Report to:	**Audit Committee**
Relevant Officer:	Tony Doyle, Head of ICT Services
Date of Meeting	15 March 2018

CYBER SECURITY UPDATE

1.0 Purpose of the report:

1.1 To provide an update on cyber threats and actions 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. An update was provided to Audit Committee on 2nd March 2017, this paper provides a further update as the threats, and risks continue to evolve.

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 **Recent Threats**

5.1.1 Over the past 12 months Cyber Security Risks have remained high on the agenda and have continued to increase in sophistication across the world. In May 2017 unprecedented disruption was caused nationally to the NHS and Fylde Coast NHS Trusts after a Ransomware attack called WannaCry spread rapidly through NHS networks and infected huge numbers of PCs and systems across the NHS. For many public sector organisations this was a wakeup call for the level of risk we all now face in our daily lives from Cyber Attack. The attack was attributed to North Korea by the UK's National Cyber Security Centre (NCSC, part of GCHQ).

5.1.2 New, more sophisticated, attack methods continue to be developed and a worrying new trend is the use of compromised Internet connected devices. These are often domestic devices such as home routers and CCTV cameras which are used in unison to attack other networks. Many of the devices now connected in people's homes have weak security out of the box. End users often fail or lack the knowledge to make basic changes to default passwords or perform software security updates which makes it easy for hackers to take control of a device. When many of these devices are compromised and controlled by hackers they can be weaponised to direct network traffic at larger networks and potentially cause huge disruption even to the biggest and best resourced Company networks.

5.1.3 In January 2018 two significant security vulnerabilities (Meltdown and Spectre) were discovered to be present in the microprocessors of nearly all computers. Consequently the Council's ICT Service has had to spend a significant amount of time, updating software operating systems and firmware to protect the Council's ICT estate from these new risks. There were concerns that the security updates could have a significant performance impact but we are pleased to report that so far no noticeable impact in performance has been detected or reported.

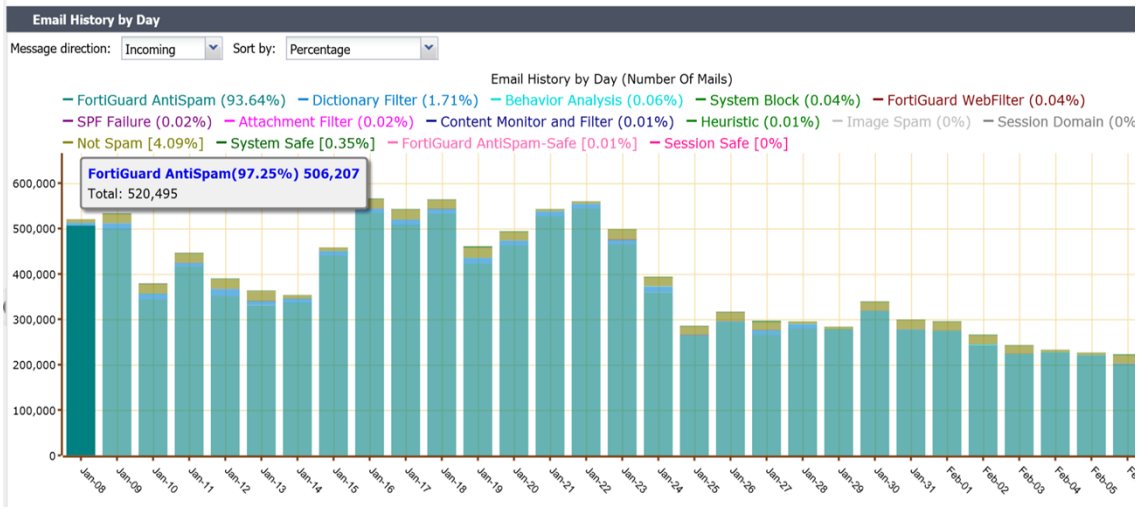
5.1.4 In February 2018 another high profile cyber security incident was widely reported in which many public sector websites were compromised as a consequence of using a popular accessibility tool by the name of Browsealoud. The Browsealoud code which is served to thousands of websites from a central source was infected with Bitcoin mining software. This meant any visitor to a website using the Browsealoud software was having their computer's processor hijacked to carry out the task of mining Bitcoins. Bitcoin Mining is a way of producing new Bitcoins by computer processors solving complex algorithms. As Bitcoins have become more popular and their value has increased, the algorithms that require solving to generate new Bitcoins, have become more complex. Now huge amounts of processing power and electricity is required to generate a new Bitcoin. This has therefore led to hackers developing more sophisticated ways to steal processing power from other computers to seek monetary reward from generating new Bitcoins. None of the Council's main websites were impacted by this, although a jointly commissioned website with the NHS

FYIDirectory used the Browsealoud software and may have been impacted for a short period. The vulnerability was quickly discovered by Browsealoud and NCSC and the service was taken down temporarily while the vulnerability was removed. No data would have been compromised but users of the Browsealoud service may have temporarily found their devices would have run slow during this short period.

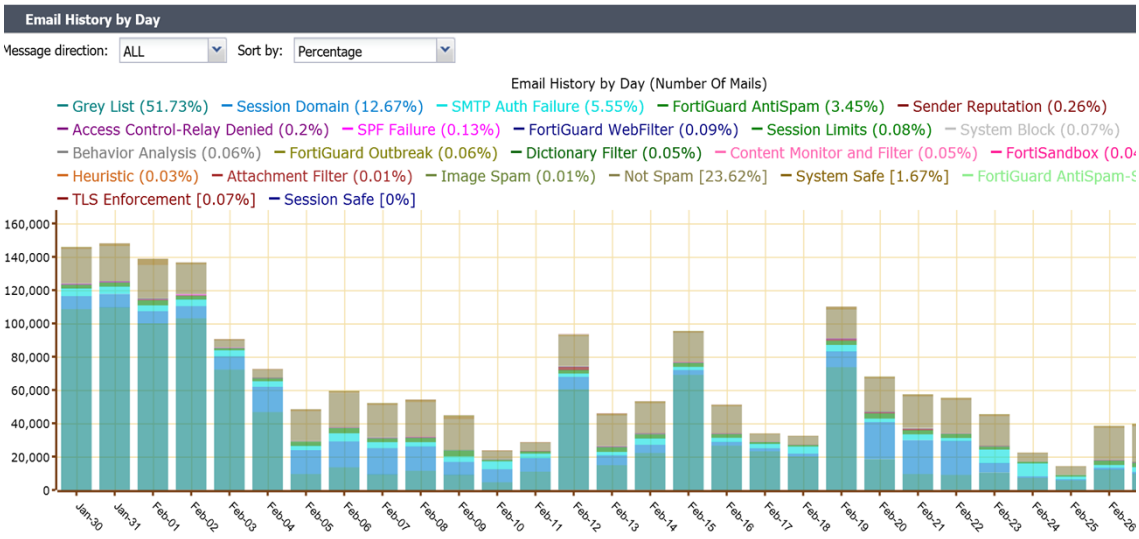
5.2 Continued Threat from Email

5.2.1 By far the largest threat the Council continues to face is from sophisticated email attacks. Consequently, we continue to invest in and optimise our email filtering technologies. We are pleased to report that since updating Audit Committee last year we have seen a reduction in SPAM emails in spite of the Global trend which continues to see increases in the volume of SPAM emails being sent.

5.2.2 Below is a graph which illustrates the volumes reported this time last year(2017) which demonstrates it was not unusual to see over 1/2 million emails a day, 97% of which was SPAM/Malicious email, was being sent to the Council each day.



5.2.3 The following graph shows the volumes reported at the start of 2018 and illustrates a significant drop in the amount of SPAM/Malicious emails being aimed at the Council. Typically now less than 100,000 emails a day approximately 60% of which are SPAM/Malicious emails. We attribute this reduction to a number of new counter measures within the technology we are using, as well as global law enforcement efforts to shutdown Botnets responsible for creating large volumes of SPAM and Malicious emails.



5.2.4 However we cannot afford to be complacent. Although the volume has reduced, the level of sophistication to evade detection continues to evolve and consequently the need to increase the awareness and cyber intelligence of the Council's employees and Elected Members continues to be a major priority.

5.3 Awareness and Cyber Skills Training

5.3.1 At Audit Committee last year Members asked if training could be provided for Elected Members. Two training sessions were arranged for Elected Members. One was arranged for Audit Committee Members in January but was unfortunately postponed at the last minute due to unforeseen circumstances and rearranged for this evening. Another session for non-Audit Committee Elected Members was arranged in early February and this was attended by 7 Elected Members.

5.3.2 The training currently being provided has recently been developed in conjunction with 8 other Local Authorities by production company Matobo, who have also developed the BBC Employee Cyber Awareness Training. The training seeks to educate and raise awareness of the most likely cyber threats employees and Members will encounter. It seeks to minimise the risk of the Employee being inadvertently tricked in to taking an action that could put the individual or the wider organisation at risk.

5.3.3 This new refresher training will be rolled out to all employees from April 2018 as part of a mandatory Ipool module.

5.4 GDPR and Cyber Security

5.4.1 The new General Data Protection Regulation (GDPR) comes in to force in May 2018 and puts requirements on the Council to have technical and organisational security

measures in place. There is a significant overlap between cyber security and data protection. If any cyber incident led to a loss of personal data the Council would be at significant risks from fines and will be under an obligation to report this quickly to the ICO. However whilst we need all employees to be handling data with extreme care in a compliant way we need to also support employees on how to safely share data especially with external organisations such as the NHS. One of the new risks is that Employees living in fear of a fine from the new GDPR regulation may start to fear sharing important data which is necessary to reduce risks to vulnerable Children or Adults.

Does the information submitted include any exempt information? No

5.5 **List of Appendices:**

5.5.1 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 4% of turnover or 20 Million 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