Southend-on-Sea City Council

Report of the Executive Director (Strategy, Change & Governance)

To

Audit Committee

On

26 April 2023

Report prepared by: Carol Thomas, Director Digital & ICT

Digital & Cyber Security Report

A Part 1 Public Agenda Item

---

1. Purpose of Report

1.1 To update the Audit Committee on the progress made in delivering the Cyber Security Strategy for 2022/23.

2. Recommendations

2.1 **The Audit Committee notes the progress made in delivering the 2022/23 Cyber Security Strategy.**

3. Executive Summary

3.1 Digitalisation and digital enablement are bringing huge change to most organisations. The benefits of these are many and include improved efficiency and more effective services. However the need to digitalise must be balanced with an increased cyber awareness and security.

3.2 As organisations increasingly transact online, they also increasingly become a target for cyber criminals. Keeping the organisation and the data it holds safe, is a race to stay one step ahead of the criminals. It is far more than an ICT issue – it is a strategic organisational risk which should be managed appropriately to ensure that the organisation can continue to deliver services.

3.3 For this reason, the ICT security team work closely with other colleagues across services, including finance, HR and procurement, to ensure that systems are as secure as possible and work to continuously improve our security. People are both the first line of defence and the weakest links, and training and education are ongoing, with a least-privilege approach to system access in support.

3.4 As the broader ICT team work on building a professional Information technology environment which will form the foundation for the future, the security strategy horizons are following in close alignment. Best practice frameworks and standards are being implemented within the budget envelope that has been provided. Security is embedded into the design of new solutions and added to existing tools. Security process maturity continues to grow as these changes are embedded and continuously improved. Controls have been documented and matured as has been noted in the recent cyber incident audit.

3.5 Appendix 1 sets out the threat landscape for local authorities and the horizons of the current security strategy.

3.6 Appendix 2 sets out some statistics related to security incidents, a recent phishing exercise conducted to test awareness, and notes the cyber incident response audit outcome.

3.7 In addition to the Cyber Security work the ICT team support all other services and council sites via the provision of Design Services (enterprise architecture); Project and Programme delivery; Infrastructure and Operations who manage physical infrastructure and networks, and provide a Service Desk; Change Enablement who aid users with change; Commissioning and Performance services who actively manage suppliers and contracts.

4. Reasons for Recommendations

4.1 Cyber security is a strategic risk area. Having oversight of the actions taken within the cyber security function of ICT will provide assurance to assist the Audit Committee to effectively discharge its responsibilities as per its Terms of Reference.

5. Corporate Implications

5.1 Contribution to the Corporate Plan and Southend 2050 Road Map

Digital is an enabler to the Corporate Plan and Southend 2050. Security of the information we hold is essential to achieving the outcomes of these strategic aspirations.

5.2 Financial Implications

The Cyber security activities are scheduled to be delivered within the approved ICT budget.

5.3 Legal Implications

Data Protection legislation requires the Council to protect the data that it is responsible for and having effective cyber security arrangements contributes to discharging this duty.

5.4 People Implications

The ongoing development of officers within the cyber security function is part of the approved ICT Talent Strategy.

5.5 Property implications

None

5.6 Consultation

Cyber security and other information technology risks are part of the regular reporting to Executive Directors and Directors.

5.7 Equalities and Diversity Implications

The relevance of equality and diversity is considered during the planning and implementation of changes to the information technology environment.

5.8 Risk Assessment

Cyber security risk is a strategic risk included in the corporate risk register.

Other risks the team continues to manage are the potential loss of staff and the ability of the service to replace this resource.

5.9 Value for Money

Opportunities to improve value for money in the delivery of services are identified during some reviews and recommendations made as appropriate.

5.10 Community Safety Implications

None.

5.11 Environmental Impact

Increased digitalisation reduces the need to rely on other physical resources and therefore contributes to the Council's environmental objectives.

6. Appendices

Appendix 1	The Threat Landscape and Security Strategy Horizon progress
Appendix 2	Statistics and Cyber Response Audit

Appendix 1: The Threat Landscape and Security Strategy Horizon progress

Statistics from 2022 show that attacks on UK Councils were constantly increasing and the council's security team anticipate that 2023 will reflect similar statistics.[3] National Cyber Security Centre (NCSC) guidance and National Institute of Standards and Technology (NIST) standards form the basis of the security approach, and the team work constantly to further improve to keep the data of the council and residents safe.

Through the work done already the overall security maturity has been improved. Continuous improvement and adapting and avoiding of distraction are key to vigilance. The team recognise that there is no such thing as being 100% cybersecure and therefore are working on preparedness as well as protection and continuously improving security. Users are an essential part of this as they are both the first line of defence and the weakest link, and therefore there is regular training and support offered to all users.

Part of the security approach is to apply a least privilege approach to access, meaning that when access is given it is the minimum possible required to deliver the role and any further access has to be motivated and approved. SCC ICT work closely with NCSC, Local Digital, Essex Police and others to ensure that approaches are aligned to best practices. Tools and approaches are selected that are aligned to our standards and within our budget envelope, ensuring that as far as possible best of breed tools are used to secure council data.

The Threat Landscape: Key Cyber Threats and Risks in the Local Authority Sector[4]

Phishing

The biggest threat facing the sector are phishing attacks with over 50% of phishing attacks directed at government. Phishing arrives via email or messaging and these are very sophisticated, often replicating the logo and information of known people to convince the targets to respond. Those who are most often the targets are councillors, but many other staff are also targeted. There is a form of phishing that now also targets messaging services in mobile devices.

For this reason, cyber security training and refreshing is mandatory for all users, including councillors.

The Council provide phishing training, provide updates via newsletters, and conduct regular phishing exercises to ensure awareness.

A specific email address: phishing@southend.gov.uk is set up for users to report suspect emails. Those users who do click on attachments in the exercise are retrained. The most recent phishing exercise yielded more than 514 users who potentially compromised security, including 13 councillors. The first click was within less than a minute and the first report of the phishing was 5 minutes later. 166 users in total reported the phishing email.

Ransomware

Ransomware is a very real threat to local government[5]. The NHS WannaCry attack in 2017, and several subsequent successful ransomware attacks against local councils have highlighted the need to build awareness and take action to protect our council against the potential reputational and financial risk. At Southend we have a ransomware solution in place which will lock down the network automatically if an intrusion is detected, which has been added to our arsenal of tools.

Insider threats

Insider threats are threats posed by those who may have gained unauthorised access or even disgruntled employees. This is a mode of attack being used by cyber criminals recently – they gain access via a user whose credentials are compromised and use this access to observe (sometimes for months) before taking action. Safeguarding of user credentials and constant vigilance are essential, as is awareness and users are regularly reminded of the need to be careful and vigilant.

SCC Cyber Security Strategy and Horizons

Vision for Cyber Security: "Cyber security will be a demonstrable strength within the organisation, and we shall be an acknowledged leader in local government when it comes to securing the data and technology used in delivering the Council's services. Our current and future digital services will, as well as being innovative, be secure and resilient from cyber-attacks. Whilst keeping people's information and data safe, we will be mindful of privacy and ethics. We will always ensure data is collected and used lawfully and ethically to benefit the residents and visitors to our city."

Digitisation is essential to survive and thrive today, but becoming more digital also exposes an organisation to an ever growing cyber risk threat[1]. Cyber risk is a strategic risk as a successful cyber attack could impact the resilience of the entire council. A Cyber Security Strategy has been in place since late 2022, aligned to the Corporate Plan and Southend 2050. This strategy has three time horizons focused on three aspects of the cyber environment and is due for a review and update in 2023:

Horizon 1: 2020/21: Establish foundational capabilities, and address key enterprise risks [0-18 Months]
To define, develop and deliver foundational level cyber security and ICT capabilities across People, Technology, Information and Process areas. Utilising recognised frameworks and standards to inform the future security architecture, whilst addressing gaps in foundational controls and capabilities through remediation of end user computing, network and infrastructure. In doing so we will be better equipped to manage our own compliance and set appropriate standards for assessing risk and compliance in our supply chain.

Key Outcome: Increase cyber resilience to a level which would be able to maintain Council operations whilst swiftly identifying and responding to repeated known and identifiable threats.

Horizon 2: Improve and Optimise [18 Months to 3 Years]
To Improve and optimise security capabilities through regular measurement and assessment of security controls and capabilities. Exploit opportunities to refine cyber security tactics, techniques, and protocols so that a proactive posture is established to improve prevention, detection and response to cyber events. We will look to further enhance security culture with increased targeted and role-based learning. We will aim to be compliant with all external standards and requirements and have established alignment with our own standards for minimum standards for cyber security.

Key Outcome: Increase cyber resiliency to a level whereby we could withstand repeated known threats and be proactive in monitoring for and responding swiftly to more unknown cyber threats.

Horizon 3: Adapt and Innovate: [3-5 Years]
Continuous improvement of cyber security capabilities seeking out opportunity to innovate and anticipate the future needs of the SBC organisation, people technology and threat landscape. Adapt dynamically to changes in the threat landscape or through business change. Be able to quickly measure compliance and adherence to standards and external requirements.

Key Outcome: Be able to adapt quickly to the changes in threat landscape and respond swiftly to more complex, unknown and advanced and persistent threats.

Horizon 1 was delivered in late 2021 and the work on Horizon 2 began once horizon 1 was delivered. Horizon 3 will begin towards the end of 2023, and overlaps horizon 2.

SCC ICT have conducted maturity assessments, improved capabilities within the ICT team and collaboration with other service areas. The control environment has improved through the application of standards and frameworks and over the past year the council have taken part in DLUHC Digital[2] work to build a cyber assessment framework for local authorities and gained some useful insights and some funding for the work.

The ICT security team participate in the NCSC portal which is a platform for information sharing within government departments. It monitors current incidents, provides early warnings, shares information, conducts cyber assessments and provides general technical support to government authorities. The team also belong to the Cyber Information Sharing Partnership (CISP) a joint industry and government digital service for sharing of cyber threat information in a secure and confidential environment. The Council is also part of the Essex Digital Partnership and the (National Local Authority Warning, Advice and Reporting Point (NLAWARP).

Supporting links

[1] Cyber Security Outlook 2023 - PwC UK

[2] Insights from the Cyber Assessment Framework for Local Government pilot - DLUHC Digital (blog.gov.uk)

[3] Cyber-criminals are increasingly targeting UK councils, with more than two million attempted attacks recorded in 2022 to date. There has been a 14% rise in the number of cyber-attacks year-on-year. Phishing attacks are the biggest threat to councils with 75% stating it is the most common type of cyber-attack experienced.

UK councils hit by 10,000 cyber-attacks every day so far in 2022 | Gallagher UK (ajg.com)

Appendix 2: Statistics and Cyber Response Audit

The council receives and sends a significant volume of email. On average 2 million emails are sent (0.5 million) and received (1.5 million) every month. These emails are automatically scanned using an industry standard database for known malicious senders, with emails from these senders then blocked. On average 100,000 are blocked every month, and a further 45,000 emails are sent to junk mail folders.

Over 420,000 MS Teams chat messages are shared every month, and approximately 14,000 meetings held every month.

There are 5.7 million files stored in Onedrive and a further 5 million stored in Sharepoint. 63,000 of these were viewed in the last month. All Onedrive files have been migrated to a cloud environment, with planning for the Sharepoint migration in flight.

Security Statistics

Over the past six months 253 account breach attempts have been stopped and the team have resolved 29 malicious URLs clicked by users.

Penetration testing has been conducted on a legacy tool used by one of the services and high-risk vulnerabilities found. The supplier has been approached to fix their security weaknesses. A review of security in proposed new tools and websites, and a policy to manage this, is being considered for ongoing standard practice.

Cyber Incident Response Audit

A cyber incident response audit was conducted in late 2022, which noted satisfactory assurance and made six recommendations to improve the cyber incident response further.

[1] Cyber Security Outlook 2023 - PwC UK

[2] Insights from the Cyber Assessment Framework for Local Government pilot - DLUHC Digital (blog.gov.uk)

[3] Cyber-criminals are increasingly targeting UK councils, with more than two million attempted attacks recorded in 2022 to date. There has been a 14% rise in the number of cyber-attacks year-on-year. Phishing attacks are the biggest threat to councils with 75% stating it is the most common type of cyber-attack experienced. UK councils hit by 10,000 cyber-attacks every day so far in 2022 | Gallagher UK (ajg.com)

[4] The 4 Top cyber threats for cities and governments in 2023 (imagineiti.com)