Questions to Ask Your IT Provider

Whether you're choosing a new IT provider (MSP) or checking in with your current one, these questions gauge how well they align with Blueprint Basics: A Small Business Guide to Ransomware Defense. A good provider should be able to *show you* — not just tell you. Check each box as you go and jot what they said; if they can't answer clearly, that's a red flag.

☐ **1. Can you walk me through what happens if we get hit with ransomware — who do I call, and what are the first three things you'll do?** **(17.3 · Incident response)**

Look for: *A confident, specific answer is a good sign — vague reassurances aren't.*

☐ **2. Do you maintain an inventory of all our devices, software, and accounts? Can you show me a current report?** **(1.1 · 2.1 · 5.1 · Inventories)**

Look for: *You should be able to see the list, not just be told it exists.*

☐ **3. What's your process for managing our accounts when someone joins or leaves our team?** **(6.1 · 6.2 · Access on/offboarding)**

Look for: *Ask specifically how fast a departing employee's accounts get disabled.*

☐ **4. What's your plan for turning on multi-factor authentication (MFA) across our key accounts and apps — and which should come first?** **(6.3 · 6.4 · 6.5 · MFA)**

Look for: *They should name specifics — email, banking, and anything with customer or payment data first — and favor an authenticator app over text codes.*

☐ **5. How quickly can you restore our systems if we get attacked — and have you actually tested it recently?** **(11.1 · Data recovery)**

Look for: *Untested backups aren't backups. Ask for the date of the last successful restore test.*

☐ **6. Are our backups isolated from our main network so ransomware can't reach and encrypt them? Can you show me evidence?** **(11.4 · Isolated backups)**

Look for: *This is an 'air-gapped' or 'immutable' backup — ask them to show proof, not just say yes.*

☐ **7. How do you handle security patches — do you need my approval each time, or do they happen automatically?** **(7.1 · 7.2 · Patching)**

Look for: *Patches should be applied quickly; a backlog of unpatched systems is a major risk.*

☐ **8. Can you provide a simple report showing how your services align with the Blueprint for Ransomware Defense? (Blueprint alignment)**

Look for: *MSPs who know the Blueprint can map their services to its controls — a reasonable ask.*