Cyber assessment questionnaire

10 simple questions to answer:

1. Who is responsible for cybersecurity in your organisation
   Not who handles IT day to day, but who owns the risk.

2. Is your IT security managed in house, outsourced, or shared with a third party
   And do you know who to contact if there is an issue.

3. Do you know which systems are most critical to keeping the business running
   For example finance systems, customer data, operations, or communications.

4. What types of sensitive data does your organisation handle
   Such as personal data, financial information, commercial data, or regulated data.

5. Do third party suppliers have access to your systems or data
   And if so, do you know which ones.

6. If a cyber incident happened tomorrow, do you know who would lead the response
   This includes internal decision making, not just technical response.

7. Have you experienced a cyber incident or security issue in the past
   Including near misses, supplier incidents, or suspected compromises.

8. Do you have a clear process for people joining and leaving the organisation
   Particularly around access to systems and data.

9. Are you confident you could evidence oversight of your IT or security suppliers
   If asked by a regulator, insurer, or customer.

10. Is there anyone in the organisation who assumes cybersecurity is someone else's responsibility
    If the answer might be yes, that is worth exploring.

Please complete your answers on a separate document and send it to info@sccyber.co.uk.

www.sccyber.co.uk
info@sccyber.co.uk