TORBAY COUNCIL

Meeting: Cabinet **Date:** 15 August 2023

Wards affected: All

Report Title: Cyber Security – Renewal of 24-Hour Cyber Security Operations Centre Monitoring Contract

When does the decision need to be implemented? By 31st August contract renewal date.

Cabinet Member Contact Details: Councillor Alan Tyerman, Cabinet Member for Finance and Corporate Services, alan.tyerman@torbay.gov.uk

Director/Divisional Director Contact Details: Matt Fairclough-Kay, Director of Corporate Services, matthew.fairclough-kay@torbay.gov.uk

1. Purpose of Report

1.1 To approve a contract for the renewal of 24-Hour Cyber Security Operations Centre Monitoring.

1.2 Following the approval in 2022 of the Endpoint Detection and Response & 24 Cyber Security Monitoring by a Security Operations Centre (SOC), the Security Information and Event Management (SIEM) & SOC solution was implemented during late 2022.

1.3 The SOC has proven to be invaluable and has directly helped prevent a number of potentially catastrophic malware attacks. In a turnaround from pre-implementation - all clients are now monitored with the SOC and the Council now knowing about malware before the users do.

1.4 Having 24-hour monitoring considerably reduces the risk of cyber attack. Cyber attacks typically take place in the middle of the night or outside core working hours. The purpose of this report is to request renewal of the SOC service and award the contract to the preferred bidder sought from the KCS Framework.

2. Reason for Proposal and its benefits

2.1 Having 24-hour monitoring considerably reduces the risk of cyber attack. Renewal of the service reduces the risk of Cyber Attack which could cripple the Council in terms of service delivery or risk its confidential data being leaked to the Dark Web.

3. Recommendation(s) / Proposed Decision

1. That the preferred bidder, sought from the KCS Framework, be awarded the contract for the 24-Hour Cyber Security Operations Centre Monitoring service for a 3 year term as set out in exempt Appendix 1.

Appendices

Appendix 1: Exempt Appendix 1 – Preferred bidder

Background Documents

None

Supporting Information

1. Introduction

1.1 Following the approval in 2022 of the Endpoint Detection and Response & 24 Cyber Security Monitoring by a Security Operations Centre (SOC), the SIEM & SOC solution was implemented during late 2022. The SOC service needs to be renewed prior to contract expiry on 31st August 2023.

2. Options under consideration

2.1 **Options – Cyber Security 24 Hour Monitoring**

Options	Option 1 - Do Nothing	Option 2 – Renew the Proactive Monitoring
Description	Do nothing and lose the 24 hour Cyber Security Operations Centre Monitoring	Renew the existing Security Operations Centre Cyber Monitoring
Option Outline	NA	Renew existing 24-hour support and proactive monitoring from a specialist Security Operations Centre.
Pros	Save budget.	Will provide monitoring to alert of presence of hackers or a cyber-attack. Likely to obtain cyber insurance.
Cons	High security risk & Cyber Insurance will be declined.	None.
Risk/Dependencies	Likely to be hit with a cyber-attack with limited knowledge without SOC.	This is just a renewal. Dependency is procurement which should be renewed using KCS Framework.
Timeline	NA	1-2 Months
Effort/Cost	NA	Annual Revenue is set out in exempt appendix 1
Recommendation	Not Recommended	Recommended

3. Financial Opportunities and Implications

3.1 The budget has already been approved. Without such protection the cost to the Council could be significant should a cyber attack be successful.

4. Legal Implications

4.1 The preferred bidder has been sought from the KCS Framework in accordance with procurement requirements.

4.2 The impact of a cyber attack could have significant legal and reputational ramifications.

5. Engagement and Consultation

5.1 N/A – procurement processes have been followed.

6. Purchasing or Hiring of Goods and/or Services

6.1 Procurement have been engaged with the preferred bidder sought via the KCS Framework.

7. Tackling Climate Change

7.1 No impact.

8. Associated Risks

8.1 Risk of Cyber Attack if service not renewed. Implications are the crippling of Council service delivery and data being leaked to the Dark Web and used for criminal activity.

9. Equality Impacts - Identify the potential positive and negative impacts on specific groups

	Positive Impact	Negative Impact & Mitigating Actions	Neutral Impact
Older or younger people	Protect citizens data & Lower risk of Council Services being disabled.		
People with caring Responsibilities	Protect citizens data & Lower risk of		

	Council Services being disabled.		
People with a disability	Protect citizens data & Lower risk of Council Services being disabled.		
Women or men	Protect citizens data & Lower risk of Council Services being disabled.		
People who are black or from a minority ethnic background (BME) (Please note Gypsies / Roma are within this community)	Protect citizens data & Lower risk of Council Services being disabled.		
Religion or belief (including lack of belief)	Protect citizens data & Lower risk of Council Services being disabled.		
People who are lesbian, gay or bisexual	Protect citizens data & Lower risk of Council Services being disabled.		
People who are transgendered	Protect citizens data & Lower risk of Council Services being disabled.		
People who are in a marriage or civil partnership	Protect citizens data & Lower risk of Council Services being disabled.		
Women who are pregnant / on maternity leave	Protect citizens data & Lower risk of Council Services being disabled.		
Socio-economic impacts (Including impact on child poverty issues and deprivation)	Protect citizens data & Lower risk of Council Services being disabled.		
Public Health impacts (How will your proposal impact on the general health of the population of Torbay)	Protect citizens data & Lower risk of Council Services being disabled.		

10. Cumulative Council Impact

10.1 None

11. Cumulative Community Impacts

11.1 None