digital octopii

Are you Secure Enough To Be My Supplier?

A quick security check for small businesses

Your customers may trust you with their data, systems, money or ability to operate. Could you give them convincing evidence that you are managing that risk?

Tick ✓ if you can confidently answer YES — and could provide evidence.

1. Protecting your systems

☐ **Multi-factor authentication (MFA)** is enabled for important accounts, especially email, Microsoft 365/Google Workspace, cloud services and administrator accounts.

☐ **Software and devices are kept up to date**, with security updates installed promptly.

☐ **Users do not routinely have administrator access** unless they genuinely need it.

☐ **Devices and systems are securely configured**, with unnecessary accounts, software and services removed or disabled.

☐ **Malware and other security protections** are enabled and kept up to date.

2. Protecting your information

☐ We know **what sensitive or customer information we hold and where it is stored**.

☐ Access to sensitive information is limited to **people who actually need it**.

☐ We have **backups of important information** that would allow us to recover following an incident.

☐ We have **tested restoring from backup**, rather than simply assuming our backups work.

3. Being ready when something goes wrong

☐ Staff know **who to contact if they suspect a cyber incident**.

☐ We know how we would **disable a compromised account or device quickly**.

☐ We know which **customers, insurers, regulators or other parties may need to be notified** following an incident.

☐ We know which systems and services are **critical to delivering our products or services**.

☐ We have considered how we would **continue operating if a critical system was unavailable.**

4. Managing your own suppliers

☐ We know which suppliers — such as **IT support, cloud, payroll, software or telecoms providers — could seriously disrupt our business if they failed**.

☐ We consider security when selecting important suppliers.

☐ We know how we would operate if a **critical supplier suffered a cyberattack or prolonged outage**.

5. Proving it to a customer

If a new customer asked today, could you provide:

☐ Your **information/cyber security policy**

☐ Evidence of **MFA, patching, backups and other key controls**

☐ Details of your **incident response and recovery arrangements**

☐ Evidence that staff receive **security awareness training**

☐ Evidence of recognised assurance, where appropriate — for example **Cyber Essentials, Cyber Essentials Plus or ISO/IEC 27001**

☐ Clear answers to a customer's **security questionnaire without guessing**

How did you do?

18–21 ✓ — Strong position

You should be able to give customers meaningful assurance — but make sure you can **prove** your answers.

12–17 ✓ — Some gaps

You have useful controls in place, but a customer questionnaire or tender may expose weaknesses.

0–11 ✓ — Start here

Focus first on the basics: **MFA, updates, secure configuration, access control, malware protection, backups and incident response.**

The question to take away:

Could you provide convincing security evidence to a new customer this week?

Security isn't just about avoiding an attack. It's increasingly about being able to demonstrate that you are a supplier your customers can trust.