10 CYBERSECURITY QUESTIONS TO ASK YOUR IT PROVIDER

TECH SEVEN PARTNERS

A practical checklist for business leaders evaluating how well their IT provider protects the business.

You don't need to be technical to evaluate cybersecurity.

These 10 questions help you understand how proactively your IT provider protects your business, how they respond to threats, and how they keep you informed and accountable.

1 How do you verify our backups are actually working and recoverable?

- ✓ Listen for: Regular human verification and periodic recovery testing.
- ⚠ Red flag: "Our backup software alerts us if something goes wrong."

2 Who reviews our security alerts, and how quickly are real threats investigated?

- ✓ Listen for: Someone responsible for reviewing alerts and taking action when needed.
- ⚠ Red flag: "The software handles that automatically."

3 What happens if we have a cybersecurity incident after hours?

- ✓ Listen for: 24/7 monitoring or a documented escalation process with people available.
- ⚠ Red flag: "We would address it when the office opens."

4 How do you know all of our computers are actually receiving critical security patches?

- ✓ Listen for: Verification that updates installed successfully and follow-up when they fail.
- ⚠ Red flag: "We automatically push updates to every computer."

5 How do you monitor for compromised employee passwords or accounts?

- ✓ Listen for: Ongoing monitoring for exposed credentials and suspicious account activity.
- ⚠ Red flag: "We require employees to change their passwords periodically."

6 What ongoing cybersecurity training and phishing testing do you provide our employees?

- ✓ Listen for: Regular training, phishing simulations, reporting, and follow-up for employees.
- ⚠ Red flag: "We cover cybersecurity during onboarding."

7 How often do you proactively review our technology against documented IT standards?

- ✓ Listen for: A recurring review with documented findings and accountability for fixes.
- ⚠ Red flag: "We keep an eye on things."

8 How do you help us plan technology around our business goals, budget, and growth?

- ✓ Listen for: Regular strategic conversations about goals, risks, budget, and future priorities.
- ⚠ Red flag: "We will let you know when something needs to be replaced."

9 If we were hit by ransomware or another major cyberattack tomorrow, what happens?

- ✓ Listen for: A documented incident response process with clear roles and responsibilities.
- ⚠ Red flag: "We would figure out what happened and go from there."

10 What reporting do you provide that shows us our risks, issues, and technology roadmap?

- ✓ Listen for: Clear reporting on risks, issues, improvements made, and recommended next steps.
- ⚠ Red flag: "You will hear from us if there is a problem."

Protection starts with process, accountability, and proof.

Your IT provider should be able to show you how your business is protected, who is responsible, and how that protection is verified.