Governance and Audit Committee

Item **11**

19 October 2021

Report of	**Dan Gascoyne, Chief Operating Officer & Senior Information Risk Owner (SIRO)**	**Author**	**Wayne Murray** ☎ 07966 236074
Title	**Briefing Note: Assurance on Council's Cyber Security provision**		
Wards affected	Not applicable		

1. Executive Summary

1.1 This report provides an overview as to how Colchester Borough Council ensures appropriate levels of Cyber Security are maintained and monitored.

2. Recommended Decision

2.1 The Committee are invited to note the contents of the report

3. Reason for Recommended Decision

3.1 At its meeting in June 2021 the Committee noted the threat of a successful cyber security attack was an increasing risk to the Council and requested that a report be presented to the Committee to reassure Councillors and members of the public that all necessary steps were being taken to mitigate this risk

4. Alternative Options

4.1 Not applicable

5. Background Information

5.1 Colchester Borough Council's ICT (Information and Communication Technology) Team are responsible for providing the technical ICT services (including Networking, Infrastructure, Information Governance and Cyber Security) to Colchester Borough Homes, CCHL (Colchester Commercial Holdings Limited) Ltd, and the Council. They are tasked with providing a robust infrastructure that allows staff and Councillors to fulfil their roles and responsibilities whilst ensuring all Council data is secure and only accessible to the relevant people. This includes maintenance of all systems and related servers, networks, end point devices such as laptops and mobile phones as well as user and data permissions and access

5.2 The Council currently has 862 E3 licenced users (these are full time staff that require full access such as Outlook, SharePoint, Office365 applications) and 565 F3 licenced users (these are full time or casual staff that require limited applications such as email only). This is a total of 1,427 licence user accounts that ICT manage

5.3 The Council has adopted a modern, cloud first approach to technology that ensures infrastructure and devices are always up to date and as secure as possible.

5.4 The risk of the Council suffering a successful cyber-attack is captured as a significant risk on the Council's Corporate Risk Register with mitigation and controls defined as ensuring policies and protocols are subject to ongoing review, and ensuring training is in place for staff and Members.

5.5 The Council's approach to keeping our information and systems secure is based upon guidance from the National Cyber Security Centre (NCSC) and the 5 key factors of cyber security:

- Infrastructure
- Analysis
- Alerting
- Actions
- Awareness

5.6 The Council works closely with other organisations and bodies such as NCSC, Microsoft, the local Warning, Advice and Reporting Point (WARP), Essex Online Partnership and more, to share best practice and gain insight and early warning about cyber threats and trends.

5.7 Cyber security and Network resilience are areas that are tested both externally as part of our annual penetration testing, and internally as part of the Council's corporate audit plan. There are no outstanding urgent recommendations from audits or from penetration testing.

5.8 The Network Resilience Audit was completed by our Internal Auditors in April 2021 and the high-level report was shared with this Committee. Good practice was identified in the Audit Report and the overall assurance level was Reasonable Assurance (the second highest level of assurance). The Key findings and Management Action Plan are monitored regularly, and actions are underway.

5.9 The Cyber Maturity Audit by our Internal Auditors is currently in progress and builds upon the Network Resilience Audit previously undertaken.

5.9 All staff and Members are required to complete mandatory Data Protection training annually and this year's training included an element on Cyber Security best practice and hints and tips around how to spot a cyber threat. The most recent round of training has seen 99% completion by staff and 2/3rds of Members have completed it so far.

5.10 All Members were invited to a briefing and training session recently that provided further information on the level of risk to the Council, the Council's approach to prevention and to mitigation of issues, and the mechanisms in place to help prevent or respond to cyber incidents

6. Equality, Diversity and Human Rights implications

6.1 None identified

7. Strategic Plan References

7.1 Secure, resilient, and robust ICT systems underpin our service delivery, ensure that data is protected, and enable delivery of our Strategic Objectives

8. Consultation

8.1 Not applicable

9. Publicity Considerations

9.1 Not applicable

10. Financial implications

10.1 Not applicable

11. Health, Wellbeing and Community Safety Implications

11.1 Not applicable

12. Health and Safety Implications

12.1 Not applicable

13. Risk Management Implications

13.1 The risk of a cyber breach is recognised as a significant threat on the Corporate Risk Register.

14. Environmental and Sustainability Implications

14.1 Not applicable

Appendices

None

Background Papers

None