ISLE OF ANGLESEY COUNTY COUNCIL	
Report to:	Audit and Governance Committee
Date:	3rd December 2019
Subject:	Cyber Security Annual Report 2019
Head of Service	Carys Edwards, Head of Profession HR and Transformation (01248) 752502 CarysEdwards@ynysmon.gov.uk
Report Author:	Lee Evans, IT Service and Performance Management Manager (01248) 752526 LeeEvans@ynysmon.gov.uk
Nature and Reason for Reporting: The report allows the Committee to monitor the Council's arrangements in mitigating Cyber Threats as well providing details of other monitoring and assurance activities relating to this area.	

1. Introduction

This report provides information relating to the Cyber Threats facing the Council and how the IT Division is taking action to mitigate them.

2. Recommendation

To note the assurance provided in the report.

CYNGOR SIR
YNYS MÔN
ISLE OF ANGLESEY
COUNTY COUNCIL

Adain TG
IT Division

Cyber Security

Annual Report 2019

OFFICIAL

Desg Gymorth TG / IT Service Desk
Cyngor Sir Ynys Môn / Isle of Anglesey County Council
(01248) 752525
DesgGymorthTG@ynysmon.gov.uk ITServiceDesk@anglesey.gov.uk
http://monitor.ynysmon.gov.uk/tgch http://monitor.anglesey.gov.uk/ict

SHORTLISTED SCDI IT SERVICE & SUPPORT AWARDS Best Small Service Desk 2017

OUTSTANDING ACHIEVEMENT SCDI IT SERVICE & SUPPORT AWARDS Most Improved Service Desk 2017

CYBER ESSENTIALS PLUS

Cyber Security Annual Report 2019

1. BACKGROUND

Reports of Cyber Attacks have become common place in the news with high profile attacks on a weekly and even daily basis, the most well-known example being the WannaCry ransomware attack on the NHS. At best, such attacks erode the trust of services and customers and cause reputational damage, at worse they can cripple an organisation and prevent the provision of essential services.

Cyber attacks vary in their approach and complexity but are consistent in their intent to disrupt, damage or steal.

Cyber Security is the practice of defending computer systems from cyber threats and protecting the integrity, confidentiality and availability of the organisation's information.

Similar to any Internet connected organisation, the Council's network is under constant 24hr attack and the significant volume of sensitive personal data held by the Council means it is imperative that we reduce the risk of a successful cyber-attack as much as is reasonably possible. The risk of Cyber Attack is recognised by the Council and is recorded within the corporate Risk Register which is monitored by the Senior Leadership Team (SLT).

This report summaries the Cyber Threats facing the Council and some of the mitigations the Council has in place. One of the key principles of effective Cyber Security is "security by obscurity", therefore the report will only provide a high level overview and not detail the technologies or products used.

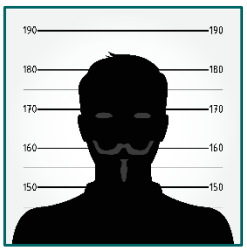
2. WHO ARE THE POTENTIAL ATTACKERS?

As with all organisations, the origins of attempted cyber-attacks vary in terms of method and motive and fall into the following broad categories;

Criminals

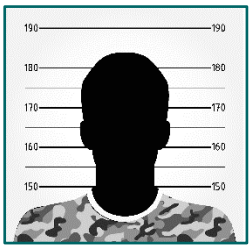
Motivated purely by financial gain. Cybercrime allows criminals to operate internationally and anonymously, offering a low risk method of stealing versus traditional crimes and potentially much higher returns. The low cost of set up means criminals can launch an attack on thousands of potential victims and only need a small number of successes to make large financial gain.

Hacktivists and Glory Seekers



Individuals or groups of attackers who carry out their malicious activity to promote their chosen agenda. Such an attack can include disruption to the availability of a system or “de-facing” corporate websites and social media with the attackers chosen message - this could be a political topic, religious belief or social ideology or can even be simply to demonstrate their technical ability to peers.

Foreign Nation States



Groups sponsored by nation states. Local Councils are the Gateway to central government and crucial public services. State-sponsored attackers have particular objectives aligned with either the political, commercial or military interests of their country of origin. These types of attack are extremely sophisticated and difficult to detect. The National Cyber Security Centre has published advisories stating that the risk of attack from these groups is real, particularly around major national events such as elections.

Insider Threats

The insider threat is a threat to an organization's security or data that comes from within. This type of threat comes from employees or former employees, but may also arise from third parties, including contractors, temporary workers, employees or customers. It is widely stated that 50% of the worst information security breaches are caused by inadvertent human error such as opening a malicious email.

3. WHAT ARE THE CYBER THREATS?

Malware

Malware, or “malicious software,” is an umbrella term that describes any malicious program or code that is harmful to systems.

Malware seeks to damage or disable computers, servers, networks and other computing devices.

Example of Malware include Viruses, Trojan Horses, Ransomware and Key Loggers;

1879

malware attacks

Viruses

The most well-known type of Malware, Viruses mostly seek to cause disruption to a system or destroy data. Virus spread from computer to computer via networks, email and removable media. A virus infection can take place by the victim running a malicious file or simply by plugging in a USB Stick.

Ransomware

Ransomware is a form of malware that encrypts a victim's files. Having prevented access to their data, the attacker then demands a ransom from the victim to restore access to the data upon payment.

The ransomware software shows the victim instructions on how to pay the ransom and often include a support number where “help” is given to complete the transaction. The disruption caused by ransomware can bring an organisation to a halt and the cost of the ransom can be as much as tens of thousands of pounds with little realistic chance of the perpetrators being brought to justice.

Key Loggers

A Key Logger is software which is installed on a victim’s PC without their knowledge will capture their keystrokes over a period of months or even years. Information captured by the Key Logger is relayed back to the attacker over the Internet where they will filter if for login details, passwords and credit card information which are then used to facilitate financial crime.

781

types of Malware

Trojan Horses

Posing as useful and non-malicious software so as to be innocently installed by a victim, a Trojan Horse will secretly download other Malware such as Ransomware or Key Loggers to a user’s PC without their knowledge and without any obvious signs which would raise suspicion.

Mitigation

Anti-Malware Software

All Council computers and servers operate anti-Malware software which scans for signatures of known malicious code and block access if found.

There are several potential sources of Malware attack and these include; email attachments, malicious websites and removable media;

Email Filtering

All email attachments received by the Council are subject to Malware analysis. Any known risky file types are either automatically blocked or sanitised so that any "active content" is removed.

The Council is also subscribed to an email blacklisting service ensuring that emails from known malicious sources are automatically blocked.

180,400
malicious emails blocked monthly

980
Malicious

Web Filtering

The Council is subscribed to the National Cyber Security Centre (NCSC) Protective Domain Name resolution Service.

In plain terms, this means that any web address accessed by a Council computer is checked against a list of known malicious sites and access blocked if necessary.

In addition, the Council uses a web filtering service which blocks access to undesirable websites such as Games, Gambling, Pornography and Illegal activity.

Removable Media

Removable media such as CD's and USB sticks have historically been convenient and cheap means of data transfer. However, they can also be used for Malware to spread from one network to another and can also easily be lost leading to a data breach. In response to this risk the Council has retired the use of USB Sticks on Council computers with the exception of a small number where there is an overriding business case.

Software Vulnerabilities

Software vulnerabilities are bugs or loopholes in software code which if exploited by an attacker can cause the software to behave in an un-expected and undesirable manner, for example allowing an attacker to remotely access the system without permission.

Where software is current and still supported by the supplier, corrected code packages known as “updates” or “patches” are made available to address the software bugs and close the potential security loophole. Depending on the software it may be manual process to update each device or it may be possible to manage the process centrally.

Mitigation

Early Windows 10 Adoption

In order to take advantage of the enhanced security features it provides, the Council took a strategic decision several years ago to upgrade every PC or Laptop to Windows 10. This project identified a raft of legacy software which was no longer updated by the supplier and was potentially a risk going forward. A decision was taken to remove the legacy software and reduce the overall estate of software which needed updating.

Application Virtualisation

Traditionally, application software was installed on each and every computer or laptop which was a significant burden to manage software security updates. With the rollout of Windows 10, a decision was taken to move away from this model to “application virtualisation”. In simple terms this means that for each application there is a master copy which runs on a central server. Each of the computers or laptops access this central copy of the software meaning there is only one copy to keep up to date and manage.

Vulnerability Testing

In line with Cabinet Office and industry requirements, the Council arranges for third party “ethical hackers” to carry out vulnerability assessments on the Council’s network. This process identifies any software which is out of date, is missing patches and poses a risk, the highlighted software is then either updated or retired.

Insider Threats

According to McAfee, 43% of Cyber incidents are caused by Insider Threats – these can be categorised as accidental staff actions, malicious staff actions or the actions of contractors.

Many of the threats discussed in this report have been technical in nature, however the success of those attacks usually rely on a human clicking a malicious link, opening a malicious attachment, revealing their password or some other action.

Mitigation

Cyber Security Training

In ensuring that staff are aware of the risks associated with Cyber Threats the Council played a leading role in the procurement of a bilingual, all-Wales E-Learning package on Cyber Awareness.

The Cyber Awareness module has been deployed on the Council's e-Learning platform and SLT have mandated that all IT connected staff must complete this module.

Baselines Personnel Security Standard (BPSS)

All staff who have access to OFFICIAL-SENSITIVE data which is derived from the cabinet office must go through the BPSS process which requires them to produce proof of ID, nationality and undergo a DBS check.

Data Processing Agreements

All contractors who either host Council IT systems or have remote access to Council IT systems are required to sign a Data Processing Agreement (DPA).

The DPA outlines the responsibilities of the contractor in terms of Cyber Security and also legally requires them to accept full financial liability for any breaches or damages which arise as a result of their failure to comply.

Policy Agreement

The Council has various policies in place for the safe use of IT, including an Acceptable Usage Policy and IT Security policy. The Acceptable Usage and IT Security Policy outline the responsibilities on staff in protecting the security of the Council's IT systems and it is mandatory that all IT connected staff review and accept these policies.

Phishing

This type of attack is used to obtain financial or other confidential information from a victim. This is typically achieved by sending an email that looks as if it is from a legitimate organisation such as a bank but contains a link to a fake website that replicates the real one. The victim's login details are captured by the fake website upon login and passed to the attacker.

Whereas a generic Phishing attack is mailed out to thousands of potential victims at a time, there is a variation of Phishing known as "Spear-Phishing". In a Spear-Phishing attack a specific organisation or even individual is targeted and therefore the email and fake website will be tailored to seem more familiar and credible to the victim. For example, the attacker may attempt to pose as the organisation's IT Helpdesk.

Mitigation

Email and Web Filtering

As previously noted, the Council has sophisticated filtering technology in place which aims to block Phishing emails and in addition, block the malicious websites that they attempt to divert victims to.

Cyber Security Training

Configuring Email and Web filtering systems is a balance between blocking suspected malicious content and ensuring that legitimate business activities are not blocked. With this in mind, it is inevitable that some Phishing emails will get through and it is imperative that all staff have an awareness of Cyber Threats.

As previously noted, all IT connected Council staff must complete a mandatory E-Learning module on Cyber Security Awareness. This module has specific sections on the dangers of malicious emails and in particular Phishing. Staff also review and record their acceptance of an IT Security Policy which notes the dangers posed by malicious emails.

4. WHAT ASSURANCES ARE IN PLACE?

This section of the report details some of the checks in place to ensure that the protective measures the Council has in place are adequate enough to reduce the risk of a successful Cyber Attack to a reasonable level.

Cabinet Office PSN Accreditation

The Public Sector Network (PSN) is a high-speed Government network used by public sector to exchange data in a secure manner. As the PSN effectively allows connection to Cabinet Office and Department for Work and Pensions systems, the Council must undergo a rigorous independent assessment on an annual basis. Failure to achieve the required Cyber Security standard results in disconnection and an inability to process benefits subsidies.

The Council has successfully passed the annual PSN assessment every year since it became a requirement.

Cyber Essentials+ and IASME Accreditation

Through a programme funded by Welsh Government and managed by the WLGA, local authorities have been testing their cyber security and information governance arrangements against the best practice.

After a rigorous audit process, the Council is one of only seven authorities in Wales to have achieved Cyber Essentials Plus and the full IASME Accreditation.

The accreditation included security testing of all IT systems and devices which was a akin to a cyber-attack, as well as a rigorous onsite audit which covered IT security and information governance policies and required significant contribution from colleagues in HR and Information Governance.

Internal Audit

As Cyber Threats are recorded on the Corporate Risk Register, the Council's arrangements in this area are subject to review by Internal Audit. During 2018/19 the Internal Audit team carried out a review to establish whether the Council has "adequate protection, detection and response arrangements in place to mitigate the risk to the Council's network, systems, information and services from a cybersecurity breach".

As a result of the review it was concluded that the Council has a number of effective, operational controls in place to manage the risk to cybersecurity and to prevent and reduce the impact to Council services, systems and information of malicious, external attacks.

5. WHAT ARE THE CHALLENGES GOING FORWARD

To date, the Council has been able to demonstrate and provide assurance that reasonable measures in place to manage Cyber Threats to an acceptable level, however as the volume and sophistication of these threats grows, so also does the burden in terms of;

- Researching emerging threats and developing protective measures
- Funding, operating and monitoring the ever-increasing number of threat protection technologies which are required.
- Liaising with security colleagues within WARP and NCSC to share intelligence.
- Resourcing the development of policy, awareness and compliance monitoring

These challenges are not unique to the Council and resourcing requirements will continue to monitored, supported by bids for additional funding when required.

6. RECOMMENDATION

It is recommended to note the assurance provided in the report.