Overview and Scrutiny Committee –

Bulletin Summary – IT Cyber Security

Overview: At Members request the following is a summary bulletin which explains in generic terms, the health of East Herts IT systems including an explanation of the questions posed below:

*1.	Why it's important especially in the public sector (eg prevention, detection and responding) and the consequences of Cyber attacks*

Public sector organizations are attractive targets for cyberattacks due to the sensitive data they hold. These attacks can disrupt essential services, expose citizen information, and damage public trust. Robust cybersecurity measures are crucial for prevention, detection, and response to cyberattacks.

*2.	Types of Cyber Threats (Malware, Ransomeware and Phishing*

Cyber threats are malicious attempts to gain unauthorised access to computer systems or networks. They can be carried out by individuals, groups, or even nation-states. Cyber threats can be used to steal data, disrupt operations, or even cause physical damage. There are many different types of cyber threats, but some of the most common include malware, ransomware, and phishing.

Malware is any software that is designed to harm a computer system. It can include viruses, worms, trojans, spyware, and ransomware. Malware can be spread through email attachments, malicious websites, or infected USB drives. Once malware is on a computer system, it can steal data, encrypt files, or damage the system. Ransomware is a type of malware that encrypts a victim's files and then demands a ransom payment in exchange for the decryption key. Ransomware attacks can be devastating for businesses and individuals, as they can lead to the loss of important data and financial losses.

Phishing is a type of social engineering attack that attempts to trick users into revealing sensitive information, such as passwords or credit card numbers. Phishing attacks are often carried out through email, but they can also be carried out through text messages or social media. Phishing attacks can be very convincing, and even experienced users can fall victim to them.

*3.	The critical components of Cyber Strategy. (eg Risk Assessment, Security Policies and procedures, Network and End Point Security, Access* *controls. Data Encryption, Incident Response Plan and Third Party Risk Management*

A successful cyber strategy comprises of several essential components, including:

- Governance: Establishing clear roles and responsibilities for cybersecurity and developing and implementing policies and procedures.
- Risk management: Identifying and assessing cybersecurity risks and developing and implementing plans to mitigate those risks.
- Security awareness and training: Ensuring that employees are aware of cybersecurity risks and know how to protect their systems and data.
- Technical controls: Implementing technical security controls, such as firewalls, intrusion detection systems, and encryption.
- Incident response: Having a plan in place for responding to and recovering from cyber incidents.

It is important to remember that a cyber strategy is not a one-size-fits-all solution. The specific components of a cyber strategy will vary depending on the size and complexity of the organization, as well as the industry in which it operates.

4. The Role of the Information, Governance and Protection Manager?

The Information, Governance and Protection Manager doesn't sit within the ICT shared services, so it would need to be answered by James Ellis. In East Herts, the post sits under him.

5. What funding is available and is value for money achieved?

It is important to note that the funding for cyber security comes from the existing ICT budget.

6. How often health checks/progress reports are undertaken?

Yearly. We are currently participating in the pilot program run by the Department for Levelling Up, Housing and Communities (DLUHC) aimed at achieving the National Cyber Security Centre's (NCSC) Cyber Assessment Framework (CAF) accreditation. This accreditation is set to become the standard for cyber security within the Local Government. Additionally, we are also actively working towards obtaining the National Cyber Security Centre's Cyber Essentials Plus accreditation.

7. How are employees trained?

All employees are required to complete an annual mandatory e-learning course.

Matt Canterford, Head of IT