Agenda Item: 4

To:	Overview and Scrutiny Committee
From:	Head of ICT and OHU - John Fagg
Presenting Officer:	Deputy Chief Executive Officer – Matthew Warren
	Telephone: 01480 444619
	Email: matthew.warren@cambsfire.gov.uk
Date:	21 April 2022

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 and make comments as they deem appropriate.

3. Risk Assessment

3.1 Political – the current situation in Ukraine has elevated the risk of cyber incidents across the world. Public sector organisations in the UK are 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; less sophisticated attacks are 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 mean 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 posing 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-attacks increased as a result of the COVID-19 pandemic and the recent events in Ukraine have elevated risks of cyber security incidents further, either through targeted or untargeted attacks.

4.2 Cambridgeshire Fire and Rescue Service (CFRS) has always taken cyber security seriously, being the only fire service to have achieved and maintained their ISO 27001 (Information Security Management) accreditation. This standard requires regular external audits from the British Standard Institute (BSI) inspectors to ensure compliance is being maintained. The last full recertification inspection in April 2021 identified only two minor non-conformities and highlighted a number of areas of good practice. The 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 vulnerabilities. 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 the new system solution and the future move to the Emergency Services Network (ESN).

4.4 In 2021, CFRS engaged an independent company (jointly with Bedfordshire Fire and Rescue Service) to validate existing cyber measures, security tools and training to identify any areas of improvement. They confirmed that we were in a good position compared to many other businesses that they had audited but did make a number of suggestions on areas that could be further enhanced. The ICT Shared Service staff have been evaluating a number of options as a result of the external recommendations, with further investment in cyber security tools to be made this financial year. These will primarily be to automate some areas of system monitoring to relieve pressure on staff and to ensure any future cyber incidents are quickly identified and mitigated.

4.5 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.

4.6 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.

4.7 CFRS are therefore in a good position with regard to defensive technologies and our ability to respond to any perceived or actual cyber incident.

Bibliography

Source Documents: None