Report to:	Performance, Assets and Strategy Overview and Scrutiny Committee – 3 March 2026
Lead Cabinet Member:	Councillor Simon Smith, Cabinet Member for Finance and Resources
Lead Officer:	Simon Oliver, Chief Digital and Information Officer

Cybersecurity Update

Executive Summary

1. Cybersecurity remains a key risk for the Council. It is rated Amber on the Corporate Risk Register and is therefore reported individually within the Quarterly Performance Report.

2. Several activities have been instigated following the commencement of the Chief Digital and Information Officer (CDIO) role in December 2024.

3. The new approach to Risk Management enables a simpler approach to identifying risks and ownership.

4. The new approach to Risk Mitigation enables a simpler approach to identifying the benefit of such activity and investments.

5. Investments in new capabilities have had a positive impact, which will be built upon during 2026.

Details

6. The Shared Services nature of the Council's ICT infrastructure and Operational IT approach means that any of the 3C Partner Council's approach to Cybersecurity is only as strong as the weakest Partner. As a result, a joint approach to ownership and mitigation is essential.

7. Ensuring visibility and ownership of risks and mitigations is essential. It cannot be ascertained that all risks are to be managed by "the ICT Service", or that risk mitigation decisions can be left to Service Managers. Effective risk ownership has been a key area for improvement in 2025 and will continue into 2026.

8. The National Cyber Security Centre has produced sector-wide guidance on the threat landscape for councils, with risks broken down into the 6 key areas:

    a. Ransomware

b. Supply Chain Attack

c. Privileged Access Management

d. Known Vulnerabilities

e. Unsupported Software

f. Staff Awareness

9. The CDIO has recently sought to align all activity under three new headings to provide Members with greater detail as to the purpose of activities, where the technical nature of the changes may not be immediately apparent to those without a technical background:

    a. PREVENT: Activities that seek to prevent a Cybersecurity incident/breach.

    b. REDUCE: Activities that reduce the impact of an incident/breach.

    c. RECOVER: Activities that will improve the ability of the Council to restore Services after an incident/breach.

10. The Council's preparedness is underpinned by an approach which addresses risks and mitigations across the following considerations;

    a. PEOPLE: Implementing training and controls which are aligned with the wider users of the IT and Digital services, so they can work safely and within policy. Where process and controls are not possible, or users can operate outside of these due to operational reasons, the risks and 'best practice' approaches are known through training. Knowledge of which processes are available to utilise is essential. Ensure colleagues are comfortable raising potential breaches, and how, and are not fearful of consequences.

    b. PROCESS: Ensuring that 'best practice' and statutory obligations are met through processes which align to these and prevent activity which would pose a risk. These are updated to stay aligned with the changing threat, legislative and regulatory landscapes.

    c. SYSTEMS/TECHNOLOGY: Ensuring that the systems and technologies used are up to date and align with legislative requirements and adhere to policies and approved processes. Seeking to remove utilisation of non-approved solutions and ensure any risks regarding solutions in use are known, monitored, and have mitigation plans.

11. The ownership of the risks and mitigations regarding Cybersecurity has been reviewed to ensure that each individual risk has an identified owner, agreed mitigation, and an agreed mitigation delivery date. The ownership of risks has been updated to reflect the following responsibilities:

    a. Senior Information Risk Owner (SIRO): The Director-level Officer who is responsible for keeping the Leadership informed on all risks and ensuring

that risks are responded to in line with the Corporate Plan. The SIRO may accept risks on behalf of the Council via formal exception reporting.

b. Chief Digital and Information Officer: Responsible for strategic advice to the 3C Partner Councils, regarding the current state and optimal future state for Cybersecurity. Acting as the Director lead of technical mitigations within the 3C Shared Service.

c. Data Protection Officer: A statutory role under GDPR, responsible for advising the SIROs on Information Risks and ensuring that risks in relation to personal data are correctly identified and escalated in line with appropriate governance routes. Responsible for ensuring adherence to the organisational aspects of cybersecurity, such as policies and training, and ownership of the Cybersecurity Risk Register.

d. Cyber Security Lead Officer: Responsible for the technical implementation of cyber security measures and ensuring the council's adherence to standards set by Government, such as PSN, and other 'best practice' frameworks adopted by the Council.

12. Cybersecurity oversight is undertaken by several governance boards:

a. Information Assurance Board: A quarterly board chaired by the 3C Partner Council SIROs, responsible for oversight of Information Security risks, approval of policies relating to personal data and information security and a strategic approach to information risks.

b. ICT Software Review Group: An operational meeting to ensure that new software adheres to appropriate standards of compliance

c. ICT Change Approval Board: An Internal ICT operational meeting where changes are approved to ensure consistency and resilience

13. During 2025, the 3C ICT Service has adopted a new approach to policies by ensuring alignment with the ISO27001 framework. This work is on schedule for completion by April 2026.

14. During 2025, the 3C ICT Service has adopted a new approach to the Information Security Risk Register by ensuring alignment with the ISO27005 framework. This work is ongoing.

15. In addition, several other activities were undertaken during 2025 that have contributed to the maturing approach to Cybersecurity;

Workstream	**Implementation**	**Purpose**	**Type**
ISO27005 Standard Adoption	April 2025	PREVENT	Processes
Phishing Simulations	Quarterly Ongoing	PREVENT	People
E5 Adoption	October 2025	PREVENT	Systems

Microsoft Security Workshops	October – December 2025	PREVENT	Systems
CyberSecurity Exercise	June 2025	REDUCE/RECOVER	Processes
Cyber Essentials Audit	June 2025	PREVENT	Processes
ISO27001 Policy Review	April 2025	PREVENT	Processes
SIRO Training	August 2025	REDUCE	People
Trend Review	December 2025	PREVENT	Systems
CIS 5.0 Benchmark	September 2025	PREVENT	Systems
Staff Information Security Training	Ongoing	PREVENT	People
Applications Rationalisation	December 2025	REDUCE	Processes
OAuth Application Control	November 2025	REDUCE	Systems
Multi Factor Authentication	January2026	PREVENT	Systems

16. The investment made to adopt Microsoft E5 licensing has led to several new capabilities being made available, and work continues to adopt the new capabilities and remove legacy systems. This has been a significant undertaking to date.

17. While starting with a solid foundation of cybersecurity systems in place, the progress made during 2025 has been significant.

18. Although 2025 activity has been focused on Systems and Processes, the most important improvement has been the changes implemented towards the PEOPLE aspect. With SIRO training in place to support leadership on Cyber Security, the ongoing phishing and mandatory training have led to a sentiment among staff where 85% are confident in ICT's ability to protect and respond to cyber threats. This confidence does not preclude continued vigilance and awareness being advocated with staff.

19. The CDIO continues to champion Cybersecurity improvements, and these will continue throughout 2026.

20. Further implementation of the benefits of the investment into the Microsoft E5 capabilities will be made, which will provide improved centralised insight into technical risks, potential breach activity, non-conformant user activity, assessments against ‘best practice’ configurations, anti-virus, etc.

21. The investment into the E5 Capabilities also extends into Information Management, and will enable improved Data Retention, Data Loss Prevention (document sharing and through external AI adoption), and GDPR adherence.

22. At the time of writing a budget bid has been recommended to Full Council to move to an external Security Operations Centre (SOC) approach via an external

Managed Service. This will enable the Council to benefit from a 24/7/365 service that continuously monitors potential vulnerabilities and breaches. In the event of an incident, the capability and capacity needed to act and remediate will be immediately available. This will be a significant improvement, enabled by adopting Microsoft E5 licensing.

Report Author:

Simon Oliver - Chief Digital and Information Officer