10 Questions to Ask Your IT Provider

Before you sign or stay, use these to find out if your IT support is protecting your business or just keeping the lights on.

For Hampton Roads small businesses

Helix Stax • Portsmouth, VA • helixstax.com • hello@helixstax.com

Why These Questions Matter

Most business owners have no way to evaluate their IT provider. Not because they are not smart enough. Because nobody told them what good looks like.

So they renew contracts on autopilot. They assume that because nothing obvious has broken, everything must be fine. Then something breaks, or a breach happens, or a competitor's more efficient operations start showing up in the numbers.

These 10 questions are not a gotcha test. They are the questions your provider should be able to answer clearly, without hedging. If your provider stumbles on several, that is worth paying attention to.

Section 1: Security

Question 1: Is multi-factor authentication enforced across all our accounts and systems?

Why ask this: MFA is one of the most effective defenses against account compromise. Microsoft's 2024 Digital Defense Report found MFA blocks over 99% of identity-based attacks. If your provider is not enforcing it, your business is exposed on the most common attack vector.

What a good answer sounds like: "Yes. MFA is required on all email accounts, remote access, and any cloud service we manage for you. We enforce it, not just recommend it."

Question 2: When did you last test our backups by actually restoring data from them?

Why ask this: A backup that has never been tested is a guess, not a safety net. Plenty of businesses discover their backups were corrupted or incomplete only after a ransomware attack or hardware failure.

What a good answer sounds like: "We run restore tests on a scheduled basis, at minimum quarterly. I can show you the last test date and what we verified."

Question 3: How would you notify us if we had a breach or a security incident?

Why ask this: The Verizon 2024 Data Breach Investigations Report found 68% of breaches involve the human element. Your provider should have a clear, fast escalation path. "We would email you" is not a plan.

What a good answer sounds like: "We would call you directly within an hour of detection. We have a documented incident response process and we would walk you through containment in real time."

Section 2: Backups and Recovery

Question 4: Where is our data backed up, and how long would it take to get us operational after a failure?

Why ask this: Recovery time is what actually matters during a crisis, not just whether the backup exists. Losing three days of data is a different problem than losing three hours. Your provider should know your recovery objectives, not just their standard defaults. This includes your Microsoft 365 email and files and any cloud services your team uses day to day.

What a good answer sounds like: "Your data is backed up to encrypted cloud storage in a US data center. Based on your setup, we could have you operational within a defined window. If you need faster recovery, here is what that would require."

Question 5: If our office burned down tonight, what would it take to get us back to work tomorrow?

Why ask this: This question cuts past technical jargon. A provider who has thought about business continuity will give you a clear sequence of steps. One who has not will give you a vague answer.

What a good answer sounds like: "Here is exactly what we would do, in order. You would be able to do core functions within hours, and be fully operational within a defined time."

Section 3: Response and Support

Question 6: What is your actual response time when we have a critical problem, and is that in our contract?

Why ask this: Every provider says they are responsive. The question is whether that is a promise or a preference. Response time SLAs (service level agreements) define the difference. If it is not in writing, it is not a commitment.

What a good answer sounds like: "Critical issues get a response within a specific time, and that is in your service agreement. Here is where to find it." If they cannot point to it in your contract, it does not exist.

Question 7: Who actually handles our support tickets, and what are their qualifications?

Why ask this: Some providers route your tickets to whoever is available, or to an offshore help desk. Others have dedicated technicians who know your environment. The person who picks up the phone matters.

What a good answer sounds like: "Your account is handled by a specific team. Here are their certifications and how long they have been with us. We keep notes on your environment so whoever helps you already knows your setup."

Section 4: Proactivity and Strategy

Question 8: What do you send us each month, and what does it actually show?

Why ask this: Reactive IT support fixes problems after they happen. A proactive provider shows you what they are monitoring, what they found, and what they did about it. Monthly reporting is the minimum bar.

What a good answer sounds like: "Every month you get a report showing your security patch status, any alerts we investigated, uptime stats, and anything we recommend addressing. Here is an example."

Question 9: Are you recommending any changes to our setup in the next 12 months, and why?

Why ask this: Technology ages. Software goes end-of-life. Security requirements change. A provider with nothing to recommend is either not paying attention or not having the right conversations with you.

What a good answer sounds like: "Yes, we have a few things on our radar for your environment, with reasons and a timeline for each."

Section 5: Contracts and Billing

Question 10: If we decide to leave, what happens to our data, our accounts, and our systems?

Why ask this: Offboarding is where bad IT relationships get ugly. Some providers retain admin access longer than necessary. Some charge large transition fees. Some delay handing over credentials. You should know the answer before you need it.

What a good answer sounds like: "You own all your data and credentials. If you leave, we provide a full transition package including all credentials, documentation, and network diagrams within a defined time. Our contract outlines the offboarding process."

Scoring Your Provider

There is no pass or fail here. But there are patterns worth noticing.

8 to 10	Stumbled on 3 to 5	6 or more unclear
confident, specific answers	gaps to address	serious concern

8 to 10 confident, specific answers You are in good hands. Keep the relationship.

Stumbled on 3 to 5 You have some gaps to address. Bring these to your next business review and see how they respond. Some providers will rise to the feedback.

Could not answer 6 or more clearly That is not a small problem. These are basic components of good IT support. It may be time to get a second opinion.

One note: a good provider will not be defensive when you ask these questions. They will welcome them. A defensive response is itself useful information.

About Helix Stax

Helix Stax is a managed IT company based in Portsmouth, Virginia, working with small and mid-size businesses across Hampton Roads. We help local teams keep their technology secure, backed up, and out of the way so they can focus on running their business.

This guide is built on current data from named sources like Verizon, Microsoft, and the FBI, and on what we see working with real businesses in the area. No fear tactics, no jargon.

Portsmouth, VA • (804) 452-7829 • hello@helixstax.com • helixstax.com

[Space reserved for a client review or certification badge. Add one real testimonial or logo here before publishing.]

Want to Know How Your Setup Actually Holds Up?

We will answer all 10 of these questions about your current IT environment, free, no pressure. No slides. No sales pitch. Just an honest look at where things stand and what, if anything, needs attention.

This is what we call a Free IT Assessment. It takes about an hour. You walk away knowing what you have and what you do not.

Book a Free IT Assessment

cal.com/helixstax/assessment

Helix Stax • Portsmouth, VA • helixstax.com • hello@helixstax.com