BRIEFING REPORT

Cyber Security Risk Response

1. BACKGROUND

The Council recognises the threat of a major attack on our systems and data to be one of our highest scoring risks on our risk logs. This position is consistent with the national risk assessment, the 2025 National Risk Register - National Risk Register - 2025 edition includes cyber attacks on infrastructure and underlines the importance of protecting our systems and data across critical services supporting our residents.

The National Cyber Security Centre (NCSC) described the threats faced by organisations in the UK in their 2025 annual report - It's time to act - NCSC Annual Review 2025. The threats are varied in nature and origination, but the evidence is clear that significant attacks are increasing and that it requires a management response not just a technical one to effectively counter them.

The systems and data that the Council relies upon to deliver services to our residents were regularly attacked during the last year. The defences we have put in place provide good protection to avoid major issues and we didn't suffer systems unavailability or data theft in 2025. It is however clear that the sophistication of attacks is continuing to rise and as the NCSC describe, organisations should prepare themselves to deal with a successful cyber attack as well as strengthening their defences to help avoid being attacked.

2. RESPONSE

The Council has recognised and accepted the position and responded with the creation of a Cyber and Information Security Board comprising resources from both PCC and Delt with expertise in both the threats we face and how to mitigate them. The Board also includes representation from Devon Audit Partnership in order that they have first-hand understanding of the Council's response to our cyber threat and can contribute their expertise. This board meets monthly and maintains a detailed risk log which is updated regularly to ensure the Council is learning from the experience of others as well as the attacks on our systems.

The board have developed a detailed risk log breaking down the different types of threats the Council faces to our systems and data. The risk log is scored and our highest scoring risks all now have active mitigations in place, including where required investment to support he implementation of the mitigation.

Note: despite the investment and organisation that has gone into the Council's cyber defences over the last 5 years our risk score has broadly stayed consistent. This is because the sophistication of the threat has risen over the same period. Our improved defences have resulted (broadly) in the Council holding our position regarding our exposure to the threat, rather than reduced our likelihood or the impact of an attack.

The board also produce a quarterly report for CMT providing them with details of important cyber incidents occurring in the last 3 months as well as the progress made in mitigating risks.

3. AUDIT FINDINGS

This report provides the Audit and Governance Committee with a response to three specific areas of audit findings that required improvement when they were raised. These are detailed in the

spreadsheets used to track the audit recommendations. For clarity the report below summarises the audit findings and the actions taken in response:

Action/audit finding	Response to date	Remaining action
The IT/Cyber Risk Management Policy is overdue for review and has elements that could be strengthened	The Council's Cyber Risk Management policy OR04 has been updated and published on Staffroom ORO4. The detailed recommendations made in the audit finding have been included in the new policy	No further action required
Lack of defined roles and responsibilities for IT Risk Management	OR04 sets out the management roles and responsibilities around cyber security and can be accessed here OR04	No further action required
The known weaknesses in the end-to-end user management processes should be identified at the Cyber Board and the risks appropriately managed. The creation of a risk register to provide transparency and a means of governing the associated risks should be considered. Furthermore, the commencing of a workstream/ project to make the necessary improvements would provide a timeline around which some impetus could be achieved.	The Cyber and Information Governance Board review the Council's risk register on a monthly basis, this register includes risk around user management. The specific risks around account management was mitigated manually whilst the new payroll systems (ITrent) was introduced last year. The Council and Delt are now working on proposals to automate more of this process	Finalise the design and investment requirements for the automated solution to user management. Implement automation using the principle of least privilege (where the minimum permissions and access rights necessary to perform a specific function are provided, and nothing more). Target date: end September 2026