Committee Report

PURPOSE: Final Decision Report

KEY OR NON-KEY DECISION: Key decision over £500k

COMMITTEE: Strategy and Resources Committee

DATE: 16 September 2024

TITLE: **Cyber Security Maturity Assessment and procurement of a managed service**

Ward(s): None

Officer presenting the report: Tim Borrett **Job title:** Director: Policy, Strategy and Digital

Committee Chair: Cllr Tony Dyer

Executive Director lead: Paul Martin, Chief Executive Officer

Proposal origin: BCC Staff

Purpose of Report:

1. This report informs Committee of the outcomes of an independent Cyber Security Maturity Assessment and seeks approval to procure and award a contract for a Managed Extended Defence and Response service. This is a third-party provision of 24/7 cyber security monitoring and active defence against cyber-attacks. This report also proposes a small in-house staffing increase to ensure the council can further strengthen cyber security in line with its risk appetite.

Evidence Base:

1. As highlighted by the Local Government Association's Cyber 360 Framework, recent years have seen a significant rise in cyber security related incidents affecting the public sector across the globe, as well as a marked increase in the number of attacks targeting national infrastructure, including local government. Incidents are becoming more frequent and sophisticated, and appear to be carried out by advanced, persistent threat actors that have access to considerable resources. It is therefore vital that the council has the knowledge, means and support to defend against cyber-attacks.

2. In recent years the council has invested significantly in its IT and Digital infrastructure and estate, moving to more modern, secure solutions. These have subsequently been optimised and configured alongside third-party security professionals as part of the council's drive to achieve the National Cyber Security Centre (NCSC) 'Better' standard for cyber.

3. An independent review undertaken in July 2024 assessed the council's cyber maturity against the National Institute of Standards and Technology (NIST) Cyber Security Framework. The results of this assessment are detailed in Exempt Appendix Ei.

4. With many of the council's IT and digital projects which address its higher risks now nearing completion, and with the benefit of a completed cyber maturity assessment and Board-agreed risk appetite of 'Cautious', there is now greater opportunity and impetus to further strengthen cyber security. For a 'Cautious' risk appetite the target risk score within the council's Risk Management Assurance Policy should be 12 (medium), and the highest tolerated risk score would be 15 (High), but risk levels have plateaued at 20 (High) as noted in regular quarterly corporate risk reporting to Committee.

5. There are a number of security options open to organisations, including Endpoint detection and response (EDR), Network detection and response (NDR), Extended detection and response (XDR), Managed detection and response (MDR), and Managed extended detection and response (MXDR).

6. Because the council would require significant staff numbers for 24/7 staffed coverage, a Managed Service run by external expert contractors is recommended. This would require an MDR or MXDR service.

7. Managed detection and response (MDR) is a cyber-security service that helps protect organisations by using advanced detection and rapid incident response. MDR services include a combination of technology and live staffing oversight to hunt for threats, monitor the IT environment and respond. Managed extended detection and response (MXDR) is the next generation of MDR. It is also a managed service that combines technological solutions with staff expertise. However, with MXDR, the provider uses more tools to extend the protection across a wider variety of IT environments, covering more ground. Because these services offer comprehensive coverage, real-time monitoring, and cyberthreat hunting beyond the physical devices that connect to and exchange information with the computer network, they are often faster and more effective than traditional MDR. MXDR typically also provides a more complete picture of any cyber-attack.

8. Taking a realistic estimate of contractual and staffing costs required to further strengthen our cyber security, and applying anticipated indexation, a budget envelope of up to £3m over five years is anticipated, with a worst-case scenario of £3.2m. This constitutes growth in IT staffing and contract budgets, and in Information Security staffing budget. Further detail is provided with the Finance Advice section of this report. This growth is currently unfunded and would require consideration within the council's Medium Term Financial Plan and budget-setting process to establish relevant budgets.

9. To set any investment in context, the reported cost of major cyber-attacks against local government organisations includes Hackney (£12.5m cost reported by 2022) and Redcar & Cleveland (over £10m direct costs). However, attacks of this scale and magnitude are rare.

Officer Recommendations:

That the Committee for Strategy and Resources:

1. Authorises the Director: Policy, Strategy and Digital in consultation with Chair of the Strategy and Resources Committee, Director of Finance (S151) and Director of Legal & Democratic Services to procure and award a Managed Extended Defence and Response contract, in-line with the maximum budget envelopes outlined in this report, subject to identification of funding within the Medium Term Financial Plan and the setting of the council's budget for 2025/26.

2. Authorises the Director: Policy, Strategy and Digital to invoke any subsequent extensions or variations specifically defined in the contract(s) being awarded, up to the maximum budget envelope outlined in this report.

Corporate Strategy alignment:

1. This proposal aligns with the Corporate Strategy 'Building Block' of Resilience by seeking to provide a more secure and resilient IT infrastructure, prioritising monitoring and early intervention to reduce the risk of damaging cyber-attack(s).

City Benefits:

1. The service will help reduce the risk of successful cyber-attack, the impact of which can have major impacts on the council's ability to provide critical services over the short, medium or long-term.

Consultation Details:

1. Public consultation is not required, and there are no staffing changes requiring staff consultation, as the proposal does not outsource an existing service, rather it introduces a new one. Engagement has been undertaken with the Senior Information Risk Owner (SIRO), the Head of Information Assurance, and the Information Governance Board.

Background Documents:

1. None.

Revenue Cost	**£3,210,000 over 5 years**	**Source of Revenue Funding**	IT Operations Service (General Fund) Information Security Service (General Fund)
Capital Cost	**£/**	**Source of Capital Funding**	/
One off cost ☐ **Ongoing cost** ☒		**Saving Proposal** ☐ **If yes - existing or new saving?** Choose an item. **OR Income generation proposal** ☐	

1. **Finance Advice:** This report seeks approval to procure and award a contract for a Managed Extended Defence and Response service, a third-party provision of 24/7 cyber security monitoring and active defence against cyber-attacks**,** with an estimated revenue cost of up to £3.2m over five years. The recommended approach is a Managed Service (MDR and MXDR services) which will have a total revenue cost of £0.57m to £0.62m per annum. This is comprised of the Managed Service contract itself with an indicative annual cost of £0.3m - £0.35m per annum, and additional staffing costs of c. £0.27m per annum.

Item	**25/26 £000**	**26/27 £000**	**27/28 £000**	**28/29 £000**	**29/30 £000**	**Total (5 year) £000**
MXDR Contract (upper limit)	350	355	360	365	370	1,800
MXDR (likely case)	300	305	310	315	320	1,550
IT Staffing (2FTE	135	138	141	144	147	705

increase)						
Information Security Staffing (2FTE increase)	135	138	141	144	147	705
Total (upper limit)	**620**	**631**	**642**	**653**	**664**	**3,210**
Total (likely case)	**570**	**581**	**592**	**603**	**614**	**2,960**

The alternative option of an in-house Security Operations Centre is considered a costly and resource intensive undertaking, with estimated costs of £0.9m - £1.1m per annum, resulting in a revenue cost in excess of £4.5m over 5 years and is therefore not recommended.

Further analysis will need to take place to assess whether any savings could be achieved, such as replacing any lower level cyber related systems or any reductions in insurance premiums as a result of this enhanced service. These are currently assumed to be immaterial in relation to the total budget request.

This proposal is currently unfunded and would require budget growth. Any decision to progress the agreed approach would be subject to further approval via the Medium Term Financial Plan refresh and annual budget setting process. It should also be noted that the cost of the Managed Service may vary depending on the level of risk appetite that the council is prepared to accept.

Finance Business Partner: Kathryn Long, Finance Business Partner: Resources, 3 September 2024

2. Legal Advice: Given the value of the contract, the procurement route will need to comply with the Public Contract Regulations 2015, unless commencing after October 2023, when the new Procurement Act 2023 comes into operation. The use of a CCS Framework is a compliant route. (Tt is assumed that the framework has been assessed as suitable for the Council's needs). When using a framework it is important to ensure the call off process is followed; and no additional conditions are imposed unless the framework allows for this. Care should be taken to ensure the specification/statement of requirements is comprehensive, to avoid any potential dispute later. It is noted that procurement **cannot** commence until budget provision has been identified.

Legal Team Leader: Eric Andrews, Legal Services, 20 August 2024

3. Implications on IT: The proposals in the report accord with the council's Digital Strategy, particularly strategic ambition 2: Simple, Stable and Secure. Additional staffing resource as outlined in the report would be required across IT and Information Governance functions to provide a robust client-side for the Managed Service and respond to other recommendations within the cyber maturity assessment.

IT Team Leader: Tim Borrett, Director: Policy, Strategy and Digital, 26 July 2024

4. HR Advice: Whilst it is acknowledged that the proposed additional posts will require specialist knowledge and skills, consideration should be given to making opportunities available to existing staff where possible. Any changes to services as a result of this proposal will be undertaken in line with the Council's Managing Change Policy.

HR Partner: James Brereton, Head of Human Resources, 26 July 2024

APPENDICES

Appendix A – Further essential background / detail on the proposal	**NO**
Appendix B – Equality Impact Assessment (EqIA)	**YES**
Appendix C – Environmental Impact Assessment	**YES**
Appendix D – Decision Risk Assessment	**NO**
Appendix E – Exempt Information	**YES**

Ei – **Exempt** Additional Information - Cyber Security Maturity Assessment and procurement of a managed service

Eii - **Exempt** Cyber Security Maturity Assessment report

Eiii - **Exempt** Decision Risk Assessment - Cyber Security

Appendix F – **Details of consultation carried out - internal and external**	**NO**
Appendix G – **Options appraisal matrix**	**NO**
Appendix H – **Business case / financial analysis**	**NO**