Request

1. Can you provide details on the specific cybersecurity measures and protocols in place to protect sensitive data and systems within the council?

2. How frequently are cybersecurity risk assessments conducted, and what actions are taken to address any vulnerabilities identified?

3. Could you provide information on the number of the following types of cyberattacks that your municipal council has encountered over the past two years?

    a) Phishing attempts
    b) Ransomware
    c) Data breaches

4. What is the current annual budget allocated to cybersecurity, and has this increased or decreased (in real terms) in the past two years?

5. What are current priorities for that investment:

    a) Staff training
    b) Security infrastructure / hardware
    c) Protection software
    d) Audits

6. Have you observed any changes in the quality/intensity of cyberattacks over the past two years, particularly in terms of the use of generative AI in an offensive capacity / as a method of attack?

Response

1. 1.The Council confirms that it holds this information. The status of cyber-attacks against the council is being withheld from disclosure. Section 31(1)(a) of the Freedom of Information Act 2000 (FoIA) states that information is exempt information if its disclosure under this Act would, or would be likely to, prejudice the prevention or detection of crime.

   Disclosure under the FoIA is deemed to be disclosure to the world at large, i.e. placing it in the public domain. The council must take steps to avoid malicious attack on its infrastructure, we therefore believe that the exemption at section 31(1)(a) of the FoIA is engaged.

   This exemption is subject to a Public Interest Test. Whilst the Council acknowledges the inherent public interest in transparency in its activities, it believes in this case the public interest in protecting the personal and sensitive data held on its systems is of more significance. Furthermore, the cost to the public purse of responding to cyber attacks adds to the balance of arguments against disclosure. Taking these factors into consideration, the Council assesses the public interest is not in favour of disclosure.

2. The Council confirms that it holds this information. The status of cyber-attacks against the council is being withheld from disclosure. Section 31(1)(a) of the Freedom of Information Act 2000 (FoIA) states that information is exempt information if its disclosure under this Act would, or would be likely to, prejudice the prevention or detection of crime.

   Disclosure under the FoIA is deemed to be disclosure to the world at large, i.e. placing it in the public domain. The council must take steps to avoid malicious attack on its infrastructure, we therefore believe that the exemption at section 31(1)(a) of the FoIA is engaged.

   This exemption is subject to a Public Interest Test. Whilst the Council acknowledges the inherent public interest in transparency in its activities, it believes in this case the public interest in protecting the personal and sensitive data held on its systems is of more significance. Furthermore, the cost to the public purse of responding to cyber attacks adds to the balance of arguments against disclosure. Taking these factors into consideration, the Council assesses the public interest is not in favour of disclosure.

3. The Council confirms that it holds this information. The status of cyber-attacks against the council is being withheld from disclosure. Section 31(1)(a) of the Freedom of Information Act 2000 (FoIA) states that information is exempt information if its disclosure under this Act would, or would be likely to, prejudice the prevention or detection of crime.

   Disclosure under the FoIA is deemed to be disclosure to the world at large, i.e. placing it in the public domain. The council must take steps to avoid malicious attack on its infrastructure, we therefore believe that the exemption at section 31(1)(a) of the FoIA is engaged.

   This exemption is subject to a Public Interest Test. Whilst the Council acknowledges the inherent public interest in transparency in its activities, it believes in this case the public interest in protecting the personal and sensitive data held on its systems is of more significance. Furthermore, the cost to the public purse of responding to cyber attacks adds to

the balance of arguments against disclosure. Taking these factors into consideration, the Council assesses the public interest is not in favour of disclosure.

4. Wigan Council have a fully managed service provided by Agilisys Ltd. The overall service includes cyber security, its not possible to separate.

5. We do not hold this information.

6. Yes it is clear cyber attacks are becoming more sophisticated.