Report to:	**AUDIT COMMITTEE**
Relevant Officer:	Tony Doyle, Head of ICT Services
Date of Meeting	2 March 2017

SAFEGUARDING AGAINST CYBER RISKS

1.0 Purpose of the report:

1.1 To provide an update in relation to the actions being taken to reduce cyber risks.

2.0 Recommendation(s):

2.1 To consider the contents of the report and make any recommendations as appropriate.

3.0 Reasons for recommendation(s):

3.1 At its 20 October 2016 meeting, 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:

N/a

4.0 Council Priority:

4.1 The relevant Council Priorities are:

- "The economy: Maximising growth and opportunity across Blackpool"
- "Communities: Creating stronger communities and increasing resilience"

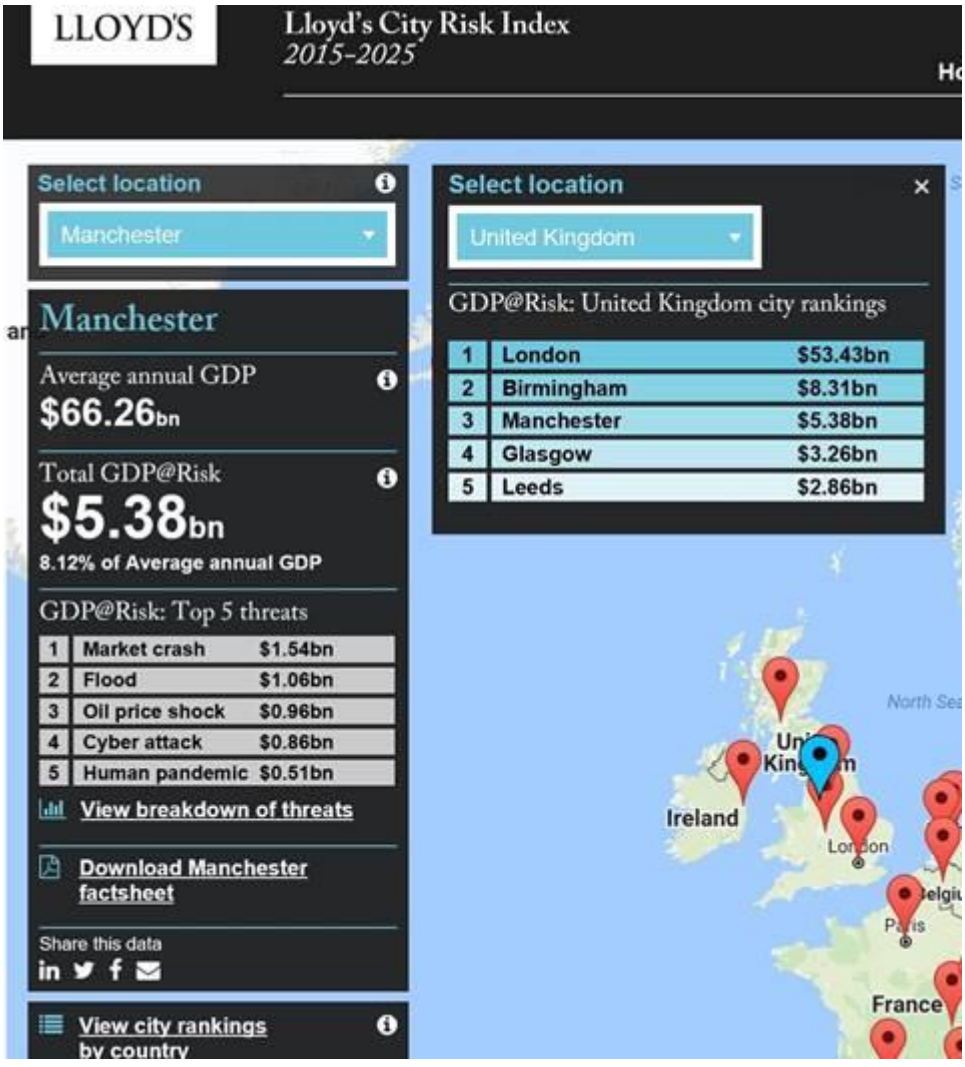
5.0 Background Information

5.1 **What is the cyber risk to the Council?**

5.1.1 The Council has never been more connected than it is right now. Its dependencies on digital infrastructures are greater than ever before. Digital services are now

crucial to the Council and our residents in most things it does. In many respects, digital has become the way of life. The Council would not function and be able to deliver its services without digital. Its ability to adapt and meet its future challenges largely depends on effective use of digital technologies. The Council therefore must protect our digital systems like never before. Cyber-attack is now a critical threat to national security it is a very real threat to Blackpool including the Council, its residents and its businesses. It is inevitable that this risk will continue to grow even further in the future as digital systems continue to grow.

5.1.2 Below is an extract from the Lloyds of London's City Risk Index. Cyber-attack is now one of the top five threats to the Gross Domestic Product (GDP) of all the UK's major cities. It is fourth largest threat to the GDP of the Council's nearest major city Manchester.



5.1.3 In another report Lloyds describe Cyber as the most complex and critical business risk businesses face today: It is a matter of 'when' not 'if' a business becomes a victim of a cyber-incident.

5.2 **How do we protect the Council?**

5.2.2 It is for this very reason in recent years we have added cyber risk insurance to the Council's insurance policy. However having cyber risk insurance by no means creates complacency and we have in recent years matched our investment in digital systems with investment in cyber security systems and expertise to avert and minimise risks.

5.2.3 The following bullet list provides a high level description of many of the measures being taken to reduce the risks to the Council's infrastructure and systems. It is does not cover every single measure and activity being taken, since risk reduction in this area is implicit in the everyday business activities of the Council and we are constantly changing and adapting to the latest known threats.

5.2.4
- Purchasing leading network and security systems from world class vendors such Fortinet(www.fortinet.com), Cisco (www.cisco.com)Intel Security (www.McAfee.com)

5.2.5
- A partnership with Lancaster University based TNP (The Networking People) (www.tnp.net.uk/services/security) who support the Council in configuring and managing network and security systems. TNP have the coveted International Standard for Information Security Management ISO27001, the UK Government Cyber Essentials Accreditation, Platinum partnership with Fortinet, Premier partnership with Cisco meaning they are highly trusted by these world class companies to integrate their security systems into network infrastructures. In particular all staff at TNP have comprehensive Network Security Expert qualifications with Fortinet. The leading member of the TNP team holds the Fortinet Network Security Expert Qualification at Level 8 (the highest level) and we understand he is currently the only person in Europe to have obtained this level of qualification with Fortinet.

5.2.6
- Regular Ethical Hacking/Penetration Tests by highly qualified external experts NTA Monitor (www.NTA-monitor.com), who are accredited under the CHECK system by the Communications-Electronics Security Group (CESG) part of Government Communications Headquarters (GCHQ) to detect and report on vulnerabilities.

5.2.7
- Compliance with the Cabinet Office's Public Services Network Code of Connection a security assessment and standard which includes an externally assessed Annual IT Health Check to confirm the Local Authority can be trusted to share and handle information securely with other public bodies.

5.2.8
- Compliance with the Payment Card Industry Data Security Standard to ensure the Council is trusted to process its large number of credit and debit card transactions.

5.2.9
- Compliance with the NHS N3 Information Governance Toolkit to ensure the Local Authority can be trusted to share and handle information securely with other NHS bodies.

5.2.10 • All the Council's ICT Staff to meet a minimum of the Government Baseline Personnel Security Standard (BPSS).

5.2.11 • Regularly patching of software and firmware for known vulnerabilities.

5.2.12 • Keeping comprehensive Data Backups.

5.2.13 • A contract for secure disposal of IT equipment with an ISO27001 accredited recycler.

5.2.14 • Regular attendance and intelligence sharing at the North West Warning, Advice and Reporting Point (WARP). http://i-network.org.uk/services/warp/

5.2.15 • Acting on information from numerous Intelligence bulletins such as from the National Cyber Security Centre -Cyber-security Information Sharing Partnership.

5.2.16 • Requiring all employees to complete the Ipool ICT Security and Data Protection Training.

5.2.17 • Regular awareness raising for employees about known threats via emails, the Hub, electronic, screens and attendance at meetings.

5.2.18 • Attendance at key cyber security events in Manchester and London.

5.3 **The top three known cyber threats to the Council and our user community**

5.3.1 **Email** - It is a well-known fact amongst ICT Security experts that email is our greatest threat and vulnerability. It is the entrance through which most cyber-attacks gain a foothold. The Council receives approximately 1/2 million emails on a typical day. 485,000 of these emails are filtered out with approximately only 15,000 being legitimate emails.

5.3.2 In recent years this growth in unwanted email has gone exponential and a larger and larger percentage of these unwanted emails are phishing attacks, nefarious in nature and socially engineered to manipulate the receiver into clicking on a link, to either steal some sensitive information such as a password, or to download a payload to infect a network with ransomware.

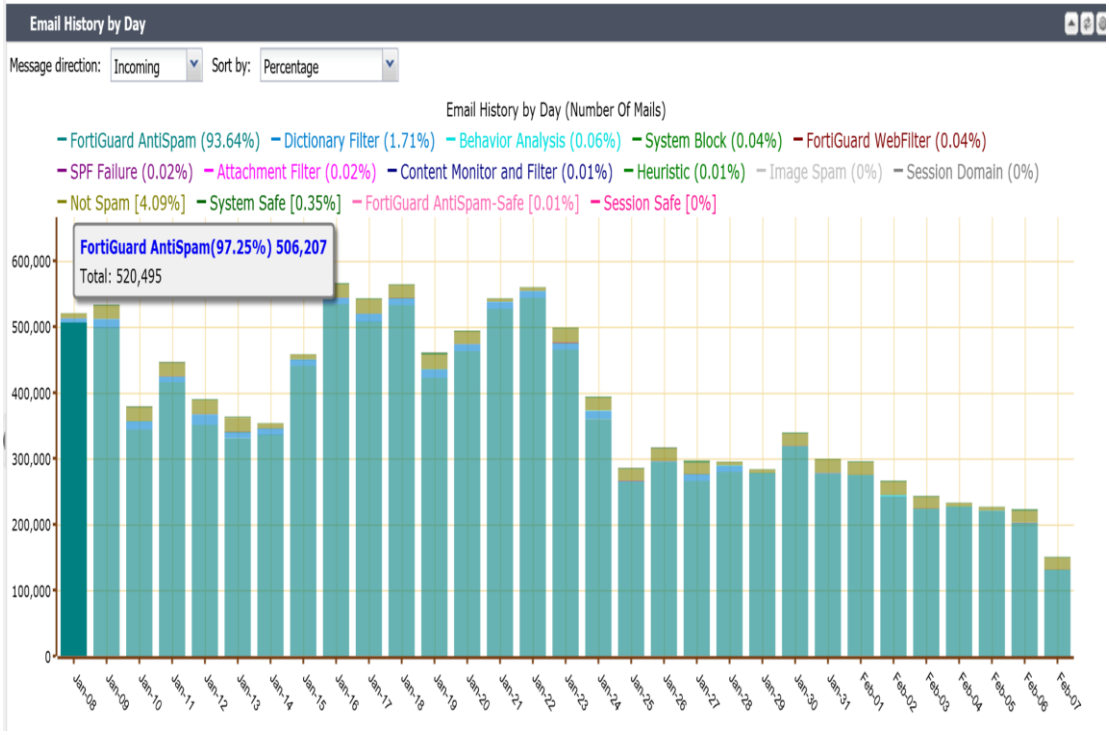
5.3.3 These emails may at first appear to contain legitimate attachments or website links but the consequences of being fooled can be catastrophic for the individual and the organisation.

5.3.4 Most of the time our security systems can detect these emails and filter them out but along with the growth in phishing emails there has been a growth in zero day attacks and levels of sophistication. Zero day attacks are emails that the security vendors have not yet detected and consequently they can sometimes bypass the

security filters. Whilst we have other methods for detecting these it is inevitable a small number will circumnavigate the filters.

5.3.5 The best form of defence in this situation is for all users of email to be naturally suspicious and cautious when opening emails even from known sources whose email accounts may have been compromised.

5.3.6 The following graph shows the number of emails being blocked each day in January and the early part of February. You will see from this it is not unusual for 97% of emails to be blocked by the filter.



5.3.7 **Ransomware** - As mentioned above some of the zero day threat emails are designed to encourage email users to download a ransomware payload. Ransomware is designed to encrypt the files on the device and the network it sits on. In order to regain access to the files the ransomware demands the victim to pay a ransom. The longer the victim leaves it to pay the ransom the higher the ransom goes. The only way to recover from a ransomware attack without paying a ransom is to ensure you have a secure backup of the data before it is encrypted.

5.3.8 Last year Lincolnshire County Council had to shut down all of its computer systems for four days to recover from a ransomware attack.

5.3.9 More recently, Tiverton Town Council in Devon has fallen victim to a ransomware attack with many sensitive files encrypted and a ransom demand for £3,000. It is reported an email user "slipped up" whilst in an early morning rush opened an email disguised as a parcel delivery reminder.

5.3.10 **Password Security** - Just before Christmas it was reported that the Internet giant Yahoo was hacked with over one billion customer account details including passwords being stolen. Hackers know people struggle to remember passwords so tend to use the same password or combinations of the same password for more than one account. It is widely known the Yahoo hacked passwords are for sale on the Dark web (the Internet black market). This potentially makes many people's accounts vulnerable.

5.3.11 In the Council, we regularly require users to reset complex passwords every 90 days and for external access from the Internet we require some form of two factor authentication. This mitigates the risk to some degree. However, it is always possible we have users who may have broken the ICT Security Policy and stored some Council data outside of the Council's security systems such as in a Dropbox account or Google Drive. Potentially such data could become vulnerable if a user's password was compromised in the Yahoo attack and same password is being used for other accounts.

5.4 **ICT Staff Turnover and Cyber Skills**

5.4.1 On 20 October 2016, the Audit Committee asked about the turnover of ICT Staff and whether the suitable people were in place. During the last 12 months, there has been a turnover of six employees who succeeded in gaining higher salaries with other employers in the North West.

5.4.2 The IT and Digital industries continue to grow at unprecedented rates and it is not unusual for good quality employees to move on quickly and gain promotion. In the current austere environment, it is a challenge for the public sector to retain skilled and talented IT staff due to the current pay restraints. In particular, employees with cyber skills are in very high demand.

5.4.3 The main way we have mitigated against this risk is through the partnership we have with TNP. TNP are based at the Lancaster University InfoLab and often recruit from within the University. Lancaster University is one of the few Universities in the UK that have the Government sponsored Academic Centre Of Excellence in Cyber Security Research Status. TNP who specialise in networking and security are in many ways better placed than the Council to attract talented cyber security and network specialists.

5.4.4 Alongside TNP the Council does have a number of in-house experienced members of IT team who understand the requirements to build and maintain compliant and secure IT systems. A combination of the in-house team, the partnership with TNP and security testing with NTA monitor(who provided ethical hacking services), means we are as well positioned as other Councils to meet the cyber security challenge. However, the challenge of cyber security is stretching the resources of even the world’s largest organisations with no organisation in this day and age able to claim it is immune to the cyber threat and totally secure.

5.5 Does the information submitted include any exempt information? No

5.6 **List of Appendices:**
None.

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 2% of turnover or 10,000 Euros.

7.0 Human Resources considerations:

7.1 The completion of the ICT Security and Data Protection ipool 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.