Report to:	**AUDIT COMMITTEE**
Relevant Officer:	Tony Doyle, Head of ICT Services
Date of Meeting	17 January 2019

COUNCIL SAFEGUARDS AGAINST CYBER RISKS

1.0 Purpose of the report:

1.1 To provide Audit Committee with an annual update in relation to the actions the Council is taking to reduce cyber risks. To update on the emerging threat landscape the Council faces in relation to cyber-attacks.

2.0 Recommendation(s):

2.1 To note the update on how the Council safeguards against cyber risks.

3.0 Reasons for recommendation(s):

3.1 The Audit Committee requested further information about the actions which the Council is taking to reduce the risk of a cyber-attack.

3.2a	Is the recommendation contrary to a plan or strategy adopted or approved by the Council?	No
3.2b	Is the recommendation in accordance with the Council's approved budget?	Yes

3.3 Other alternative options to be considered:

3.4 None.

4.0 Council Priority:

4.1 The report relates to all of the Councils priorities.

5.0 Background Information

5.1 **Recent threats**

The ICT Service and the Council's network partner The Networking People (TNP)

continue to spend an increasing proportion of time defending and protecting the Council's Network from Cyber-attack. During the last 12 months the ICT service have managed and contained a Distributed Denial of Service Attack (DDos Attack) on the Council's website with attack traffic coming from across the globe as well as mitigated daily thousands of malicious emails that attempt to infect or steal data from the Council's network. The service has seen increasing evidence of cleverly crafted and personally profiled spear phishing emails that even the most savvy end user would be tempted to click on. There is no doubt the cyber threat is growing and in spite of continuing investment and commitment of time and resources, the threats will continue to challenge the Council in the future.

Type of attack	**Number of attacks over a 12 month Period**
Malware blocked from websites visited and emails attachments	15,460
Ransomware blocked	2,256
Attacks blocked on Council websites	21,164,974

LGA Cyber Stocktake

In August 2018 the Council participated in a cyber-stocktake organised by the Local Government Association (LGA). The LGA cyber stocktake was devised in conjunction with Rand Europe and SOCITM. The Council received an overall rating of Green/Amber, which puts the Council in the upper quartile of the stocktake. 100% of all Local Authorities participated in the Stocktake.

The stocktake has also provided a focus for areas that can be improved which included the overall cyber awareness of employees and Elected Members and testing of employees' susceptibility to cyber-attack.

New ICT Security Policy, Mandatory Cyber Security Training and internal phishing test

In December 2018 an updated ICT Security policy was launched which coincided with the introduction of the new mandatory cyber skills training. A deadline has been set for all employees to complete the training by 31 January 2019. As of 4 January 2019, 781 employees have completed the training.

Also in December 2018, for the first time, the ICT service ran an internal phishing test to ascertain how susceptible employees were to clicking on phishing emails. The service is pleased to report that less than one percent of employees were fooled into

clicking on the email. However, there is no room for complacency here given the increasing levels of sophistication the email scammers are using.

Public Services Network (PSN) Code of Connection

After a significant amount of effort by the team through the Summer and Autumn of 2018, in December 2018 the Council received a new PSN Compliance certificate after an assessment of its security infrastructure by an external PSN assessor. This provides assurance that the Council's infrastructure is sufficiently secure to interconnect with other Government networks and public sector infrastructures. The Council understands since the Wannacry cyber-attack on the NHS, PSN assessments have become more stringent and a significant number of local authorities including some of the bigger authorities are struggling to achieve compliance.

GDPR (General Data Protection Regulations)

In May 2018 the new General Data Protection Regulations came into force. The regulation requires the Council to have appropriate technical and organisation measures in place as a security principle. Consequently, the Council's ICT service has developed some new security processes to further safeguard data, these have included increasing password length and complexity as well carrying out a security infrastructure due diligence process for all new software systems as part of Data Privacy Impact Assessment (DPIA). This has become particularly important for data being hosted outside of the Council network in third party clouds. It has become apparent that some suppliers in the software marketplace struggle to meet equivalent requirements to the Council's PSN compliance.

Threat Intelligence

The ICT Service continues to attend the North West WARP(Warning Advice and Reporting Point) and Society of Information Technology Management (SOCITM) in which intelligence about cyber threats is regularly shared within the Local Government Community and where external experts such as from the National Cyber Security Centre (NCSC) part of GCHQ share their expertise. In addition, the ICT Service subscribes to a number electronic intelligence sharing services, which quickly advise on new security vulnerabilities and attacks.

National Cyber Security Centre (NCSC) Active Cyber Defence Protective Services

NCSC have also introduced some protective services and standards which the Council has subscribed to. These include a protective Domain Name System (DNS) Service, a web checker service for quickly identifying vulnerabilities on Council websites and a Mail Check standard for reducing the risk of fraudulent emails.

Future Threats

Email Scams increasing in sophistication

The ICT service are having some success in reducing the volume of spam emails targeting the Council. However, the emerging trend is the increasing level of sophistication of personally targeted Cyber Scams. The Council can no longer assume that every phishing email will be easy to spot by an employee. The number of targeted attacks is increasing in which employees social media profiles and job roles have been carefully studied and this information alongside the use of professional branding and logos is being used as part of a scam.

The adoption of Cloud based systems

The ICT service are increasingly seeing software suppliers encouraging Council services to move their software systems to Cloud based hosted systems. The more distributed the Council data becomes the more challenging it is to holistically manage the security. The recently implemented Data Privacy Impact Assessment (DPIA) process which incorporates a security due diligence process is helping to minimize and manage these risks. It is essential that Council data is only hosted in a third party cloud when we are satisfied the risks have been assessed and understood and a formal legal contract has been put in place to ensure there is adequate data protection.

The digital transformation of cyber crime

Whilst the Council continues to progress with its own digital transformation many of the new technologies we seek to exploit, are also being cleverly exploited by cyber criminals. Attacks using machine learning, agile development, automation and encryption are widely being used by Cyber criminals to transform their own levels of sophistication. It is essential that we continue to invest and develop the Council's cyber defense capabilities to provide adequate assurance in this area.

5.2 Does the information submitted include any exempt information? No

6.0 Legal considerations:

6.1 A cyber-attack could result in a Data Protection breach which could result in a significant fine for the Council. From May 2018 the new General Data Protection Regulation (GDPR)comes in the force with fines up to 4% of turnover or 20 million euros

7.0 Human Resources considerations:

7.1 The completion of the ICT Security and Data Protection i-pool courses are mandatory for all Council employees.

8.0 Equalities considerations:

8.1 None.

9.0 Financial considerations:

9.1 The implementation of effective controls to reduce the risk of a cyber-attack need to be managed within the constraints of the available budget.

10.0 Risk management considerations:

10.1 Dealing with cyber risks is a key priority of the Council and is identified as one of the strategic risks which need to be managed.

11.0 Ethical considerations:

11.1 None.

12.0 Internal/ External Consultation undertaken:

12.1 None.

13.0 Background papers:

13.1 None.