Cheshire East Council

Working for a brighter future together

Corporate Policy Committee

Date of Meeting:	3rd March 2022
Report Title:	Cyber Security Update
Report of:	Jane Burns, Executive Director Corporate Services
Report Reference No:	CP/64/21-22
Ward(s) Affected:	N/A

1. Purpose of Report

1.1. This report provides an update on Cyber Security within the Council and outlines key aspects to assure the Committee that information is continued to be treated as a valued asset, with ongoing measures to protect and manage it in line with compliance.

2. Executive Summary

2.1. Threats to the Cheshire East Council's Information Security arrangements are recognised on the Council's Strategic Risk Register (SR4 Information Security and Cyber Threat).

2.2. Cyber Security is defined as the protection of computer systems from the theft or damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide. One of the most widespread and damaging threats to materialise is the ransomware exploit. It comes in several variants, each becoming more sophisticated in techniques for spreading and exploitation. The ransomware is designed to extort money from victims through social engineering and intimidation.

2.3. This briefing note seeks to assure members across a number of areas about the protections in place to mitigate any associated risk.

3. Background

3.1. Cyber Risks are becoming more widespread and more sophisticated and the skills and technologies to carry out these attacks are easily acquired by

non-technical criminals from the ‘dark web’. The Covid-19 pandemic has increased criminal activity across several areas including the rise of cyber threats as highlighted by the National Cyber Security Centre.

3.2. As recently published Governments Cyber Security Strategy “the government remains an attractive target for a broad range of malicious actors, with approximately 40% of the 777 incidents managed by NCSC between September 2020 and August 2021 affecting the public sector. This is expected to continue to grow.”

3.3. In 2020, both Redcar & Cleveland and Hackney councils were hit by ransomware attacks. Despite the relatively small sizes of these organisations the impact on critical public services was disproportionate and acute. These attacks are not an anomaly but part of a significant upward trend.

3.4. The Redcar and Hackney attacks have been estimated to have cost £10m for each Council and affected hundreds of thousands of residents. Most systems were recovered within 4 months, but some had taken upwards of six months to recover.

3.5. It is now commonplace for organisation to be targeted, and the Council has valuable information and resources that an attacker would likely seek to exploit.

3.6. It is noted that threats from nation state actors is of considerable concern, with nearly half of nation state activity being targeted at governments across the world, with the UK being the third most targeted country behind the USA and Ukraine. The NCSC is currently investigating the recent reports of malicious cyber incidents in Ukraine. Incidents of this nature are similar to a pattern of Russian behaviour seen before in previous situations, including the destructive NotPetya attack in 2017 and cyber-attacks against Georgia. The UK Government has attributed responsibility for both these attacks to the Russian Government.

3.7. The Cyber Security Strategy states that “while use of ransomware rises, the costs of remediating the impact of ransomware attacks remain significant. This only reinforces the need for strong cyber resilience and strengthens the case for appropriate cyber security prioritisation and investment, to mitigate the risks before they turn into serious incidents”.

4. Briefing Information

Awareness

4.1. To understand cyber risks numerous resources and guidance are used to help understand potential threats and issues including linking to local WARPs (Warning Advice and Reporting Points), government advice and guidance through the NCSC (National Cyber Security Centre) and the LGA (Local Government Association), whilst also monitoring cyber security best practice from industry product specialists and suppliers.

- LGA Cyber Maturity report has been used to help identify any gaps.
- Participation in the National Cyber Security Programme (NCSP) including access to the Resilience Direct Cyber Hub
- ICT Security have subscribed to use several NCSC resources e.g., CNR (CERT UK Reporting Network/ and the Network Early Warning Service (NEWS), ACD (Active Cyber Defence) portal incorporating Web check, Mailcheck and PDNS, and through these channels have contact to NCSC representatives.

4.2. The Council has a membership with iNetwork and NWWARP (North West WARP) and are working with the NCSC on trial reporting capabilities to increase awareness and visibility of emerging threats.

NWWARP membership includes quarterly meetings to discuss relevant technology and security developments and enhancements within the marketplace, access to the KHub (Knowledge Hub Portal), and CISP (Cyber Security Information Sharing Partnership) platform, which provide opportunity to review government cyber updates and initiatives with other northwest NHS and LA representatives.

4.3. The security landscape is changing so ICT staff regularly review process and policies, against issued best practice and guidance. The LGA offered a funding grant (2020/21) in which they recognised that an authority of this size needed two staff at a certain level of formal training for its IT staff. The grant has been used to train six officers to a level of Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM).

4.4. The Council has been working with the Department for Levelling Up, Housing and Communities (DLUHC) to access additional funding with a view to improve the Council's security posture. A joint workshop was held where areas of risk were discussed and following this a Risk Treatment Plan was developed. This has been submitted to the DLUHC to assess and a decision on funding is expected February 2022.

4.5. The ICT Security team keep abreast of evolving technology trends and reporting to support and protect the authority's information assets, to the best of its ability, from emerging threats impacting service delivery.

4.6. It is important that the Council's workforce cyber culture and behaviours are continually assessed and developed, there is mandatory information handling training, cyber awareness training and simulated phishing attacks through which risks can be mitigated.

Protection

4.7. The Council is moving from a traditional ICT Service infrastructure into one that employs several technologies such as “cloud”. This offers several benefits, but the risks afforded need a different approach to security. It is essential that the Council moves Cyber Architecture into a position where the maximum amount of protection can be applied to its Information Assets to offset the risks generated through the rise of malware and in particular ransomware.

4.8. The traditional approach of a perimeter defence with your valuable assets protected inside is one many still adopt however it comes with some limitations and some risk. An approach such as “zero trust” would allow the Council a greater level of security whilst allowing a greater flexibility in deploying technologies and using information effectively. The main concept behind zero trust is “never trust, always verify,” which means that users and devices should not be trusted by default.

4.9. A Security and Compliance business case has been developed to enable the Council to move to a zero-trust model and mitigate the increasing risks and challenges from cyber-attacks, agile working and increased sharing of information.

Recovery

4.10. The Council creates regular backup copies of its live production data hosted in the core data centre. It is sent over the Cheshire WAN to an offsite location away from the main data centre. The same solution is used for some of the data held in our Azure cloud with the remainder using Azure Backup services. Investigations are underway to modify the on-premises backup system to make additional offline/air gapped backup copies of data.

4.11. With the trend to Software as a Service (SaaS), vendors are responsible for the ensuring the availability and security of their services. A standard ICT Security questionnaire issued to all vendors is used to determine whether they follow best practice and meet the security standards expected for storing, protecting, and processing Council data.

4.12. Where possible, the Council is adopting a Single Sign On approach to accessing SaaS based applications. This means that security best practice such as password controls, Multi-Factor Authentication (MFA) and conditional access can be applied to further secure who can access data, from what device, and from what location.

The Council is currently looking at options to take an offline backup of information held in Microsoft 365 to allow continuity should the service be unavailable for a prolonged period of time and to provide a further level of protection against ransomware resulting in data encryption or deliberate data deletion.

5. Implications

5.1. Legal

5.1.1. The Council must comply with the General Data Protection Regulation (GDPR), the Data Protection Act 2018, the Computer Misuse Act 1990, the Freedom of Information Act 2000 and other relevant legislation in particular that relating to retention of information.

5.1.2. GDPR has brought in substantially higher levels of penalties for data controllers than the previous legislation, up to €20 million (£17m) or 4% of annual worldwide turnover although it is capped at €20 million for public authorities. GDPR has also introduced fines for data processors.

The Council needs to understand what data they control and what is processed on their behalf and build data protection into its day to day processes to ensure that it and organisations processing data on its behalf are compliant.

5.2. Finance

5.2.1. Compliance with GDPR and UK data protection legislation is mandatory; penalties for the Council as a Data Controller under GDPR can be up to €20 million.

5.3. Human Resources

5.3.1. Under the new GDPR data subjects have several rights in relation to their personal data, including confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. This requirement cannot be met if information is not managed in a compliant manner or used as a storage mechanism for information.

Access to Information	
Contact Officer:	Gareth Pawlett, Chief Information Officer and Head of ICT Services Gareth.Pawlett@cheshireeast.gov.uk
Appendices:	None
Background Papers:	N/A