REPORT TO:	Executive Board
DATE:	11 July 2024
REPORTING OFFICER:	Director ICT & Support Services
PORTFOLIO:	Corporate Services
SUBJECT:	Delivery of Managed Detection Response System – Key Decision
WARD(S)	‘Borough wide’

1.0 PURPOSE OF THE REPORT

1.1 To update the executive following approval of the Digital Strategy and ICT Capital programme on a key project that will adopt/deliver innovative security technologies to address the evolving cyber threat landscape, reducing cyber risk and detection time, the primary aim of which will be to improve the security footprint of the authority. Delivering a solution that will rapidly identify and limit the impact of cyber based threats by performing threat hunting, monitoring and response.

2.0 RECOMMENDATION: That

1) **the Board approves the procurement of a MDR (Managed Detection Response) System for a single payment of £638,001 delivering over five year contracted term; and**

2) **the Board approves the investment strategy.**

3.0 SUPPORTING INFORMATION

3.1 Following approval of the Halton Digital Strategy by Management Team and Executive Board in March and April 2024, the IT Security Team have evaluated eight security offerings within the market place this was narrowed down to three Tier 1 solutions, the offerings in question are cloud based remote management services primarily for Threat detection, response and remediation.

3.2 The three chosen for final evaluation were all tier 1 suppliers within the security management space.

3.3 Following the detailed evaluation over the last 4 months (documentation available but would pose a security risk if published externally) the chosen MDR offers the price point and far out ways the other offerings with the level of services offered within the package offering, together with the peace of mind for the authority that this supplier being one of the largest suppliers in the world has the in-house resource to manage and maintain what is now becoming an essential a key technology solution.

3.4 So what is MDR: It is 24/7/365 managed (by humans as well as tech)

- Threat Detection
- Threat Hunting
- Response and Remediation
- Point of Contact
- Incident response
- Data Location
- Service Level Management
- Managed Risk Services
- Security Awareness training
- PEN Testing and attack simulation management

3.5 Within HBC our technology assets and our data assets live in an ever changing world were the opportunity for criminal activity is increasing on a daily basis. In reality at a rate that is starting to become a major threat to the operation and sustainability of the authority.

3.6 We are now at the mercy of many attack vectors from individuals and criminal gangs through to foreign government backed agencies.

3.7 This is a world-wide issue that is hitting our news feeds and TV screens constantly with prominent attacks across a number of London hospitals recently causing millions of pounds worth of issues and disruption as business's are not able to operate without access to technology anymore. Many of our employees born in the late 80's early 90's have never experienced a workplace without technology.

3.8 As an organisation we closely follow NCSC and DHLUC cyber security frameworks and guidelines but this isn't enough.

3.9 We need 24/7 monitoring especially with the advent of the cloud and 3rd parties now linked into or managing our data assets. To deliver 24/7 monitoring and response would be an unaffordable proposition as we are not in a position to afford the skills base needed in-house to manage such an onslaught of technical requirement.

3.10 It must be noted that purchasing this contract is not a magic pill and that we would never be subject to any attack but this will considerably mitigate the potential for attack and improve our security stance.

3.11 As part of the procurement process the supplier will implement a 20 day proof of concept installation across the HBC technology landscape.

To involve Managed Detection and Response

- Operating hours: 24 hours a day, 7 days a week (24x7)
- Onboarding
- Detection
- Response & Remediation

Project Kick-off Three (3) days
Tenant creation, vulnerability scan, and reporting review Up to fifteen (15) days
Project Closeout Two (2) days

3.12 Following a successful POC Onboarding will begin

- Service initiation meeting (kick off meeting)
- Customer completed pre-engagement checklist
- Review Customer IT Environment
- SecureWorks XDR application enablement
- Agent rollout assistance

3.13 Detection • 24x7 Access to security analysts

- Threat Detection and Investigations

3.14 Response and Remediation leading to Threat Response Action's set for HBC

4.0 POLICY IMPLICATIONS

4.1 None identified at this stage.

5.0 FINANCIAL IMPLICATIONS

5.1 Following the approval of the increased ICT rolling Capital Programme to support the development of the transformation programme. Key projects have been identified and detailed evaluation across a number of key software and managed services platforms has started.

5.2 This key project will adopt/deliver innovative security technologies to address the evolving threat landscape, reducing risk and detection time, the primary aim of which will be to improve the security footprint of the authority. A solution that will rapidly identify and limit the impact of threats by performing threat hunting, monitoring and response.

5.3 This managed services platform will integrate with the HBC platforms out of which it will support the Digital Journey of considerable change to the current HBC technology environment.

5.4 At this stage we are still building the platform and linking with other major projects such as M365 and the new device strategies. This will now start to pull these solutions together and evaluate and remediate issues and the changes required to deliver a fully integrated platform for the authority.

5.5 This project will be funded by capital rolled over from the 2023/2024 capital programme together with 2024/2025 capital.

5.6 £419,000 from 23/24 - £219,001 from 24/25.

5.7 By procuring this solution upfront and over the five year commitment has brought considerable savings in relation to the project overall - negotiations discussed the spread and coverage of services as well as the associated costs and the potential hidden costs.

5.8 It is possible to pay for the solution quarterly in arrears but this would increase the contractual costs by £124,000 – following discussion it is cheaper to procure using existing capital funding.

5.9 All three of the final evaluation set altered pricing considerably and changed the offerings accordingly, the final product set chosen and the contractual cost offers a huge saving over the initial prices and offers a greater level of included services and systems. Again detailed evaluation is available but for commercial and security reasons this cannot be published within this document under section 31a of the FOI rule set but is available for review if required by internal HBC resource.

6.0 IMPLICATIONS FOR THE COUNCIL’S PRIORITIES

The business case for technology investment outlined in this report will enable and support transformational change to be delivered within all service areas across the authority, also supporting other workstreams comprising the Re-imagine Halton transformational programme.

It is important we invest in technology platforms that will allow our customers, both internal and external, improved user experience and access to services by facilitating self- service, 24/7, multi-channel delivery. Service managers will also benefit from having access to a platform for facilitating the redesign of the way they deliver their services to improve service efficiency and build capacity.

6.1 Children & Young People in Halton

As 6.0

6.2 Employment, Learning & Skills in Halton

As 6.0

6.3 A Healthy Halton

As 6.0

6.4 **A Safer Halton**

As 6.0

6.5 **Halton's Urban Renewal**

As 6.0

7.0 RISK ANALYSIS

7.1 Failure to invest in new technology to facilitate transformative change risks the gradual erosion of service levels and loss of capacity to make transformational change in the future. The continued risk of Cyber-attack.

8.0 EQUALITY AND DIVERSITY ISSUES

8.1 The authority's policies and process will be followed.

9.0 CLIMATE CHANGE IMPLICATIONS

9.1 None

10.0 REASONS FOR DECISION

10.1 The security of the authority, compliance with the DHLUC Cyber Assessment Framework (CAF)

11.0 ALTERNATIVE OPTIONS CONSIDERED AND REJECTED

11.1 Following approval of the Halton Digital Strategy by Management Team and Executive Board in March and April 2024, the IT Security Team have evaluated eight security offerings within the market place this was narrowed down to three Tier 1 solutions, the offerings in question are cloud based remote management services primarily for Threat detection, response and remediation.

11.2 For security reasons: Specific information is removed related to Section 31a Freedom of Information Act prejudice to law enforcement.

11.3 IMPLEMENTATION DATE

11.4 It is intended to initiate a 20 day proof of concept installation 24th June 2024 prior to any go live, this will also comply with additional cyber security requirement prior to the general election.

12.0 LIST OF BACKGROUND PAPERS UNDER SECTION 100D OF THE LOCAL GOVERNMENT ACT 1972

For security reasons: Specific information related to Section 31a Freedom of Information Act prejudice to law enforcement.

With regards to this project this covers several areas related to ICT security (including by not limited to, backup and recovery, vulnerabilities, encryption methods) and as such this information is exempt under Section 31(a) of the FOI Act.

Exempt information has been used in the production of this report, which is protected by s31 Freedom of Information Act 2000