Improvement and Innovation Board

24 May 2018

LGA Cyber Security Funded Programme

Purpose of report

For discussion.

Summary

This report advises that funding for the Cyber Security programme has been confirmed by Cabinet Office and HM Treasury. It updates the Board on the status of the programme and progress made to date. It also advises about the next steps and timescales in relation to the stocktake.

Recommendations

That Members of the Improvement and Innovation Board:

1. Note the current position with regard to the funding and the progress made to date.

2. Actively support and encourage all councils to support and complete the stocktake.

Action

Subject to members' views, officers to pursue the activities outlined at paragraph 12 onwards.

Lead Member: Cllr Ron Woodley

Contact officer: Susan Attard

Position: Head of Productivity

Phone no: 07825 530528

Email: susan.attard@local.gov.uk

LGA Cyber Security Funded Programme

Background

1. The National Cyber Security Programme is overseen by Cabinet Office and supports and funds work to deliver the National Cyber Security Strategy. Last autumn, Cabinet Office invited the LGA, via the Local Government Cyber Security Stakeholder Group, to submit a bid on behalf of the sector for funding to the Cyber Security Programme (NCSP). The LGA worked with a number of partners including: Socitm, Solace, and Cipfa, and sought input from the WARPs (Warning Advice Reporting Points), the Technical Advisory Group and the Local CIO Council to put a bid together on behalf of the sector.

Outline of the funded programme

2. The LGA has been informed by Cabinet Office that the bid has been successful subject to final sign off by the Treasury. Formal notification of the funding was provided by Treasury on 27 April 2018. The funding is for one year, (with a recommendation to bid for further funding in the autumn), to undertake a comprehensive stocktake and analysis of the current cyber security arrangements across all principal councils in England. This aims to:

    2.1. Capture existing cyber security arrangements.

    2.2. Identify good practice - and those councils delivering it.

    2.3. Identify risks - and those councils at potential risk.

3. The findings and analysis from this work will be used to inform and implement a plan of support for the sector.

Preparation for the stocktake exercise

4. A high-level outline for the stocktake into council's cyber security arrangements has been drafted. This will capture the cyber security arrangements across a range of disciplines, currently in place in councils. This breaks down into several work areas including:

    4.1. Leadership i.e. the role of senior officers and elected members.

    4.2. Governance i.e. board oversight, emergency planning, contingency and risk planning.

    4.3. Information and technology i.e. robust IT tools and data processes.

    4.4. Staff and elected member, training and awareness raising;

4.5. Engagement with the wider sector around cyber security i.e. WARPs, NCSC and CISPs.

5. This will be a stocktake of both the prevention measures in place to mitigate the risk of cyber-attack and the arrangements in place to respond to such an incident if and when one takes place.

6. We will be commissioning an external provider to deliver the stocktake. A supplier briefing session was held in March to help inform how best to do the stocktake and to achieve the outcomes we want to deliver. We commenced the procurement process to commission a research partner at the end of April. The provider will be ready to commence the stocktake in June 2018.

Support and improvement

7. The purpose of the stocktake is to help make every council as safe and secure as possible. We will help councils to understand their strengths and weaknesses. We will target support quickly to those councils identified as potentially being most at risk. We will identify good practice across the sector and recruit and fund peers from these councils to deliver support. We will implement a grant funding scheme, targeting funds at those councils and WARPs with an agreed project/activity for them to carry out, to improve their cyber resilience.

8. The stocktake exercise is likely to be carried out as an online questionnaire.

9. In order to develop a clear view of where the strengths and weaknesses lie across our sector and deliver the support needed it will be essential that we secure a 100 per cent response rate i.e. all councils. We would be grateful if members would ensure the stocktake is completed in their council and if members could also encourage their neighbouring councils to take part.

Implications for Wales

10. There are no implications for Wales. Improvement work is provided directly by the WLGA.

Financial Implications

11. There are no additional financial implications arising from this report.

Timeline and Next steps

12. April - May 2018: Procurement exercise to commission a research partner.

13. June - August 2018: Councils will be asked to complete their online stocktake questionnaire.

14. September 2018: Early findings from stocktake will help us to identify strengths and weaknesses across the sector.

15. September - October 2018: We will work with those councils potentially most at risk.

16. September - March 2019: We will recruit and allocate sector peers.

17. October - March 2019: We will implement a grant funding scheme.

18. October 2018: We will submit a bid for future funding to address longer term issues raised by the stocktake and help build sustainable cyber resilience.