Report to:	Audit and Governance Committee	**Date of Meeting:**	Wednesday 15 March 2023
Subject:	Cyber Security Assurance		
Report of:	Executive Director of Corporate Resources and Customer Services	**Wards Affected:**	(All Wards);
Portfolio:	Cabinet Member – Regulatory, Compliance and Corporate Services		
Is this a Key Decision:	No	**Included in Forward Plan:**	Yes
Exempt / Confidential Report:	No		

Summary:

This report outlines the external assurance sought in relation to the Cyber Security of Sefton Council, it sets out the key findings from three key assessments completed in 2022, further improvement plans in progress and key next steps.

Recommendation(s):

That Audit and Governance Committee note the content of the report and endorse the ongoing programme of work.

Reasons for the Recommendation(s):

The purpose of the report is to ensure that members of Audit and Governance committee are sighted on the external assurance completed in regard to the security of Sefton's ICT Infrastructure

Alternative Options Considered and Rejected: (including any Risk Implications)

Not applicable

What will it cost and how will it be financed?

Costs are contained within the existing revenue budgets aligned to the ICT Client Team

Implications of the Proposals:

Resource Implications (Financial, IT, Staffing and Assets):

Financial:

None, any costs will be contained within existing budgets

IT:
The external assurance complements the internal verification of our security posture and ensures that Sefton has robust plans in place to improve the cyber security of the Councils network.

Staffing:
Not applicable

Assets:
Not applicable

Legal Implications:

There are no legal implications

Equality Implications:
There are no equality implications.

Climate Emergency Implications:

The recommendations within this report will

Have a positive impact	N
Have a neutral impact	Y
Have a negative impact	N
The Author has undertaken the Climate Emergency training for report authors	Y

The content of the report does not propose any changes that impact on the climate emergency

Contribution to the Council's Core Purpose:

Protect the most vulnerable:

No direct implications but the provision of a secure and robust network will ensure the continued delivery of key council services.

Facilitate confident and resilient communities:

No direct implications but the provision of a secure and robust network will ensure the continued delivery of key council services.
Commission, broker and provide core services: No direct implications but the provision of a secure and robust network will ensure the continued delivery of key council services.
Place – leadership and influencer: No direct implications but the provision of a secure and robust network will ensure the continued delivery of key council services.
Drivers of change and reform: No direct implications but the provision of a secure and robust network will ensure the continued delivery of key council services.
Facilitate sustainable economic prosperity: No direct implications but the provision of a secure and robust network will ensure the continued delivery of key council services.
Greater income for social investment: No direct implications but the provision of a secure and robust network will ensure the continued delivery of key council services.
Cleaner Greener No direct implications but the provision of a secure and robust network will ensure the continued delivery of key council services.

What consultations have taken place on the proposals and when?

(A) Internal Consultations

Consultation has taken place with colleagues within Agilisys our ICT Operational Services Provider.

The Executive Director of Corporate Resources and Customer Services (FD.7170/23.....) and the Chief Legal and Democratic Officer (LD.5370/23....) have been consulted and any comments have been incorporated into the report.

(B) External Consultations

Not applicable

Implementation Date for the Decision

Following the expiry of the "call-in" period for the Minutes of the Cabinet Meeting

Contact Officer:	Helen Spreadbury
Telephone Number:	07583 057822
Email Address:	helen.spreadbury@sefton.gov.uk

Appendices:

There are no appendices to this report

Background Papers:

There are no background papers available for inspection.

1. Introduction/Background

1.1 Cyber risk has grown exponentially over the last two years, the risk of an Information Security Breach due to a cyber-attack features on the Corporate Risk Register and although Sefton has made significant investment in its security tools, polices, and licenses the threat to our network is still significant.

1.2 The number of Cyber-attacks per week on corporate networks across the world increased by 50% in 2021 compared to 2020, this peaked in December 2021 with a major vulnerability identified Log4j. 1 in 61 worldwide organisations are impacted by Ransomware each week, with attacks on Education and Research organisations up 75% and Government and Military organisation attacks up 47%

1.3 The most common type of attack is an email Phishing attack (83% of attacks on businesses are Phishing attacks) this is followed by impersonation attacks at 23%.

1.4 In Sefton we have seen a 50% rise in Phishing emails since January 2022, with on average 30,000 attacks per month in October and November last year. We are also targeted each month with Malware (emails containing virus's) as well as receiving between 200 and 400 brute force attacks on our network each month. These attacks are all blocked by the technology and policies we have put in place and the recent introduction of new tools have also prevented further attacks on our network.

1.5 Local Government across the UK is being targeted, recent examples include

- February 2020, Redcar and Cleveland Council, total cost more than 7 million and had significant impact on service delivery including, the online appointments, bookings, social care advice and the housing complaints system. At the time of the attack the council had standard industry tools in deployed to prevent an attack.

- October 2020, Hackney Council, total cost to the Borough at least 12 million. The attack by organised criminals rendered key financial and operational

systems inaccessible and paralysed several council services, including its ability to make and receive payments and take applications for its housing waiting list. It forced the borough to make changes to its planning processes, saw stolen resident data published on the dark web, and even froze the local property market after land searches became impossible

- December 2021, Gloucester City Council were subject to a cyber-attack which affected the council's online revenues and benefits services as well Planning and Customer Services. The attack was a result of Malware being sent to a Council member by email. Initially residents were unable to access interactive online application forms used to claim for housing benefit, council tax support, test and trace support payments and discretionary housing payments, as well as the planning application website.

2.0 Cyber Security Assurance – Sefton Council

2.1 Sefton Council has developed an ongoing Security Improvement plan in partnership with the ICT Managed Services Provider Agilisys. This work programme is reviewed monthly considering the threat profile and further remediations planned or updated to take account of the changing landscape.

2.2 Over the last 12 months significant work has been completed to prevent an attack on the Sefton Network, this includes implementation of new security standards as advised by the National Cyber Security Centre, the deployment of new security tools released by Microsoft and a review of training materials released to all network users across Sefton.

2.3 Sefton's last line of defence against a Cyber Attack is its staff, in addition to the technical tools and policies regular updates and briefings are circulated to teams via the Intranet, One Council Briefings and via ICT Champions and Information Asset Owners. Dedicated Cyber training is also available to all members.

3.0 External Assurance

Each year the Council undertakes an IT Health Check, which includes an external penetration test in line with the requirements of the Public Services Network (PSN). This test and evidence are submitted to the Cabinet Office for approval for connection to the Public Services Network. Sefton Council completes this process yearly and has a current connection. However, considering the escalating threat landscape Sefton opted to complete two further external verification exercises to further check the security tools, protocols and policies implemented, and importantly the understanding of these across the organisation. The team elected to complete take part in the following

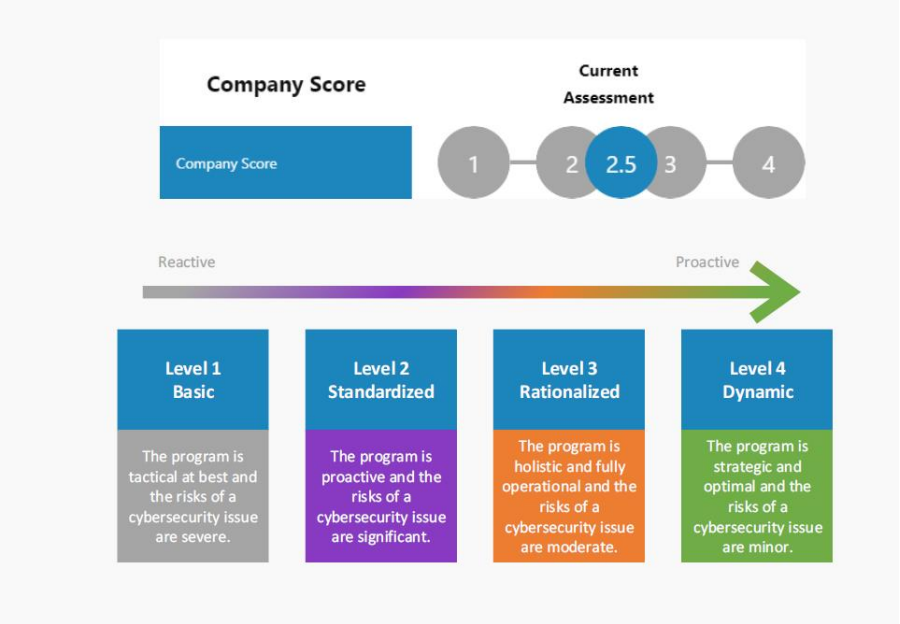
- Microsoft's Cyber Security Assessment
- LGA Cyber 360

4.0 Microsoft Cyber Security Assessment (CSAT)

The Microsoft Cyber Security Assessment was carried out in July 2022 for Sefton, it provides an overall review of the cybersecurity position and practices of the

Council, as assessed through a questionnaire and an automated scan of security related data and deployed settings. It is important to highlight that the Microsoft tools only look for Microsoft Products so in cases where Sefton has something other than a Microsoft tool to meet a requirement this would not be picked up by the CSAT assessment and would be reported as a gap. However, it was felt by the Sefton team that this would still be an incredibly useful exercise to complete as it would help Sefton gain insights into threats across, email, identity, and data to better understand, prioritise, and mitigate potential vectors of cyber-attacks against the Council.

4.1 At the end of the assessment Sefton received and overall maturity level score



To add some context into this score, the Microsoft evaluation team advised that across the CSAT assessments completed for other Councils within the UK District Councils/ County Councils/Borough Councils/Metropolitan BCs and from 18 organizations assessed the average company score achieved was 2.3. Sefton has scored 2.5 and out of 18 other councils assessed (excluding Sefton MBC) only 4 had company scores that met or exceeded 2.5. As highlighted earlier had this assessment considered the non-Microsoft products in place the score would have increased substantially.

4.2 The detailed report from Microsoft provided recommendations for improvement these recommendations were captured within the Security Improvement Plan and all actions monitored to closure.

4.3 It is proposed to revisit the CSAT in Summer 2023.

5.0 Local Government Association (LGA) Cyber 360

5.1 In October 2022 Sefton took part in an LGA Cyber 360 exercise, the main aim of the Cyber 360 is to support Councils as they work to reduce Cyber Risk. The approach aims to help Councils build cyber capabilities and improve

understanding of Cyber Security principles across the organisation, not just in IT teams.

The 360 Framework brings together existing frameworks and advice from:

- National Cyber Security Centre
- Scottish Government
- Information Security Forum
- National Institute of Standards and Technology
- Cabinet Office
- NHS Digital
- Centre for Internet Security

The 360 covers the following dimensions

5.2 The Cyber 360 team spent three days with Sefton Council on the 19th, 20th and 21st of October 2022. The key findings of the team were as follows

5.2.1 Following a large-scale IT transformation programme, the council is developing a strong cyber security culture. This is due to the strength of leadership within the council, the hard work and diligence of the security team, and the formation of good relationships and partnerships with key providers. This is the key finding of the C360 and the context for all subsequent observations. However, LGA report also stated that they have also sought to identify areas for learning and improvement.

5.2.2 A few key personnel in the council bear significant responsibility for decision-making about cyber risks, technical expertise, and communication in relation to cyber-security. The council is aware of this potential overreliance on these individuals and is looking at ways to manage this. One option is to create processes and procedures which empower service areas to take on more

responsibility themselves in relation to managing cyber risks, updating plans, and considering cyber security in supply chains. This would release some capacity within the IT team, build knowledge across the organisation, and share ownership of cyber security

5.2.3 Despite limited resources, Sefton appears to have made significant progress in implementing various cyber-security controls. The council could now consider how to balance these controls with its wider business objectives, to grow a cyber-security culture in which security is seen across the council as an enabler of Sefton's wider strategic goals. This will involve collaborating with all parts of the council to identify processes, ways of working, and security solutions which support, and are balanced with, the council's wider strategic direction and business needs.

5.2.4 The next steps for the council largely focus on further tailoring its training for staff, strengthening its business continuity exercising regime, and refining its approach to managing cyber risk to balance strong controls with achieving its business objectives

5.3 Each of the recommendations within the Cyber 360 report is now being reviewed and linked to either the ongoing Security Improvement Plan or to wider corporate pieces of work. For example, the mandatory training around Information Governance for all staff is currently being reviewed and updated to include specific training around cyber risks and a new phishing exercise and associated training tool has since been released. In addition, the Audit team has worked closely with Senior Managers to complete dedicated training and exercises around Business Continuity Planning.

6.0 Conclusion

As stated at the outset of this report the risk in terms of Cyber is significant for every Council and Sefton is no exception. The external audits and reviews completed this financial year are positive and serve to endorse the work of the security team and recognise the improvements made to protect the authority, but also highlight additional best practice that the team have either actioned or will seek to work in partnership with the wider business to put in place, in line with the ongoing service improvement plan.