



PHANTOM
Technology Solutions

PHANTOM TECHNOLOGY SOLUTIONS · BUYER'S GUIDE

10 questions your MSP should be able to answer in one meeting.

If your current IT provider hesitates, dodges, or says "let me check on that" to more than two of these, it's time to talk.

BUYER'S GUIDE

MSP
EVALUATION

FOR BUSINESS
OWNERS

Why this matters

Most business owners don't know what to ask their IT provider — so they end up evaluating their MSP on how fast tickets get closed. That's the wrong metric. A great MSP makes tickets less frequent, protects you from what you can't see, and can document every one of the decisions below in writing.

Bring these 10 questions to your next quarterly business review. Write down the answers. If the answers are vague, contradictory, or come with "we can get that for you" — you've found the problem.

1. What's our response-time commitment, in writing?

Why it matters. "We'll get to it" is not an SLA. You should know the number in minutes for critical issues, and the number should be the same every time you ask.

GOOD ANSWER

Under 15 minutes for critical issues, defined in the MSA, with credits for misses.

RED FLAG

"It depends" or "next business day" for anything serious.

2. Show me our current IT documentation — live, today.

Why it matters. If your MSP can't produce network diagrams, asset inventory, and account credentials on request, you are hostage. That documentation belongs to you.

GOOD ANSWER

A live, always-current documentation platform you have read access to.

RED FLAG

"Let me put something together" or a PDF from two years ago.

3. What security tools are running on every endpoint, and who watches them at 2 a.m.?

Why it matters. Antivirus is not security. You need EDR plus a human SOC/MDR watching the alerts around the clock.

GOOD ANSWER

AI-powered EDR on every endpoint, monitored 24/7 by a named SOC or MDR provider.

RED FLAG

"We have antivirus" or "we check alerts in the morning."

4. Have you actually tested a restore of our backups this quarter?

Why it matters. Untested backups are theater. The only backup that matters is the one that has been restored end-to-end recently.

GOOD ANSWER

Quarterly full-restore testing, with a written report.

RED FLAG

"Backups are running successfully" is not the same answer.

5. Are our backups immutable or air-gapped from production?

Why it matters. If ransomware gets to your backups, you don't have backups. Immutability is the difference between a bad week and a business-ending one.

GOOD ANSWER

Yes, with a specific explanation of how the immutability works.

RED FLAG

Blank stare or "they're in the cloud."

6. What's our patch compliance rate right now, and how old is the oldest unpatched critical vulnerability?

Why it matters. Most breaches exploit known, patched vulnerabilities. Your MSP should know this number cold.

GOOD ANSWER

A specific percentage and an answer measured in days, not months.

RED FLAG

"We run patches" with no metric attached.

7. If I got the cyber insurance application in front of me tomorrow, could you help me answer every question truthfully?

Why it matters. Many businesses attest to controls they don't actually have. If your claim is later denied, that's on the business — not the carrier.

GOOD ANSWER

Your MSP offers to sit with you and walk through it line by line.

RED FLAG

"Just check yes on the security stuff."

8. What's the plan for our business in the next 18–36 months?

Why it matters. A good MSP is a strategic partner, not a help desk. They should have a roadmap tied to your business goals.

GOOD ANSWER

A written technology roadmap reviewed quarterly by a vCIO or equivalent.

RED FLAG

"We'll react to whatever comes up."

9. What's our total cost of IT, including every line item we pay you or anyone else?

Why it matters. Break-fix invoices, project add-ons, and mystery licensing create hidden costs. You should be able to see the full number on one page.

GOOD ANSWER

A single flat rate covering everything, or a fully transparent line-item summary.

RED FLAG

Surprise invoices every quarter.

10. If we decided to leave, how would the transition work?

Why it matters. How your MSP answers this tells you whether you're a partner or a captive. A good provider makes leaving easy — which is exactly why clients stay.

GOOD ANSWER

"Here's the written offboarding process — we've done it before."

RED FLAG

Defensiveness, delay, or a surprise exit fee in the fine print.

If more than two answers gave you pause...

You don't have to switch MSPs tomorrow — but you do need a second opinion. PhantomTS will run a free Cyber Risk Report on your environment in under 24 hours and walk you through what we find, with no obligation and no high-pressure sales call. Start at phantomts.com.