Improvement & Innovation Board

15 October 2020

Cyber Security Programme Update

Purpose of report

For information.

Summary

The Cyber Security Programme is now in its final year of the initial three-year agreement. This paper takes IIB through key achievements so far, the plan for this Financial Year including a key project, and finally suggests what might be possible post March 2021.

Recommendation

That the board note the following:

- The progress of the programme to date.
- The future of the programme.

Contact officer: Owen Pritchard

Position: Cyber Security Programme Manager

Phone no: 07795 842478

Email: owen.pritchard@local.gov.uk

Cyber Security Programme Update

Background

1. In 2018, the LGA Cyber Security Programme was formed following funding from the National Cyber Security Programme (NCSP) through the Cabinet Office. The programme is now in its final year of the initial three-year agreement.

2. The aim of the programme is to improve the Cyber Security of English Local Authorities, with the desired strategic outcome being that Local Government networks and services will be as secure as possible from the moment of their first implementation, and that the public will be able to use local government digital services with confidence, trusting that their information is safe.

3. The LGA works collaboratively with representatives from MHCLG, the National Cyber Security Centre (NCSC), SOLACE, SOCITM, the NHS, the Cabinet Office and the local government community. The programme plays to the strengths of the LGA, and the improvements it already delivers for local government. The programme uses a sector-led approach to improvement to deliver sustainable cultural change within councils that both directly improves cyber security and indirectly leads to members and officers viewing it with increased importance. The programme does not consider cyber security to be solely a technological issue.

4. The programme's main achievements have been to:

    a. Develop and deliver a Cyber Security Stocktake which 100% of councils completed (year 1).
    b. Develop and deliver a self-assessment tool which 54% of councils completed (year 2).
    c. Support the response and recovery of Redcar and Cleveland Council after they were the victim of a major ransomware incident, and support the lessons learned process following incidents at Wiltshire Council and Copeland Council (year 2).
    d. Directly support over 90% of English Councils to improve cyber leadership, governance, awareness and training via c£3.1M of direct targeted grants (years 1&2).

COVID-19 Impact

5. The third year of the programme began during a demanding and difficult time for everyone involved in Local Government, which has been illustrated in the June 2020 National Cyber Security Centre report on the threats to local government considering COVID-19, with covering letter to Chief Executives from Simon Clarke MP.

6. Never has the work of councils been so vital to the most vulnerable in our society, and never have the digital communications and services that councils use been so critical to their efforts. From video conferencing and new data sharing, to the digitisation of public meetings, the LG response to COVID-19 demands continuous and accelerated digital innovation. New working conditions and the burden and pressure that all council staff, and those who work in resilience and/or support digital services, are now under will mean having an even more flexible and empathetic approach to how we work with them.

7. Cyber threats have not gone away, and many criminals are using the current situation as an opportunity to extort ransoms. This fact – when combined with the increase in vulnerabilities that distance working, new partnerships, and our increased reliance on digital services bring – means that the risk associated with a cyber incident is greater than ever and that this programme will need to remain responsive to changing demands and priorities.

Programme Response to COVID-19

8. The Programme had originally been asked to deliver a comprehensive assessment of Council's Incident Management Practices, for FY 20/21, however the focus has been rightfully realigned to support the COVID-19 response.

9. The key project this programme will now deliver is to explore and trial the vulnerability/penetration testing of new or adapted existing websites, portals, or applications that have been developed to support the response to the COVID-19 crisis, which will help support councils within the recovery period.

Vulnerability/Pen Testing Opportunities and Risks

10. The proposed project approach is to pay NCSC certified organisations to vulnerability /penetration test 10% of councils. This is an opportunity to get a detailed, thorough, and supported test for free, worth £20-30k.

11. The four project outputs are:

    a. a detailed technical report for each council;
    b. a high-level report for senior leadership for each council;
    c. a report on key sector-wide themes; and
    d. an analysis of the gap between assessed vulnerabilities and those exposed through existing assurance methodologies.

Strategic Context of Programme

12. In February 2020, a ransomware attack on Redcar and Cleveland council pushed cyber security and resilience up the agenda of the Cabinet Office and MHCLG. The incident exposed that many councils were vulnerable to ransomware due to the nature of their data back-up arrangements.

13. MHCLG and the Cabinet Office surveyed councils to understand the scope of this issue and begin to support remediation. The LGA's cyber self-assessment tool, which was designed to nudge behaviours and support continuous improvement, could not support this work due to the LGA not having the right to share its data with Central Government.

14. Following on from the technical survey, MHCLG conducted a "Discovery" project consisting of 37 interviews and a number of workshops to ascertain the cyber security priorities and key issues for LG. It didn't discover anything we didn't already know. The following is an extract from their blog report:

"Building on the work completed during pre-discovery, we were able to gain a clearer picture of problems and opportunities. These are some of the key findings that came out of the discovery:

- *There are many cyber standards, but no clear baseline.*
- *An effective cyber baseline must encompass culture, leadership and 'cyber first' processes.*
- *Leadership support is vital to embed standards and best practices across the organisation.*
- *Leaders need to understand cyber risk to inform their decisions.*
- *Legacy technology is a critical blocker to achieving cyber health.*
- *There is an opportunity for councils to collaborate in order to achieve greater security.*

Through our research it became clear that, while councils are doing the best they can with the resources and knowledge they have, there are a number of areas in which MHCLG might provide support.

What happens next

After having researched the problems and challenges that local authorities faced in improving their cyber security, we sought to generate holistic solutions that solve the largest amount of pains. Through a series of workshops with stakeholders and local authorities, we identified the main areas of focus to solve the known problems. We then selected the top five areas of opportunity for MHCLG and key stakeholders to progress into alpha.

1. ***Cyber Health Framework*** *- develop a framework of cyber security standards and guidance that organisations can apply in order to achieve a minimum level of cyber health and measure where they are against this baseline*
2. ***Cyber Roles*** *- formalise the role of the decision-maker for cyber security at the executive level within local authorities, with clear lines of communication to that person*
3. ***Peer Support*** *- explore how to formalise a professional network for cyber security professionals from local authorities and create a trusted 'safe space' where peers are able to share and learn*
4. ***Training and Support*** *- provide a range of training that fosters cyber responsible attitudes and behaviours*
5. ***Technical Remediation*** *- provide support to councils identified through the recent survey on mitigating malware and ransomware*

We are currently submitting bids to secure funding for the continuation of this work. Some of the work will be owned and carried out by MHCLG directly and some we will look to collaborate with stakeholders and leaders in this space on. We want to continue our collaboration and research with local authorities in developing the cyber framework and to continue to test our findings and recommendations using a user centred and evidence-based approach. We will look to support the councils identified as "at risk" in the ransomware survey as an immediate action."

15. The Cabinet Office are also drawing up their public sector cyber security strategy for the future, however, have suggested it is highly likely that the LGA will continue to be funded post March 2021, either through a one- or three-year rollover from the NCSP.

Implications for Wales

16. We continue to work with Welsh counterparts in the Welsh LGA , the devolved government; and at LA level (through their representation on advisory boards that we attend). Many of the lessons and improvements we identify are applicable to Welsh councils and are shared with them. Although there are no Welsh councils involved in the testing pilot – as the programme is funded to improve the cyber security of English local authorities – the reports on key sector-wide themes and the gap analysis will also be of use to the sector in Wales.

Financial Implications

17. The Cyber Security programme is only guaranteed funding until March 2021, with plans for what might come next still unconfirmed. However, if the Cabinet Office do agree a NCSP rollover then the LGA could be awarded further funding or a similar magnitude.

Next steps

18. If successful in obtaining further funding, the programme's future work could be aimed at:

    a. The development of comprehensive cyber standards with an associated maturity framework.
    b. The development of a corresponding assessment tool which greatly improves on the 2019 tool.
    c. Scaling up the trial of testing to support a greater percentage of councils.
    d. The purchasing of a cyber awareness raising package for local government saving up to £1.5M per annum.
    e. The development of systematic peer support for pre-incident and post-incident.
    f. A better understanding the comprehensive attack picture for local authorities.
    g. A review of incident management practices.