Nottinghamshire County Council

Report to Finance Committee

11 October 2021

Agenda Item: 8

REPORT OF THE HEAD OF TECHNOLOGY & DIGITAL, CHIEF EXECUTIVE'S DEPARTMENT

CYBER SECURITY ASSURANCE QUARTER 1 2021-22

Purpose of the Report

1. To provide the Finance Committee with the 1st quarter progress update towards Public Sector Network (PSN) and Cyber Essentials accreditation.

Information

Performance Update

2. To provide a balanced assessment of performance and assurance of continued focus on Cyber Security, ICT Services measure several indicators that cover monitoring, maintenance, and compliance to Public Sector Network (PSN) and Cyber Essentials standards.

3. Some information relating to this report is not for publication by virtue of Schedule 12A of the Local Government Act 1972 because the information relates to action which may be taken in connection with the prevention, investigation or prosecution of crime. Having regard to all the circumstances, on balance the public interest in disclosing the information does not outweigh the reason for exemption because divulging the information would add a limited amount to public understanding or the issues but could significantly damage the Authority's cyber security The exempt information is set out in the exempt appendix.

Public Sector Network (PSN) & Cyber Essentials compliance

4. PSN and Cyber Essentials are both compliance regimes that demonstrate a good posture in relation to a wide cross section of security controls that are representative of organisations that protect their information and systems well. Recertification against these regimes matters as failure to do so could result in access to essential central government and partner business systems could become unavailable, and access to central government funding could be denied where certification against these regimes are a prerequisite.

5. The following paragraphs describe a number of the indicators we use to measure progress against achieving accreditation.

Successful cyber-attacks/cyber breaches

6. This indicator measures how successful external threat actors are at attacking the Council's systems. A cyber-attack/breach is where an external threat actor attacks NCC and is defined as successful when it impacts the Confidentiality, Integrity or Availability (CIA) of systems or information. This means direct business or service user impact and require significant resources or systems downtime to resolve, or an investigation or fine from the Information Commissioner's Office (ICO).

7. Examples include attacks resulting in systems being unavailable, data being altered by a threat actor or a threat actor obtaining data/documents/information marked OFFICIAL or OFFICIAL-SENSITIVE as a result of an attack. It does not include obtaining a user's password by nefarious means (such as phishing/spear phishing attacks) unless this leads to a successful attack as described in paragraph 6. Also excluded are spam/malware/viruses that do not lead to a successful breach of CIA. As defined, successful cyber-attacks are very rare.

Servers without anti-virus

8. This KPI measures the number of servers that do not have anti-virus client installed. The anti-virus client protects servers against many different types of malware including ransomware. Servers missing this protection are at far greater risk of being compromised in a successful cyber-attack, or of being used as part of a wider cyber-attack against other council systems than those with the anti-virus client present.

9. All servers that support the Council's anti-virus software should have it installed at build as the potential impact from not running the anti-virus client is high, so the tolerance threshold is low.

Workstations without anti-virus

10. This KPI measures the number of workstations (end user devices including tablets/laptops/desktops) that do not have anti-virus installed. The anti-virus client protects workstations against many different types of malware. Workstations missing this protection are at a far great risk of being compromised in a successful cyber-attack as part of the normal daily work of staff checking email and using the internet. A successful attack could be used to steal credentials and allow business critical data to be stolen, modified, or deleted.

11. All workstations that support NCC's anti-virus software should have that software installed and working.

Servers with unpatched vulnerabilities

12. This KPI measures the number of servers with unpatched vulnerabilities. Vulnerabilities are flaws in software code that can be exploited to make the software work in unintended ways. For example, by granting access to an application even when the password is wrong or allowing a virus to be installed and run leading to a successful cyber-attack. Vulnerabilities are involved in such a high proportion of successful cyber-attacks that the National Cyber Security

Centre (NCSC) state that "…patching remains the single most important thing you can do to secure your technology, and is why applying patches is often described as 'doing the basics'.

Workstations with unpatched vulnerabilities

13. This KPI measures the number of workstations with unpatched vulnerabilities. Vulnerabilities are flaws in software code that can be exploited to make the software work in unintended ways. For example, by granting access to an application even when the password is wrong or allowing a virus to be installed and run leading to a successful cyber-attack.

Other Options Considered

14. No other options have been considered in this report.

Reason/s for Recommendation/s

15. To provide continual assurance of ICT's Operational performance against an agreed set of understandable and measurable criteria.

Statutory and Policy Implications

16. This report has been compiled after consideration of implications in respect of crime and disorder, data protection and information governance finance, human resources, human rights, the NHS Constitution (public health services), the public sector equality duty, safeguarding of children and adults at risk, service users, smarter working, sustainability and the environment and where such implications are material they are described below. Appropriate consultation has been undertaken and advice sought on these issues as required.

RECOMMENDATION

That the contents of the report be noted and a further report for the next quarter be brought to a future meeting of the Committee.

Paul Martin
Head of Technology & Digital, Finance, Infrastructure and Improvement

For any enquiries about this report please contact:

Paul Martin on 0115 977 5722

Constitutional Comments (KK 30/09/2021)

17. The proposals in this report are within the remit of the Finance Committee.

Financial Comments [RWK 30/09/2021]

18. There are no specific financial implications arising directly from the report.

Background Papers and Published Documents

- None

Electoral Division(s) and Member(s) Affected

- All