gov.uk.

Hayley Green, Head of IT and Facilities, extension 2309, Email hayley.green@orkney.gov.uk.

Tony Whenman, Information Security Officer, extension 2157, Email tony.whenman@orkney.gov.uk.