Agenda Item

DERBYSHIRE COUNTY COUNCIL

CABINET MEMBER FOR CORPORATE SERVICES AND BUDGET

26 May 2022

Report of the Executive Director of Corporate Services and Transformation

Direct Award of a contract to undertake Specialist ICT Forensic Analysis

1. Divisions Affected

1.1 Corporate Services & Transformation - Finance & ICT Service

2. Key Decision

2.1 This is not a Key Decision

3. Purpose

3.1 The purpose of this report is to seek Cabinet Member approval to make a direct award of a contract to Microsoft Limited for Enterprise Services Work to undertake forensic analysis of the Council's ICT infrastructure and systems in response to a recent cyber security incident.

4. Information and Analysis

4.1 On 13 May 2022 employees in the ICT Operational team identified a critical vulnerability that had been exploited by an unknown entity in one of the council's third-party ICT hardware devices. The device is used to provide firewall services in the Councils Microsoft Azure Tenant.

4.2 The vulnerability was disclosed on 4 May 2022 and was then exploited a few days later. A patch has since been released to remediate the vulnerability. It is understood that the cyber attackers are using the vulnerability to wipe device file systems, making IT services then unusable or creating a foothold into the wider network. Attackers have been conducting widespread reconnaissance to discover publicly accessible systems.

4.3 Immediate activities took place to try and resolve the issue and the ICT Team worked through the weekend of the 14th and 15th May to mitigate any threats. The work undertaken minimised the potential for immediate disruption, but further specialised ICT forensic investigative work was considered a requirement to ensure that the incident and vulnerability are completely resolved; this urgent specialist support is not available internally and is therefore required from an external resource as a matter of urgency.

4.4 The vulnerability exploited was on the Councils' Microsoft Azure firewalls, which protect the Council from unauthorised access to Council's ICT systems and services. Although the firewalls are not Microsoft, most of the Council's ICT systems and services that are protected by the firewalls are hosted on a Microsoft infrastructure, including critical user identity services.

4.5 Microsoft was approached for advice on dealing with the incident and advised that they had a professional forensic examination team, known as the Microsoft Detection and Response Team (DART) who's specific role is to support organisations in this situation. This is a paid for service, but the Council has no contract or insurance in place to cover the work. There are other specialised companies who can offer ICT forensic services, but given the nature of the incident and the need to act quickly to ensure containment and remediation it was considered appropriate to engage with Microsoft immediately. As a result, the interim Executive Director for Corporate Services and Transformation authorised an initial engagement of 5-days and this business case looks to deal with retrospective approval for that and any further work that follows.

5. Consultation

5.1 Not required.

6. Alternative Options Considered

6.1 Given the timeframes involved and the unsolicited attack on the Council's infrastructure has the potential to cause widespread disruption to council services it was impractical to go out to open tender or make use of a framework for this requirement. Due to the circumstances Microsoft were engaged to undertake the work, and it is now proposed a contract is retrospectively directly awarded to Microsoft for the service outlined in the business case under Protocol 8 of the Council's Financial Regulations.

7. Implications

7.1 Appendix 1 sets out the relevant implications considered in the preparation of the report.

8. Background Papers

8.1 Background papers are held by Mark Whelan, Head of ICT Organisational Management.

9. Appendices

9.1 Appendix 1- Implications.

10. Recommendation

10.1 That the Cabinet Member approves, a direct award of a contract to Microsoft Ltd for Specialist ICT Forensic Analysis in accordance with Protocol 8 of the Council's Financial Regulations

11. Reasons for Recommendation(s)

11.1 To ensure that the threats from the recent cyber security incident that the Council has experienced are remedied and the Council's ICT systems and services are free from any associated vulnerabilities relating to this.

12. Is it necessary to waive the call-in period?

12.1 Yes

12.1 Councillor Graham Swann, Chair of Improvement and Scrutiny Committee – Resources has approved the waiver of the call in period due to the urgent nature of the decision required; he has agreed the decision proposed is reasonable in all the circumstances and to it being treated as a matter of urgency.

Report Author: **Mark Whelan**
Contact details: **mark.whelan@derbyshire.gov.uk**

This report has been approved by the following officers:

On behalf of: Director of Legal Services and Monitoring Officer Director of Finance and ICT Managing Executive Director Executive Director(s)	

Appendix 1

Implications

Financial

1.1 The cost for the initial 5-day engagement is £104,025. Any further engagement of the DART team is priced at £93,525 for each subsequent week thereafter. A 2-week provision is factored into the overall cost.

1.2 During the course of the forensic investigations there may be a need to engage with specific technical resources to assist in undertaking any remedial work that is required. A contingency of £200,000 is recommended for the purpose,

1.3 The maximum costs that will be incurred as a result of this contract will be £491,075

1.4 Any final decision on the engagement of further resources beyond the initial 5-day engagement will be dependent on the outcomes from the previous weeks findings and sign off from the interim Executive Director for Corporate Services and Transformation.

1.5 It is proposed that the funding for the work is met from the ICT Reserve.

1.6 In accordance with Protocol 8 of the Council's Financial Regulations a business case has been approved by the Director of Finance & ICT and the Director of Legal & Democratic Services for the award a contract to Microsoft Limited for Enterprise Services Work to undertake forensic analysis of the Council's ICT infrastructure and systems in response to a recent cyber security incident.

Legal

2.1 The Director of Legal and Democratic Services is satisfied that on the basis of the information contained in the report it is appropriate to directly award a contract to Microsoft Limited for Enterprise Services Work to undertake forensic analysis of the Council's ICT infrastructure and systems in response to a recent cyber security incident in accordance with Protocol 8 of the Council's Financial Regulations.

2.2 Improvement and Scrutiny Procedure Rules State: "13(6) The call-in procedure set out above shall not apply where the decision being taken by Cabinet is urgent. A decision will be urgent if any delay likely to be caused by the call-in process would seriously prejudice the Council's or

the public interest. All reports recommending that decisions be taken should say whether or not it is proposed that call-in be waived. The record of the decision, and notice by which it is made public, shall state whether in the opinion of the decision-making person or body, the decision is an urgent one, and therefore not subject to call-in. The Chairman of the appropriate Improvement and Scrutiny Committee should agree both the decision proposed is reasonable in all the circumstances and to it being treated as a matter of urgency

Human Resources

3.1 None

Information Technology

4.1 The forensic work will exam the Council ICT systems and services to ensure any issues that has arisen as a result of the cyber incident are remediated and any future vulnerabilities associated are mitigated.

Equalities Impact

5.1 None

Corporate objectives and priorities for change

6.1 None

Other (for example, Health and Safety, Environmental Sustainability, Property and Asset Management, Risk Management and Safeguarding)

7.1 None