Committee:	Governance, Audit and Performance Committee	**Date:**	Thursday 25 July 2019
Title:	Cyber Security Update		
Report Author:	Nicola Wittman, Assistant Director – ICT & Facilities nwittman@uttlesford.gov.uk		

Summary

The report below was presented to the Governance, Audit and Performance Committee at its last meeting, on Thursday, 30 May. However, with the change in membership of the Committee, it is being re-presented so new members can obtain an understanding of the cyber issues facing the authority and the steps being taken to combat them.

As per the report, there is still a requirement for a lead member to be appointed responsible for oversight of cyber security.

Recommendations

1. It is recommended that the Committee

    a. notes the update; and

    b. appoints a member of the Committee as the lead Member responsible for oversight of cyber security.

Financial Implications

2. All financial implications are funded from the existing budget.

Background Papers

3. The following papers were referred to by the author in the preparation of this report and are available for inspection from the author of the report: none

Impact

Communication/Consultation	All staff are made aware of the importance of vigilance around cyber security and the consequences of an attack.
Community Safety	A cyber-attack could have impacts on the ability of the Council to undertake its core functions such as paying Housing Benefit. ▪
Equalities	None
Health and Safety	A cyber-attack could have impacts on the ability of the Council to undertake its core functions such as emptying bins which could have Health and safety implications.
Human Rights/Legal Implications	None
Sustainability	None
Ward-specific impacts	None
Workforce/Workplace	All staff are made aware of the importance of vigilance around cyber security and the consequences of an attack.

Situation

4. As part of the National Cyber Security Strategy, the Local Government Association (LGA) was granted phased funding by the Cabinet Office to ensure that councils are as resilient against cyber-attacks as possible.
5. The first phase of the work took place over summer 2018. Every council in England completed an online stocktake questionnaire concerning their cyber security arrangements. The LGA worked with the Cabinet Office, the National Cyber Security Centre (NCSC), the Ministry of Housing, Communities and Local Government (MHCLG), the Society of Information Technology Managers (Socitm), the Society of Local Authority Chief Executes (Solace) and the Warning, Advice and Reporting Points (WARPS) to develop this programme.
6. The first phase aimed to:
    - Capture existing cyber security arrangements
    - Identify good practice – and those councils delivering it
    - Identify risks – and those councils at risk.
7. The stocktake took a broad definition of cyber security that incorporated leadership, governance, partnerships and training arrangements, beyond the traditional information technology (IT)

security controls and adoption of standards that underpins cyber security's technology practices.

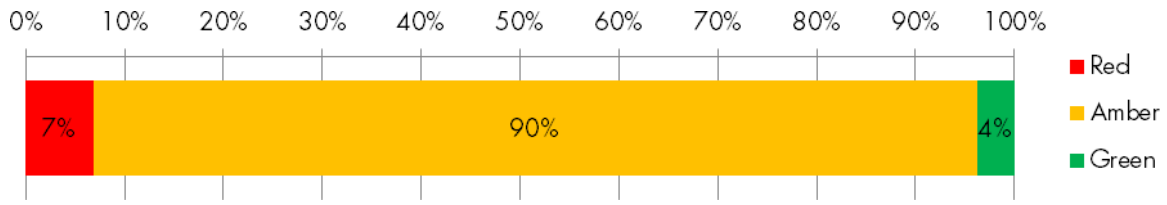
8. The study team applied a weighting and scoring method to analyse the results of the stocktake for each council and to provide them with their 'RAG' (red, amber or green) rating. A greater level of granularity was required to understand the distribution of results; therefore, the amber category was further broken down into three segments to analyse councils at the cusp of the red and green ratings.

    - Amber-Red
    - Amber-Amber
    - Amber-Green

9. Each council received an individual assessment that provided a RAG rating of their cyber security arrangements broken down into five categories with relative weighting

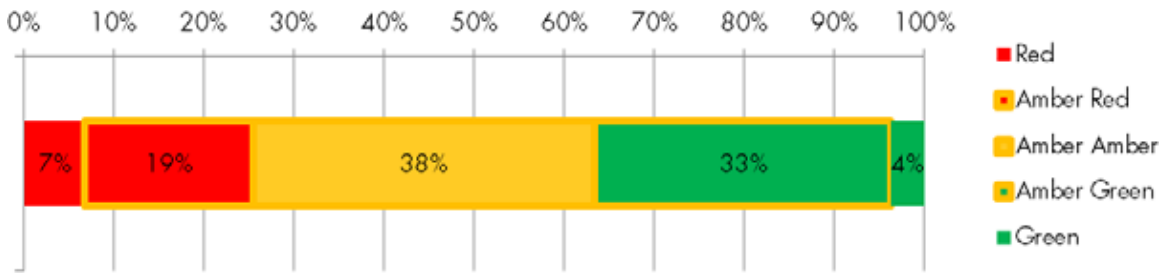
    - Leadership, reporting and ownership (30%)
    - Governance, structures and policies (25%)
    - Partnerships, information, advice and guidance (20**%)**
    - Technology, standards and compliance (15%)
    - Training and awareness (10%)

    90 percent of councils scored an amber rating (roundings mean the chart adds up to 101%)

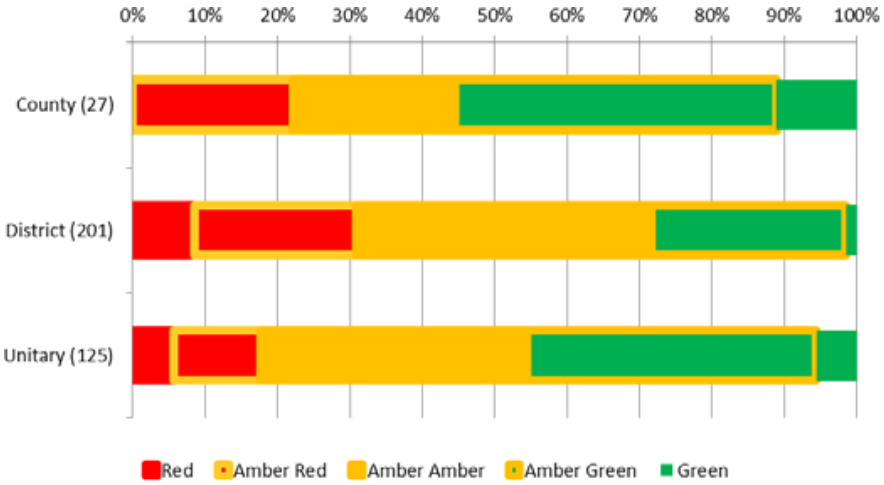


10. The following chart shows the further breakdown of the Amber section

    - Amber-Red (19%)
    - Amber – Amber (38%)
    - Amber-Green (33%)



11. The results were then broken down by council type. As might be expected, the larger bodies have more resources available and therefore have more Green and Amber-Green councils.



Uttlesford's Assessment Results

12. The Council received an Amber-Amber rating for the assessment.
13. Phase Two of the LGA funding was a round of bidding for funds to help councils move forward with their cyber security. Uttlesford was successful in being granted £5,000 which has been used to move forward with the business continuity plan and training.
14. A lot of other work has been completed since the last assessment; however the following work still needs to be finished to achieve a Green classification at the next review.

- **Leadership, reporting and ownership -** a councillor needs to be responsible as the lead Member for Cyber Security oversight, along with cyber security reporting into a committee.

- **Governance, Structures and policies** - the Council's overarching business continuity process to be updated to include sections on cyber security arrangements.

- **Overview of Technology, standards and compliance -** the council is working towards accreditation of Cyber Essentials and Payment Card Industry (PCI) standards. This will take some time to complete.

- **Training and Awareness -** A Cyber training course is being tested by a team of staff and this will be rolled out to all staff once operational.

15. It is expected that the LGA stocktake will be redone in August.

Risk Analysis

Risk	Likelihood	Impact	Mitigating actions
Failure to appoint a Member responsible for cyber security may leave the Council unable to bid for future funding rounds.	4	2	The report recommends the appointment of such a role.

1 = Little or no risk or impact

2 = Some risk or impact – action may be necessary.

3 = Significant risk or impact – action required

4 = Near certainty of risk occurring, catastrophic effect or failure of project.