OPEN

Corporate Policy Committee

11th July 2023

Cyber Security Update

Report of: Alex Thompson, Director of Finance and Customer Service

Report Reference No: CP/13/23-24

Purpose of Report

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.

Executive Summary

2 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 managed daily with quarterly reporting of any changes in the period.

3 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.

4 This briefing note seeks to assure members across several areas about the protections in place to mitigate any associated risk.

Background

5 There are many ransomware groups operating and storing their data in the “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.

6 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.

7 The NCSC state that

(a) “over the past 18 months, a new class of Russian cyber adversary has emerged. These state-aligned groups are often sympathetic to Russia’s invasion and are ideologically, rather than financially, motivated.

(b) Although these groups can align to Russia’s perceived interests, they are often not subject to formal state control, and so their actions are less constrained and their targeting broader than traditional cybercrime actors. This makes them less predictable”.

8 It is now commonplace for organisations to be targeted with ransomware. The Council has important information and resources that an attacker would likely seek to exploit. An attack can be used to encrypt the data making it unusable unless the ransom has been paid, or more commonly now to threaten to exposure the data on the internet.

9 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”.

10 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”.

Briefing Information

Awareness

11 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.

ICT Security have subscribed to use several NCSC resources

- CNR (CERT UK Reporting Network)
- NEWS - the Network Early Warning Service,
- ACD (Active Cyber Defence)
  - Web Check
  - Mail Check.

12 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.

13 The security landscape is changing so ICT staff regularly review process and policies against issued best practice and guidance.

14 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. A funding grant of £150,000 was received to cover several mitigations that were jointly agreed. These mitigations projects are in various stages of progress, with anticipated closure for all by the end of financial year 23/24.

15 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.

16 ICT Services and in particular Security Operations actively monitor security data across the Council. The incident response plan has been defined and communicated internally. This plan defines how the organisation detects a cyberattack and reacts to it. It is also conducting forensic analysis of security telematics which can help determine the root cause of security incidents, performance issues, or other unexpected events.

17 An area of increasing concern is the use and manipulation of Artificial Intelligence to design and create sophisticated malware capable of exfiltrating sensitive data.

"[T]his kind of end to end very advanced attack has previously been reserved for nation state attackers using many resources to develop each part of the overall malware. And yet despite this, a self-confessed novice has been able to create the equivalent malware in only a few hours with the help of ChatGPT." – Aaron Mulgrew, Solutions Architect Forcepoint

18 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.

19 Several cyber briefing sessions have been run over the last period, these have included Wider Leadership Community, Manager Share and Support, In the Know (all staff briefing), Secondary Heads and Primary Heads. These have been very well received and aim to make colleagues aware of the actual threat to the Council and partners as well as educate on the potential threat to personal life as well.

Protection

20 The SecOps team manage, investigate, and mitigate risks across the estate to ensure any vulnerabilities are minimised or eradicated. Event logs are collected in real time and analysed to ensure any irregularities are investigated. This analysis is currently carried out in house, but further work will investigate whether external organisations can be best used to provide this analysis during non-traditional working hours.

21 There are several tools that are used to protect the estate, particularly through the Microsoft capabilities recently procured and implemented. These will further be enhanced to enable protection of key information assets through the configuration of policy rules. These will prevent the accidental release of critical information inside and outside the authority.

22 The Council has adopted 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.

23 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 move to this concept of zero-trust will be a multi-phased approach (as detailed in the business case) across several years for the estate to be fully covered. A framework and plan are being developed to ensure this strategy will be implemented and any new and change projects will have the concept incorporated in their design.

Recovery

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

25 There is increased coverage and interest in third party breaches, with hackers compromising the system of a third-party provider. These third-party data breaches can be difficult to prevent and manage due to uncertainty of the vendors’ security systems and protocols.

26 To understand and protect the Council’s information ICT will need to have awareness and contact with all Information and Technology providers which have a Council interaction. To support this any procurement which involves Information needs to have the support and involvement with the ICT Services. The Council already uses a standard ICT Security questionnaire which is issued to all vendors to determine whether they follow best practice and meet the security standards expected for storing, protecting, and processing Council data. This questionnaire is continuingly evolving to facilitate best practice and changing threats and will need to be further strengthened to incorporate differing offerings that the Council demands.

27 The Council has adopted a principle of Single Sign On for applications. This means that security best practice such as password controls, Multi-Factor Authentication (MFA) and conditional access can be applied to secure who can access data, from what device, and from what location. Several applications have been redeveloped to support this authentication method and the Council will continue to adopt this model.

Implications

Monitoring Officer/Legal

28 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.

29 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.

30 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.

Section 151 Officer/Finance

31 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.

Policy

32 There are no policy implications in this briefing.

Equality, Diversity and Inclusion

33 There are no implications in this briefing.

Human Resources

34 There are no implications in this briefing.

Risk Management

35 There are no implications in this briefing.

Rural Communities

36 There are no implications in this briefing.

Children and Young People including Cared for Children, care leavers and Children with special educational needs and disabilities (SEND)

37 There are no implications in this briefing.

Public Health

38 There are no implications in this briefing.

Climate Change

39 There are no implications in this briefing.

Access to Information	
Contact Officer:	Gareth, Pawlett Head of ICT Gareth Pawlett
Appendices:	None
Background Papers:	None