Report to Governance and Ethics Committee
18th December 2018

Agenda Item: 7

REPORT OF THE SERVICE DIRECTOR FOR FINANCE, INFRASTRUCTURE AND IMPROVEMENT

NATIONAL AUDIT OFFICE CYBER SECURITY AND INFORMATION RISK GUIDANCE FOR AUDIT COMMITTEES

Purpose of the Report

1. To provide Members with a review of the advice for audit committees on cyber security provided by the national audit office, an assessment of the current state for Nottinghamshire County Council against this advice and to brief Members on the current activity to strengthen the Authority's position where required.

Information and Advice

Background

2. The County Council's approach to cyber security has traditionally been addressed by the ICT function and delivered through a combination of a strength in depth technical security posture combined with compliance to certification programmes such as PSN (Public Services Network).

3. This approach has recently been complemented by the formation of the Information Governance (IG) Team and the work of the IG improvement programme.

4. The National Audit Office (NAO) guidance for audit committees (Appendix 1) recognises that effective cyber security cannot be assured through technical defence alone and must include people (culture, behaviour and skills), process, technology and governance. This mirrors the approach adopted by the Authority through the IG improvement programme, the implementation of the new General Data Protection Regulations (GDPR) and the technical defences deployed.

5. In order to support committees in their oversight and governance of cyber defence capabilities with their organisations, the guidance recommends a number of questions are posed and the responses monitored. A current state assessment conducted by the ICT architecture team has been included in this report along with a summary of the rationale for the RAG status where this is other than green. A more detailed question breakdown used to inform this summary has been included as appendix 2.

Current state assessment

6. The guidance groups the questions into three sections:

   a. Section 3. High level questions
   b. Section 4. More detailed areas to explore
   c. Section 4. Additional questions

3. High Level Questions	
1. Has the organisation implemented a formal regime or structured approach to cyber security which guides its activities and expenditure?	Amber
2. How has management decided what risk it will tolerate and how does it manage that risk?	Red
3. Has the organisation identified and deployed the capability it needs in this area?	Amber

Assessment summary:

7. Question 3.1 is rated as amber due to the assessment that existing regimes and approaches are not formalised. At present, activity and resulting expenditure are focused on obtaining and maintaining compliance to national standards and best practice. Many of the component parts exist but these need formalising into an organisation wide information security management system (ISMS). Work currently underway by ICT and the Data Protection Officer to agree how this is delivered and managed in the future will strengthen this assessment.

8. Question 3.2 is rated as red due to the current risk management processes identifying and mitigating risk on an individual or departmental risk basis. Recommendations are being considered by Information Governance Group to strengthen the governance of information risk and consideration of these recommendations overlap the presentation of this report.

9. Question 3.3 is rated as amber. There are dedicated security roles in the ICT structure that design, manage and update the security policies and procedures for the Authority. The Authority has a nominated data protection officer and an information governance team. The ICT function also has a ‘flex’ model as part of the structure that allows temporary resource to be brought in for specific purposes as and when the needs arise. Tools that automate some of the threat prevention capability are assessed regularly in order to maximise the effectiveness of the resources available and the use of the higher end tools would strengthen the assessment. However, there is a significant cost implication that has to be balanced with the likelihood of the mitigated risk materialising.

4. More detailed areas to explore	
1. Information risk management regime	Amber
2. Secure configuration	Green
3. Network Security	Green
4. Managing User Privileges	Amber
5. User education and awareness	Green
6. Incident management	Green
7. Malware protection	Green
8. Monitoring	Amber
9. Removable media controls	Green
10. Home and mobile working	Green

Assessment summary:

10. Question 4.1 is currently assessed as amber but plans are in place to both exploit new tools available once migration to the new cloud based services is complete in 2019 and this will strengthen the position and hence the assessment.

11. Question 4.4 is currently assessed as amber only because audit logs are not routinely analysed for unusual behaviour, logs are analysed on a per incident basis. Other controls concerning user privileges are conducted in line with industry best practice and funding streams via the LGA are being explored to enable routine log analysis.

12. Question 4.8 is assessed as amber as a Protective Monitoring Standard ensures that logs can be monitored to detect attacks and for subsequent forensic analysis. Log analysis is currently manual and therefore quite limited. ICT Services are investigating funding opportunities from the Local Government Association cyber security stocktake to supplement the logging and monitoring capability.

5. Additional questions	
1. Using Cloud Services	Green
2. Development of new services or technology	Green

Summary

13. The NAO guidance provides a sound blueprint for the management of information and cyber security. The assessment of the current state indicates that there are improvements to be made but we are starting from a sound footing.

14. From a technical perspective, our current protection methods and infrastructure have remained resilient and currently successfully defend over 65,000 malicious emails, approx. 26,000 attempts to exploit known vulnerabilities and 3,500 attempted virus outbreaks on a weekly basis.

15. The Authority's standards and guidance on information and IT security have been refreshed and are due for publication in December 2019.

16. The establishment of an information governance team and information improvement programme have greatly improved the management of our sensitive data.

17. There are however, improvements that can be considered to improve how information and cyber risk should be governed and managed by the Authority as a whole and an update report to this committee on progress will be presented at a later date.

Statutory and Policy Implications

18. This report has been compiled after consideration of implications in respect of finance, equal opportunities, human resources, crime and disorder, human rights, the safeguarding of children, sustainability and the environment and those using the service and where such implications are material they are described below. Appropriate consultation has been undertaken and advice sought on these issues as required.

RECOMMENDATION

It is recommended that:

1) Members agree to receive an update report in 6 months' time and consider what further action they wish to take.

Nigel Stevenson
Service Director Finance, Infrastructure and Improvement

For any enquiries about this report please contact:
Adam Crevald, Group Manager Design (ICT)
(0115 9772839)

Constitutional Comments (HD 7/12/18)

The recommendations fall within the remit of the Governance and Ethics Committee by virtue of its terms of reference.

Financial Comments: (CSB 10/12/2018)

There are no specific financial implications arising directly from this report.

Background Papers

None

Electoral Division(s) and Member(s) Affected

All