Agenda Item 5

TO: Overview and Scrutiny Committee

FROM: Head of ICT and OHU - John Fagg

PRESENTING OFFICER(S) Head of ICT and OHU - John Fagg

Telephone: 07825 506687

Email: john.fagg@cambsfire.gov.uk

DATE: 4 October 2023

Cyber Security Update Report

1. Purpose

1.1 The purpose of this report is to provide the Overview and Scrutiny Committee with an update on the current position with regards cyber security.

2. Recommendation

2.1 The Committee is asked to note the contents of this report.

3. Risk Assessment

3.1 **Political** – the ongoing situation in Ukraine has elevated the risk of cyber incidents across the world. Public sector organisations in the United Kingdon are seen as potential targets for foreign state actors.

3.2 **Economic** – with the current financial situation, cybercrime has the potential to rise where individuals see it as a relatively easy and low risk source of income. Therefore, less sophisticated attacks are also possible as novice cyber criminals enter the field.

3.3 **Technological** – technological advancements and the ease of accessibility for relatively inexperienced individuals to source malware via software as a service (SaaS) portals is increasing. The reliance on technology by businesses means that any cyber incidents can pose a risk to continued operations.

3.4 **Legal** – cybercrime poses a risk to data security. The Data Protection Act requires organisations to protect personal data from compromise. Any cyber incident leaves the Service open to investigation by the Information Commissioner and poses financial and reputational risks.

4. Current Position

4.1 Cyber risks are ever apparent within all areas of business. Although usually for financial reward, attacks may also look to seek publicity or to deprive the public of services. Attackers take advantage of wider political and social economic situations to launch attacks and target unsuspecting members of staff. Nationally, cyber incidents have increased as a result of events in Ukraine, either through targeted or untargeted attacks.

4.2 Cambridgeshire Fire and Rescue Service (CFRS) has always taken cyber security seriously, being only one of two fire and rescue services to have achieved and maintained their ISO 27001 (Information Security Management) accreditation. This standard requires regular external audits from the British Standards Institution (BSI) inspectors to ensure compliance is being maintained. The last full recertification inspection in May 2023 identified only two minor non-conformities and three opportunities for improvement. Our Information Governance Manager continues to monitor and audit performance against this standard internally, working with the BSI during any external audits.

4.3 A requirement of the ISO 27001 certification is to conduct annual penetration testing of the ICT infrastructure to identify any areas of vulnerability. The evaluation involves conducting external, internal and social engineering testing by an accredited external company. The reports generated are clearly confidential due to the nature of any findings. Any remediation plans following the receipt of the reports are put into place to ensure critical and high risk vulnerabilities are rectified as a matter of urgency, with a further plan in place to address, where appropriate, any medium and low risk vulnerabilities. Additionally, a penetration test of the mobilisation system is required post any major system change as part of the Code of Connection requirements for the Airwave communication system. The requirements for this will continue with the move to new connectivity requirements for control room solutions and the future move to the Emergency Services Network (ESN).

4.4 Since an independent audit of our cyber security position in 2021, a number of enhancements have been made and additional cyber security tools have been implemented. These tools will ensure that we are well placed to quickly identify possible threats and isolate them.

4.5 In the second quarter of 2023, CFRS were invited by the Home Office to participate in an assessment by IBM against the Cyber Assessment Framework (CAF). The results of this have now been received and have confirmed further that CFRS is in a positive position with regard to cyber security. Some areas for improvement were identified but these had already been recognised and were being progressed.

4.6 ICT staff are informed of any new cyber threats via the National Cyber Security Centre's (NCSC) Cyber Incident Sharing Partnership (CiSP). This is a secure, online forum to exchange cyber security information in real time, in

a confidential and dynamic environment. Our free membership increases situational awareness. When appropriate, cyber threats are also shared directly by the Home Office on behalf of the NCSC.

4.7 The ICT Shared Service staff also sign up to the NCSC Early Warning Service. This provides timely notifications about possible incidents and security issues. The service automatically filters through trusted threat intelligence sources to offer specialised alerts for organisations so they can investigate malicious activity and take the necessary steps to protect themselves.

4.8 In summary, CFRS is in a good position with regard to defensive technologies and its ability to respond to any perceived or actual cyber incident.

BIBLIOGRAPHY

None