MEETING:	**AUDIT AND GOVERNANCE COMMITTEE**
DATE:	**15 JULY 2021**
TITLE:	**RESILIENCE OF IT SYSTEMS - CYBER SECURITY**
PURPOSE:	**To update the Committee about Gwynedd Council's cyber security resilience, and to give members an opportunity to scrutinise the situation. There has been coverage of cyber-attacks in the news recently, and with an increase in our dependency on and use of technology, it is timely to report on what is happening locally in the Council.**
AUTHOR:	**HUW YNYR, ASSISTANT HEAD OF FINANCE - INFORMATION TECHNOLOGY**
CABINET MEMBER:	**COUNCILLOR IOAN THOMAS**

1. Summary

1.1 The Council has a duty to provide a wide range of services, many of them using technological resources. It is essential that we ensure that this environment is secured from threats that could undermine the Council's ability to provide services and endanger the data the Council looks after.

1.2 This report is for information only, outlining the cyber security provision for a lay-person, which has been prepared by the Information Technology Service. Please note that provision is in place to mitigate the risk of a cyber-attack, but that it is not possible to guarantee 100% that an attack cannot breach our defences. This statement is true of all organisations; however, further measures are in place to restore our systems should an attack breach our defences.

1.3 Though the media seem to place an emphasis on cyber security, in reality, the emphasis should be on cyber resilience, which includes elements of security by building defences, but also includes the ability to recover from a fragile situation should those defences fail.

2. Background

2.1 We are aware that Cyber activists look for weaknesses in public bodies' defences. Therefore, it would be inappropriate to take a stance that the Council is not a likely target for those who carry out cyber-attacks, however a comparatively small public body without effective defences could be an easier target for cyber terrorism.

2.2 As this is a live and current environment, attacks evolve all the time and it is quite a challenge to keep environment current to sustain resilient services. The standard of the security measures depends on a wide range of factors, i.e. technological, physical and administrative measures, and every individual within the Council and its partners has a crucial role to play to avoid undermining these.

2.3 The Council draws on various sources to develop and maintain a resilient environment, including:

- Good practice and standards in the field which are published by the UK Government's advisory body on cyber items, the NCSC (*National Cyber Security Centre*);
- Membership of bodies which warn about incidents and weaknesses to enable us to respond promptly;
- Investing in specific technology and services to identify and prevent changes to our environment which have the potential to be harmful, monitoring the network for suspicious activities and identifying software that need updating;
- Investing in resilient technology;
- Using third party services to evaluate our provision;
- Ensuring information technology security policies are current and complying with them;
- Undertaking exercises to educate and raise our users' awareness of dangers and good practice and policies which should be followed.

3. Risks and mitigating measures

3.1 In relation to information technology, the loss of data or loss of access to data is the risk with the highest impact for the Council as this could affect the Council's ability to provide services to the public. It is essential that the Council takes steps to prevent, and is able to respond effectively, to these risks. See below examples of the risks facing the Council.

3.2 **Public-facing resources**: Providing services to individuals, groups and organisations in a variety of locations, means that some systems' interfaces are public-facing, which presents an opening for individuals or organisations with hostile intentions.

Gwynedd Arrangements: The Council's code development processes and procedures follow specific standards to protect us from interventions with hostile intentions, with a system is in place to monitor and assess for weaknesses which is an effective way of ensuring that these processes are followed without exception.

3.3 **Denial of Services**: A *Denial of Service* attack could be realised by arranging an overload of traffic to be sent to those public-facing digital services and this overload could be more than our systems could cope with. Often, attackers would use a series of computers under their control to carry out such an attack and it would be essential for infrastructure perimeter defences to identify such attacks, preventing the traffic from becoming harmful.

Gwynedd Arrangements: There are systems in place which continuously search for this type of activity on the various tiers of perimeters of the Council's network. These are designed to identify activities which could affect services and preventing them from achieving this.

3.4 **Malicious Material**: Malicious material can come in many different forms, and their effects vary from mild inconvenience to an organisation's inability to operate. A well-known example of this type of software is ransomware software. Software would be installed on a computer by cyber terrorists with the intention of causing malice by encrypting the computer's data so that it is not possible to read or use it; the malicious software would spread to associated computers and store areas, encrypting every piece of data along the way. The motive of such an attack is for the criminal to demand a ransomware payment to decrypt the data. The ransomware payment would usually be required in crypto currency, such as bitcoin, enabling the criminals to remain anonymous.

There are several steps to be taken to mitigate the risks involved with this, ranging from preventing the software from reaching devices in the first instance, impacting their ability to operate, and ensuring that effective recovery measures are in place should files be damaged.

Gwynedd Arrangements: The Council has processes and systems to identify and disable malicious material, including traffic and e-mail filtering software, anti-virus and anti-malware software and good practice procedures such as controlling the number of enhanced access accounts. There is a strong emphasis on recovery should a successful attack happen and arrangements are in place to ensure that there are backups available, including several versions of files should losses need to be recovered to a specific date. We will also carry out continuous exercises to inform and remind colleagues of the risks in relation to such material.

3.5 **Vulnerable Systems**: Identifying and highlighting weaknesses in items of software is a major industry, and it is essential that software suppliers create and provide timely patches before individuals or organisations that have hostile intentions can take advantage of those weaknesses for their own benefit. It is essential that every item of software has a support contract with the providers to prepare and receive patches in response to security incidents, and after their release it is essential that the Council installs the repairs in a timely manner.

Gwynedd Arrangements: The Council has systems in place to identify software that need to be updated and processes in place to download and install those updates and additional processes set up to undertake assessments about the status and versions of our software to ensure there are no failures.

3.6 **Phishing**: Phishing is a term used to describe the hostile activity of sending a message (e.g. e-mail) to someone hoping that the recipient would take action in a way which would be beneficial to the sender. There is a need to be vigilant of this risk when receiving messages, always considering whether there are any suspicious aspects to them. Unfortunately, there is a considerable increase in this type of attack, and the number falling for the scams.

Gwynedd Arrangements: The Council has an e-mail filtering system in place which assesses the suitability of a message's content together with a risk assessment of the sending address. In addition to this, there are periodical arrangements in place to notify and remind colleagues about risks and to enable them to respond in a suitable way should they receive such a message. A specific exercise has been arranged this year for the third quarter of 2021/22 to see how alert the Council's workforce is to phishing messages.

3.7 **Failure of Service/Business Continuity**: The demand for and dependency on technology has increased substantially in recent years. Furthermore, the Covid-19 crisis has confirmed this, and our users' expectations of the service provided to them have increased. The service is expected to be available at all times; therefore, maintenance work is planned outside core working hours in order to minimise the disturbance to services. In order to maintain an environment which meets the expectations of Council officers and our service users, it is essential that the provision is resilient. This means planning ways to deliver services in circumstances where systems are compromised or not available at all. In relation to information technology, this means ensuring that systems, support resources and back-up provision are in place.

Gwynedd Arrangements: A project is ongoing in order to extend the availability of the Council's key systems. Virtual Servers are provisioned from two data centres ensuring service continuity should one of these centres fail.

3.8 **Failure to Respond to Incidents**: The most effective way of testing the effectiveness of mitigating measures is by holding exercises to re-create potentially harmful circumstances, whilst assessing the success of the exercise to prevent or minimise the impact. The circumstances of an incident can vary greatly; therefore, it is essential that we plan in detail as well as review and develop our response measures.

Gwynedd Arrangements: This is a crucial part of incorporating some of the steps described in this document, and it is a continuous process. The Council is working with other agencies to establish emergency plans and practises to incident responses as part of its emergency planning duties.

4. Accreditations

4.1 **Public Services Network ("PSN")**: The purpose of the PSN is to operate as a segregated network independent from our corporate network and shared with a number of national public services across the UK.

4.2 The Council needs to connect to this network in order to provide some essential services, specifically in relation to benefits and support for adults. One of the PSN's main principles is the need to trust all organisations which have connected to the PSN network, and to that end, there is a need to satisfy specific security standards. Connection is prohibited without current accreditation.

4.3 An application to connect to the PSN network is made to the Cabinet Office (UK Government), in their role as guardian of the network, with specific evidence presented including a security assessment by a certified third party company and a mitigation plan for any high risk items discovered.

4.4 The Council secured its current accreditation in May, 2021. This accreditation provides independent assurance of the security measures and levesl established by the Council.

5. PSBA (Public Sector Broadband Aggregation)

5.1 The PSBA is an all-Wales initiative to introduce a wide area network designed for and by public sector services. Gwynedd Council was one of the first users of the PSBA, and we continue to contribute to the strategic and technical direction of the network.

5.2 The PSBA enables local health boards, local authorities, higher and further education institutions, blue light emergency services and other public bodies to provide effective services for the population, by using innovative, cost-effective, reliable network services which direction provided from cross-sector boards which also includes representation from Gwynedd Council.

5.3 Security is integral to this service, offering additional defences to what is on the perimeter and within the Council's network, and acts as a foundation which supports the rest of our infrastructure.

6. Apprentice

6.1 The Information Technology Service has appointed a Cyber Security Apprentice, through a Council-run apprenticeship scheme. The apprentice, who will be released to follow a B.Sc. degree course in Cyber Security at University, will be welcomed to the extended team in August, 2021.

7. Incident statistics

7.1 The Council has not suffered losses stemming from cyber security incidents within the last five years. Safeguarding and monitoring systems are in place on the Council network perimeter, and within the network, which draw attention to hostile items or activities. Such incidents are regular, with suspicious e-mail messages, covert scans for technical information and attempts to attack our resources being routine daily activities, rather than out of the ordinary.

8. Conclusion

8.1 These hostile activities will increase and despite our attempts to protect our infrastructure and systems from cyber terrorists, it is not possible to give a 100% guarantee that all attempts can be prevented. We have already noted that our efforts for a resilient service are a mix of cyber defences and our ability to recover from a situation should an attack breach the defences. This is reflected on the corporate risk register, with a fairly low likelihood (2) and very high impact (5) risk noted.