Cheshire East Council

Working for a brighter future together

BRIEFING REPORT

Corporate Policy Committee

Date of Meeting:	23rd March 2023
Report Title:	Cyber Security Update
Report of:	Jane Burns, Executive Director Corporate Services
Report Reference:	CP/38/22-23

1. Purpose of Report

1.1. This report provides an update on the status of Cyber Security within the Council and outlines key aspects to assure the Committee that information continues to be treated as a valued asset, with on-going 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). This risk is reviewed on a quarterly basis.

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 using social engineering and intimidation through phishing attacks. The malware steals the information and holds it hostage with threats of releasing it into the public domain if a ransom payment is not received.

2.3. This briefing note seeks to assure members across several 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 Internet can be described as having three discrete elements. There is a "Surface" web such as Google, Wikipedia and publicly available information, there is the "Deep" web where sensitive information is held i.e., bank accounts, Health & Social Data etc. Then there is the "Dark" web where there are illegal marketplaces, anonymous journalism, ransomware data. Typically, you can't browse to these sites without using specialised software.

3.2. There are many ransomware groups operating and storing their data in this "dark" web. A number of these groups have made enormous sums of money and there are suggestions that they are becoming sophisticated and joined up and are actively protecting themselves. The Council actively monitors that its data is not being stored by ransomware groups on this web.

3.3. The escalation of armed conflict has increased criminal activity across several areas including the rise of cyber threats as highlighted by the National Cyber Security Centre. Amongst this criminal activity there are several groups who have authorized agents working for sovereign powers.

3.4. The NCSC Annual Statement published August 2022 states that there were 2.7m cyber-related frauds in the 12 months to March 2022 in the UK. It also reports that 39% of all organisations have identified a cyber incident, of that 39% most (83%) said they had been targeted by phishing attacks. Approximately a fifth of those organisations impacted said that had been subjected to a more sophisticated attack such as a denial of service, malware, or ransomware attack.

3.5. In 2022, the Costa Rica Government declared a national emergency in response to a cyber-attack. There were attacks across different sectors, firstly the finance sectors in both government and the private sector. A further attack concentrated on the nation's healthcare system. These attacks were carried out by multiple ransomware groups and can be seen as examples of the devastation they can bring not out only to an organisation but on an entire nation.

3.6. It is now commonplace for organisations to be targeted with ransomware . The Council has valuable information and resources that an attacker would likely seek to exploit.

3.7. It is noted that threats from nation state actors are 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 stated that "During the invasion, Russia sought to use offensive cyber operations to support their military campaign", it also

gave a warning that “China’s technical evolution is likely to be the single biggest factor affecting the UK’s cyber security in the future”.

3.8. 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.
- 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 and Mail Check, 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.

4.3. NWWARP membership includes quarterly meetings to discuss relevant technology, 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.

4.4. The security landscape is changing so ICT staff regularly review process and policies against issued best practice and guidance. The LGA offered a further funding grant (2022/23) to train a member of staff to a level of Certified Information Systems Security Professional (CISSP).

4.5. 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

development. Following on from this workshop a funding grant of £150,000 was received to cover a number of mitigations that were jointly agreed.

4.6. The ICT Strategy 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.

4.7. ICT Services have built on their existing capabilities in cyber security to set up a new team (SecOps) dealing with Security Operations, this team co-ordinates ICT security operational monitoring activity across the Council. The SecOps function has set clear goals such as fostering security collaboration across all ICT teams, ensuring that security best practice is followed across the supply chain. It is responsible for implementing an incident response plan, which defines how the organisation detects a cyberattack and reacts to it. It will also conduct forensic analysis by analysing information which can help determine the root cause of security incidents, performance issues, or other unexpected events.

4.8. 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 understood and mitigated.

Protection

4.9. The Council have invested in improved security protection and detection capabilities through Microsoft 365 E5 licences and the Defender suite of products. This provides a holistic view of security across applications, email, documents, devices, servers, users and identity. The output from this tooling is used by the SecOps team to investigate and mitigate identified risks and to drive improvement in the configuration of both strategic and legacy systems.

4.10. The new Defender tools add automated detection capabilities such as spotting if a user is accessing from an unusual location, or if a user is exhibiting unusual behaviour such as deleting a large number of files in a single session. These alerts are flagged to the SecOps team for further investigation. Integration with Outlook has added an easy to use "Report Phishing" button to allow users to quickly report suspicious emails for further investigation. If found to be malicious the SecOps team can quickly remove all instances of the email from end user mailboxes, and even see which have been opened and links clicked. User machines can be remotely scanned for malware and if necessary, isolated from the network whilst further investigation is carried out.

4.11. A full software inventory is automatically gathered from all user machines and servers, with versions of software with known vulnerabilities flagged for remediation. This also helps with licensing compliance as it is straightforward to see which software is installed and where, and on how many devices. “Shadow IT” detection allows usage of unsanctioned web applications to be identified to help guard against inappropriate sharing of data using unapproved services that might not have appropriate data handling or security controls.

4.12. 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. The Council is moving its 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.

4.13. 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. The Council is adopting a Zero Trust framework which will 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.

4.14. A Security and Compliance business case was developed to define how 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. The Council has been working with a third-party in Info-Tech who have experience in deploying the necessary tools and processes to implement this new way of working.

Recovery

4.15. The Council creates regular backup copies of its live production data hosted in the core data centre.

4.16. With the trend to Software as a Service (SaaS), vendors are responsible for 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.

4.17. 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. A number of applications have been redeveloped to support this authentication method and the Council will continue to adopt this model.

4.18. The enhancement and investment that the Council has made in a range of technologies including Microsoft will enable it to benefit from increased levels of protection and business contingency should an incident occur.

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.

5.1.3. 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:	N/A
Background Papers:	N/A