Northstar
IT & CYBER ADVISORY

Ten Questions Every SME Board Should Ask About IT & Cyber Risk

01

QUESTION 01

What are the three most likely ways our business could be compromised?

If your IT supplier cannot name specific, realistic threats for a business of your type and size, phishing, business email compromise, ransomware via an unpatched system, that is a gap in their advisory capability. You should know your top three threats by name.

Why it matters: You cannot manage a risk you have not named.

02

QUESTION 02

When did we last independently verify our IT supplier is performing?

Asking your MSP if they are doing a good job is not oversight. It is a courtesy call. Independent verification means reviewing response times against contracted SLAs, checking that security controls are in place, and having someone with no commercial relationship with the supplier assess their performance. Most SMEs have never done this.

Why it matters: Unverified IT suppliers are unaccountable IT suppliers.

03

QUESTION 03

What would actually happen if we lost access to our systems for 72 hours?

This is the question most boards avoid because the honest answer is uncomfortable. Walk through it specifically. Which clients would be affected, what revenue would be at risk, what regulatory obligations would be triggered, and who would make the decisions. Businesses that have worked through this scenario recover faster and more effectively.

Why it matters: A plan that exists only in theory is not a plan.

04

QUESTION 04

Are our staff using AI tools, and do we have a policy governing how?

If you have not made a formal decision about AI, your staff have made informal ones for you. ChatGPT, Copilot and dozens of other AI tools are being used in most businesses right now, often with client data or personal data being processed through systems your organisation has never assessed. The absence of a policy is not neutrality. It is exposure.

Why it matters: Ungoverned AI use is a GDPR risk most boards have not assessed.

Northstar
IT & CYBER ADVISORY

Ten Questions Every SME Board Should Ask About IT & Cyber Risk

05

QUESTION 05

When did we last review what we are actually paying for in IT?

Most SMEs are overpaying for IT, not dramatically, but consistently. Unused licences, auto-renewed contracts, duplicate tools and legacy infrastructure all accumulate quietly. In a 30-person business spending five thousand pounds per month on technology, recoverable waste of ten to twenty percent is common. The answer is rarely reassuring but it is almost always actionable.

Why it matters: IT spend that is not reviewed is IT spend that is not controlled.

06

QUESTION 06

Do we know exactly where our personal and customer data is stored and who has access to it?

UK GDPR requires you to know what personal data you hold, where it lives, and who can access it. Most SMEs cannot answer this accurately. Data sits in cloud platforms, SaaS tools, email archives and shared drives, often with access that has never been reviewed. This is not a legal technicality. It is a commercial and reputational liability.

Why it matters: You cannot protect data you cannot locate.

07

QUESTION 07

Have we tested whether our backups actually work?

Having a backup in place is not the same as having a backup that works. Most SMEs assume their backup is running correctly because nobody has reported a failure. A backup that has never been tested is a backup you cannot rely on. The time to discover it does not work is not during an incident.

Why it matters: An untested backup is not a backup. It is a false sense of security.

08

QUESTION 08

Do we know which of our suppliers could cause the most damage if they were compromised?

Your cyber risk does not stop at your own systems. Every supplier with access to your network, your data, or your client information is a potential entry point. Most SMEs have never mapped their supplier risk, which means they do not know where their most significant third-party exposures are. Attackers do.

Why it matters: Your security is only as strong as your least secure supplier.

Northstar
IT & CYBER ADVISORY

Ten Questions Every SME Board Should Ask About IT & Cyber Risk

09

QUESTION 09

Could we demonstrate to a client or insurer that we take cyber security seriously?

Enterprise clients, cyber insurers and regulated sector procurement teams are increasingly asking for evidence, not assurances. Cyber Essentials certification, a documented security policy and evidence of active risk management are becoming baseline requirements. If you cannot demonstrate it, you are relying on trust rather than evidence. Trust does not satisfy an insurance assessor.

Why it matters: What you cannot evidence, you cannot defend.

10

QUESTION 10

Who is accountable for IT and cyber risk at board level in our business?

In most SMEs, the honest answer is nobody. IT is managed by the MSP, cyber risk is assumed to be covered, and the board has no designated owner for either. This is a governance gap that creates real commercial exposure, particularly when something goes wrong and the question becomes who was responsible for ensuring it did not.

Why it matters: Accountability for risk must sit somewhere. If it sits nowhere, the board owns it by default.

Carl Spencer

FOUNDER, NORTHSTAR IT & CYBER ADVISORY

Carl has 27+ years of experience in IT services, telecoms and cybersecurity. He provides fractional IT and cyber leadership to UK SMEs, independently, without vendor bias, and without the cost of a full-time hire.

northstaritadvisory.com | cs@northstaritadvisory.com | 0333 577 1714