# Is Your IT Company Truly Doing What You're Paying For?

## A lot of what you're paying for is intangible – a proactive approach that prevents issues, a data backup plan that keeps you prepared for disaster, a comprehensive approach to security that prevents attacks.

So how do you really, truly know your IT company is doing what you're paying for if it's intangible? Are you supposed to blindly trust that they're doing what they say they are? The short answer: Absolutely not. If they're not actively communicating what they're doing with you, it's time to start asking some questions. Why? Because we've seen it happen time and time again: a business trusts their technology provider to do what they say, and eventually, a natural disaster or cyber-attack DOES happen and there's unable to recover because nothing was actually done.

- The latest patches haven't been applied
- The backups weren't verified and tested on a regular basis
- The server hasn't been maintained in a while
- The cybersecurity solutions aren't actively monitored and/or used

**A lot of what you're paying for is intangible – a proactive approach that prevents issues, a data backup plan that keeps you prepared for disaster, a comprehensive approach to security that prevents attacks.**

There are so many ways an IT company can take shortcuts. That's why it's important to ask questions if they're not actively communicating what they're doing with you. Here's a few questions to ask:

## 1. How often is maintenance performed?

Ask how often they're performing some type of maintenance on your servers, computers, and any other hardware within your environment. Next, ask what type of maintenance they're doing - from patches to updates to bug fixes and everything in between.

## 2. What cybersecurity solutions do you have in place?

Ask for details on the type of cybersecurity solution they have in place. It's easy enough to say you're taking a multi-layered approach to cybersecurity, but make sure they actually are. This should include firewalls, encryption, anti-virus software, intrusion detection software, and more.

## 3. How often do you check in on our cybersecurity solutions?

Ask how often they're checking in on things like your firewall definitions, anti-virus software, and other cybersecurity solutions that are in place. Make sure they regularly update the tools in place to keep them running properly.

## 4. How often will you verify and test our backups?

Ask how often they're verifying and testing the backups in place. You want to make sure they're tested quite regularly to ensure recoverability when something goes wrong, such as a cyber-attack or human error resulting in data loss.

**Still not feeling confident that you're getting what you're paying for? Let's talk. We'll help you determine whether or not it's time to move on. Call (310) 477-4441.**