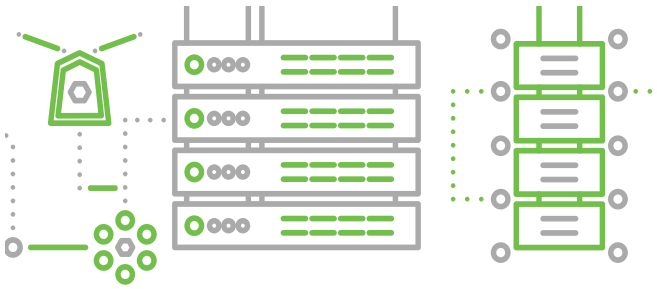


IT Services

Buyers Guide

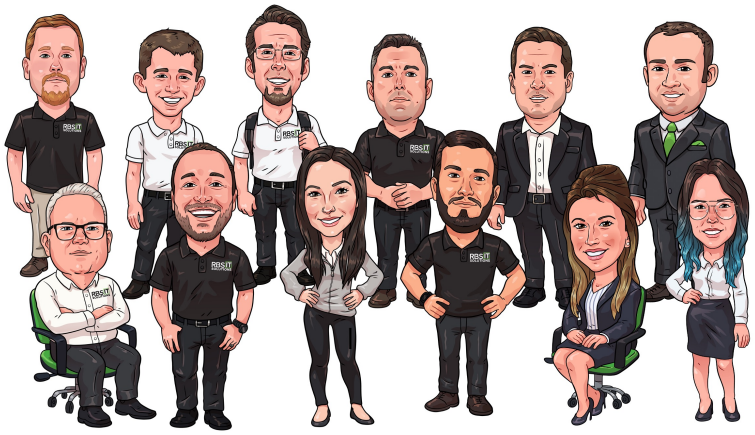
The Business Owner's Guide
To IT Support And Services

What You Should Expect To Pay For Managed IT For Your Business.

(And How To Get *Exactly* What You Need Without Unnecessary Extras, Hidden Fees And Bloated Contracts)

Read this guide and you'll discover:

- ✓ The three most common ways IT services companies charge for their services, and the pros and cons of each approach.
- ✓ A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it.
- ✓ Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to.
- ✓ How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate.
- ✓ 19 revealing questions to ask your IT support provider BEFORE giving them access to your computer network, systems and data.



If you are the the CEO or owner of a business that is currently looking to outsource some or all IT support for your company, this report contains important information that will be extremely valuable to you as you search for a competent firm you can **trust**. RBS IT Solutions has been providing IT services to businesses in the Wichita-metro area for over 15 years. You may not have heard of us before, but I'm sure you're familiar with one or more of the other 100+ businesses that we serve. A few of their comments are enclosed. One of the **most common questions** we get from new prospective clients is **"How much does it cost?"** Since this seems to almost always be a leading question or point of discussion, we to assembled this report for the following (3) reasons:

1. There is an easy way to answer this question and educate all prospective clients who come to us on the most common ways IT services companies package and price their services, and the pros and cons of each approach.

2. We hope to bring to light a few "industry secrets" about IT services contracts and SLAs (service level agreements) that almost no business thinks about, understands or knows to ask about when evaluating IT services providers that can end up burning you with hidden fees and locking you into a long-term contract when they are unwilling or unable to deliver the quality of service you need.

3. Ultimately, our goal is to educate businesses on how to pick the **right** IT services company for their specific situation, budget and needs based on the ***VALUE*** the company can deliver, not just the price, high OR low.

In the end, our purpose is to help you make the most informed decision possible, so you end up working with an IT provider who helps you solve your problems and accomplish what you want in a time frame, manner and budget that is right for you.

Dedicated to serving you,

RBS IT Solutions

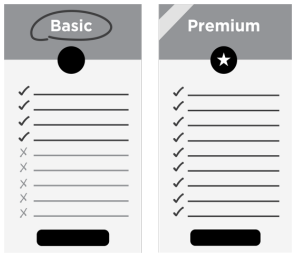
Comparing Apples To Apples: The Predominant IT Service Models Explained

Before you can accurately compare the fees, services and deliverables of one IT services company with another, you need to understand the three predominant service models most of these companies fit within. Some companies offer a blend of all three, while others are strict about offering only one service plan. The three predominant service models are:

- **Time and Materials.** In the industry, we call this "break-fix" services. Essentially you pay an agreed-upon hourly rate for a technician to "fix" your problem when something "breaks." Under this model, you might be able to negotiate a discount based on buying a block of hours. The scope of work may be simply to resolve a specific problem, like fixing a problem with your e-mail, or it may encompass a large project, like a network upgrade or move that has a specific result and end date clarified. Some companies will offer staff augmentation and placement under this model as well.

- **Managed IT Services.** This is a model where the IT services company takes the role of your fully outsourced "IT department" and not only installs and supports all the devices and PCs that connect to your server(s), but also offers phone and on-site support, antivirus, cyber security, backup and a host of other services to monitor and maintain the health, speed, performance and security of your computer network.

- **Software Vendor-Supplied IT Services.** Many software companies will offer IT support for their customers in the form of a help desk or remote support for an additional fee. However, these are typically scaled-back services, limited to troubleshooting their specific application and NOT your entire computer network and all the applications and devices connected to it. If your problem resides outside of their specific software or the server it's hosted on, they can't help you and will often refer you to "your IT department." While it's often a good idea to buy some basic-level support package with a critical software application you use to run your business, this is not enough to provide the full IT services and support most businesses need to stay up and running.



When looking to outsource your IT support, the two service models you are most likely to end up having to choose between are the "managed IT services" and "break-fix" models. Therefore, let's dive into the pros and cons of these two options, and then the typical fee structure for both.

To Schedule Your FREE Assessment,
please visit **www.rbsitsolutions.com** OR call our office at 316-365-8701.

Managed IT Services Vs. Break-Fix: Which Is The Better, More Cost-Effective Option?

You've probably heard the famous Benjamin Franklin quote, "An ounce of prevention is worth a pound of cure." I couldn't agree more – and that's why it's my sincere belief that some form of managed IT is essential for every small business.

In our company, we offer different plans to fit the needs of our clients. In some cases, where the business is small, we might offer a very basic managed services plan to ensure the most essential maintenance is done, then bill the client hourly for any support used. For our smallest clients, they often find this the most economical. But for some of our midsized organizations, we offer a fully managed approach where more comprehensive IT services are covered in a managed plan. By doing this, we can properly staff for their accounts and ensure they get the fast, responsive support and expertise they need.

The only time I would recommend a "time and materials" approach is when you already have a competent IT person or team proactively managing your computer network and simply have a specific IT project to complete that your current in-house IT team doesn't have the time nor expertise to implement (such as migrating to a cloud-based solution, implementing a cyber security plan, etc.). Outside of that specific scenario, I do not think the break-fix approach is a good idea for general IT support for one very important, fundamental reason: you'll ultimately end up paying for a pound of "cure" for problems that could have easily been avoided with an "ounce" of prevention.

Why Regular Monitoring And Maintenance Is Critical For Modern-Day Computing Environments

The fact of the matter is computing environments absolutely, positively need ongoing maintenance and monitoring to stay optimized and secure. The ever-increasing dependency we have on IT systems and the data they hold – not to mention the *type* of data we're now saving digitally – has given rise to very smart and sophisticated cybercrime organizations that work around the clock to do one thing: hack into your network to steal data or money or to hold you ransom.

As you may know, ransomware is at an all-time high because organized criminals have made millions of dollars robbing one small business owner at a time. But that's not their only incentive.

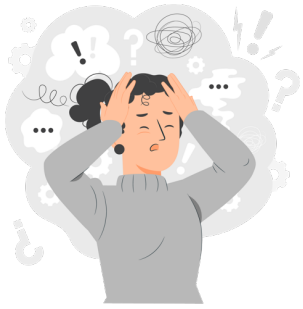
Some will attempt to hack your network to gain access to bank accounts, credit cards or passwords to rob you (and your clients). Some use your computer network to send spam using YOUR domain and servers, host pirated software and, of course, spread viruses. Some even do it just for the "fun" of it.

And don't think for a minute these cybercriminals are solo crooks working alone in a hoodie out of their basement. They are highly organized and well-run operations employing *teams* of hackers who work together to scam as many people as they can. They use advanced software that scans millions of networks for vulnerabilities and use readily available data on the dark web of YOUR usernames, passwords, e-mail addresses and other data to gain access.

Of course, this isn't the only IT danger you face. Other common "disasters" include rogue employees, lost devices, hardware failures (still a BIG reason for data loss), fire and natural disasters and a host of other issues that can interrupt or outright destroy your IT infrastructure and the data it holds. Then there's regulatory compliance for any business hosting or touching credit card or financial information, medical records and even client contact information, such as e-mail addresses.

Preventing these problems and keeping your systems up and running (which is what managed IT services is all about) is a LOT less expensive and damaging to your organization than waiting until one of these things happens and then paying for emergency IT services to restore your systems to working order (break-fix).

Should You Just Hire A Full-Time IT Manager?



In most cases, it is not cost-effective for companies with under 75-100 employees to hire a full-time IT person for a couple of reasons.

First of all, no one IT person can know everything there is to know about IT support and cyber security. If your company is big enough and growing fast enough to support a full-time IT lead, you probably need more than one guy. You need someone with help-desk expertise as well as a network engineer, a network administrator, a CIO (chief information officer) and a CISO (chief information security officer).

Therefore, even if you hire a full-time IT person, you may still need to supplement their position with co-managed IT support using an IT firm that can fill in the gaps and provide services and expertise they don't have. This is not a bad plan; what IS a bad plan is hiring one person and expecting them to know it all and do it all.

Second, finding and hiring good people is difficult; finding and hiring skilled IT people is incredibly difficult due to the skill shortage for IT. And if you're not technical, it's going to be very difficult for you to interview candidates and sift and sort through all the duds out there to find someone with good skills and experience. Because you're not technical, you might not know the right questions to ask during the interview process or the skills they need to do the job.

More often than not, the hard and soft costs of building an internal IT department for general IT support just don't provide the best return on investment for the average small to midsize business.

Why "Break-Fix" Works Entirely In Their Favor, Not Yours

Under a "break-fix" model, there is a fundamental conflict of interests between you and your IT firm. The IT services company has no incentive to prevent problems, stabilize your network or resolve problems quickly because they are getting paid by the hour when things stop working; therefore, the risk of unforeseen circumstances, scope creep, learning curve inefficiencies and outright incompetence are all shifted to YOU, the customer. Essentially, the more problems you have, the more they profit, which is precisely what you DON'T want.

Under this model, the IT provider can take the liberty of assigning a junior (lower-paid) technician to work on your problem – one who may take two to three times as long to resolve an issue that a more senior (and more expensive) technician might resolve in a fraction of the time. There is no incentive to properly manage the time of that technician or their efficiency, and there is every reason for them to prolong the project and find MORE problems than solutions. Of course, if they're ethical and want to keep you as a client, they *should* be doing everything possible to resolve your problems quickly and efficiently; however, that's akin to putting a German shepherd in charge of watching over the ham sandwiches. Not a good idea.

Second, it creates a management problem for you, the customer, who now has to keep track of the hours they've worked to make sure you aren't getting overbilled, and since you often have no way of really knowing if they've worked the hours they say they have, it creates a situation where you really, truly need to be able to trust they are being 100% ethical and honest AND tracking THEIR hours properly (not all do).

And finally, it makes budgeting for IT projects and expenses a nightmare since they may be zero one month and thousands the next.

What Should You Expect To Pay?

Important! Please note that the following price quotes are industry averages based on a recent IT industry survey conducted of over 750 different IT services firms. We are providing this information to give you a general idea of what most IT services firms charge and to help you understand the VAST DIFFERENCES in service contracts that you must be aware of before signing on the dotted line. Please understand that this does NOT reflect our pricing model or approach, which is simply to understand exactly what you want to accomplish FIRST and then customize a solution based on your specific needs, budget and situation.

To Schedule Your FREE Assessment,
please visit **www.rbsitsolutions.com** or call our office at 316-365-8701.

Hourly Break-Fix Fees:

Most IT services companies selling break-fix services charge between $100-$150 per hour with a one-hour minimum. In most cases, they will give you a discount of 5% to as much as 20% on their hourly rates if you purchase and pay for a block of hours in advance.

If they are quoting a **project**, the fees range widely based on the scope of work outlined. If you are hiring an IT consulting firm for a project, I suggest you demand the following:

- **A very detailed scope of work that specifies what "success" is.** Make sure you clearly detail what your expectations are in terms of performance, workflow, costs, security, access, etc. The more detailed you can be, the better. Detailing your expectations up front will go a long way toward avoiding potential miscommunications or additional, unanticipated expenses later on.
- **A fixed budget and time frame for completion.** Agreeing to this up front aligns both your agenda and the consultant's. Be very wary of loose estimates that allow the consulting firm to bill you for "unforeseen" circumstances. The bottom line is this: it is your IT provider's responsibility to be able to accurately assess your situation and quote a project based on their experience. You should not have to pick up the tab for a provider underestimating a job or for their inefficiencies.

Managed IT Services:

Most managed IT services firms will quote you a MONTHLY fee based on the number of devices they need to maintain, back up and support. In south-central Kansas, that fee is somewhere in the range of $125 to $250 per server, $90 to $125 per desktop and approximately $10 per smartphone or mobile device.

If you hire an IT provider and sign up for a managed IT services contract, here are some things that SHOULD be included (make sure you read your contract to validate this):

- Security patches applied weekly, if not daily, for urgent and emerging threats
- Antivirus updates and monitoring
- Firewall updates and monitoring
- Backup monitoring and test restores
- Monitoring workstations and servers for signs of failure
- Optimizing systems for maximum speed
- Documentation of your network, software licenses, credentials, etc.

The following services may **NOT be included** and will often be billed separately. This is not necessarily a "scam" or unethical UNLESS the managed IT services company tries to hide these fees in their service agreement. Make sure you review your contract carefully to know what is and is NOT included!

- Hardware
- Software licenses
- Special projects
- Upgrades

Warning! Beware the gray areas of "all-inclusive" service contracts. In order to truly compare the "cost" of one managed IT services contract with another, you need to make sure you fully understand what IS and ISN'T included AND the SLA (service level agreement) you are signing up for. It's VERY easy for one IT services provider to appear less expensive than another UNTIL you look closely at what you're getting.

19 Questions You Should Ask Your IT Services Provider Before Hiring Them

The following are questions to ask your IT services provider that will clarify exactly what you're getting for the money. Some of these items may not be that important to you, while others (like response time, adequate insurance and uptime guarantees) may be critical. Make sure you fully understand each of these items before making a decision about who the right provider is for you, then make sure you get this IN WRITING.

Customer Service:

Q1 When I have an IT problem, how do I get support?

Our Answer: When a client has a problem, a "ticket" is created in our help desk system so we can properly triage, prioritize, assign, track, resolve and document and issues. However, some IT firms force you to log in to submit a ticket and won't allow you to call or e-mail them. This is for THEIR convenience (and a thorn in your side). Also, make sure they have reliable processes in place to keep track of client "tickets" and requests. Otherwise, your requests will sometimes get overlooked, skipped and forgotten.

Requesting support should also be EASY for you. So be sure to ask how you can submit a problem to their support desk for resolution. We make it easy. Calling, e-mailing or submitting a ticket via our portal puts your IT issue on the fast track to getting resolved.

Q2 Do you offer after-hours support, and if so, what is the guaranteed response time?

Our Answer: Any good IT company will answer their phones LIVE (not voice mail or phone trees) and respond from 9:00a-5:00p every weekday. But what if you require after hours IT support during nights and weekends? Not only can you reach our after-hours support any time and any day, we GUARANTEE a response time of for problems marked "emergency," such as a network being down or a critical problem that is significantly impacting the ability to work.

Q3 Do you have a written, guaranteed response time for working on resolving problems?

Our Answer: Most IT firms offer a 60-minute or 30-minute response time to your call during normal business hours. Be very wary of someone who doesn't have a guaranteed response time IN WRITING – that's a sign they are too disorganized, understaffed or overwhelmed to handle your request.. A good IT firm should also be able to show you statistics from their PSA (professional services automation) software, where all client problems (tickets) get responded to and tracked. Ask to see a report on average ticket response and resolution times.

Q4 Do you have a feedback system in place for your clients to provide "thumbs up" or "thumbs down" ratings on your service?

Our Answer: If they don't have this type of feedback system, they may be hiding their poor customer service results. If they DO have one, ask to see the actual scores and reporting. That will tell you a lot about the quality of service they are providing. We are very proud of our positive client feedback scores and will be happy to show them to you.

IT Maintenance

Q5 Do you offer true managed IT services and support?

Our Answer: You want to find an IT company that will proactively monitor for problems and perform routine maintenance on your technology systems. If they don't have the ability to do this, or they don't offer it, we strongly recommend you look somewhere else. Our remote network monitoring tools watch over your network to pro-actively identify developing problems, security issues and other issues so we can address them BEFORE they turn into bigger problems.

Q6 What is NOT included in your managed services agreement?

Our Answer: Another "gotcha" many IT companies fail to explain is what is NOT included in your monthly managed services agreement that will trigger an invoice. Their so-called "all you can eat" option is RARELY true – there are limitations to what's included and you want to know what they are BEFORE you sign.

It's very common for projects to not be included, like a server upgrade, moving offices, adding new employees and, of course, the software and hardware you need to purchase.

- Do you offer truly unlimited help desk? (Make sure you are not nickel-and-dimed for every call.)
- Does the service include support for cloud services, such as Microsoft 365?
- Do you charge extra if you have to resolve a problem with a line-of-business application, Internet service provider, phone system, leased printer, etc.? (What you want is an IT company that will own the problems and not point fingers. We are happy to call the vendor or software company on your behalf.)
- What about on-site support calls? Or support to remote offices?
- If our employees had to work remote (due to a shutdown, natural disaster, etc.), would you provide support on their home PCs or would that trigger a bill?
- If we were to get ransomed or experience some other disaster (fire, flood, theft, tornado, hurricane, etc.), would rebuilding the network be included in the service plan or considered an extra project we would have to pay for? (Get this IN WRITING. Recovering from such a disaster could take hundreds of hours of time for your IT company's techs, so you want to know in advance how a situation like this will be handled before it happens.)

Our managed services agreement is completely transparent.

Regardless of how many tickets are initiated, how much work we perform in each month, or whether our engineers are onsite or remote – your monthly cost remains the same. This model is designed to allow our team to provide ongoing support to our clients in a limitless capacity.

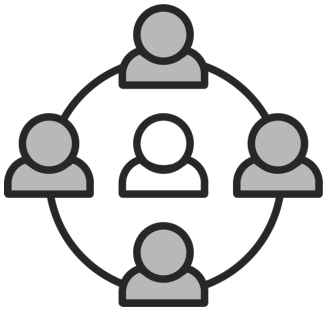
Q7 Is your help desk local or outsourced?

Our Answer: Be careful because smaller IT firms may outsource this critical function. As a result, you may get a tech who is not familiar with you, your network, previous problems and personal preferences. Or worse, they may not be as qualified. This can be frustrating and lead to the same problems cropping up over and over, longer resolution time and you having to spend time educating the tech on your account.

Fortunately, we provide a team technicians and engineers to support your company and who will get to know you, as well as your preferences and history. We don't outsource or hire contractors. Our team of employees are than more capable of successfully resolving any IT issues.

Q8 How many engineers do you have on staff?

Our Answer: Everyone gets sick, has emergencies, goes on vacation or takes a few days off from time to time. We have more than enough full-time techs on staff to cover and provide continuity when one or more of our employees are unable to work. If one tech is out or unavailable, another can step in and know your network settings, history, previous issues, etc., and how those issues were resolved. This is important or you'll be constantly frustrated with techs who are starting over to resolve a known issue or may screw up something because they don't understand or have a blueprint of your computing environment.



Q9 Do you meet with your clients quarterly as part of your managed services agreement?

Our Answer: To us, there's nothing more important than face-to-face time with our clients. Therefore, we make it a priority to meet with all our clients at least quarterly to provide a "technology review." In these meetings, we provide you with the status updates of projects you're working on and of the health and security of your network. Our quarterly meetings with you are C-level discussions where we openly discuss your business goals, including your IT budget, critical projects, compliance issues, known problems and cyber security best practices.

Our goal in these meetings is to help you improve operations, increase efficiencies and ensure your organizational productivity stays high. This is also your opportunity to give us feedback.

Cyber Security:

Q10 What cyber security certifications are held by your technicians and engineers?

Our Answer: It's important that your IT firm have *some* type of *recent* training and certifications, and they should be able to answer this question, which demonstrates a dedication to learning and keeping up with the latest cyber security protections. If they don't have any, and they aren't investing in ongoing training for their engineers, that's a red flag. Some business owners won't invest in training and give this excuse: "What if I spend all this money training my employees and then they leave us for another job?" Our response is "What if you DON'T train them and they stay?"

You can feel confident that our in-house technicians have among the most advanced cyber security training and certifications available, including Microsoft, Fortinet, The Computing Technology Industry Association CompTIA, The International Information System Security Certification Consortium (ISC)2, and The SANS Institute (officially the Escal Institute of Advanced Technologies).

Q11 How do you harden our workstations, endpoints, and servers to ensure they're not compromised and creating risk & exposure across our network?

Our Answer: As above, the question may get a bit technical. The key is that they HAVE an answer and don't hesitate to provide it. Some of the things they should mention are:

- 2FA (two-factor authentication)
- Advanced end-point protection, NOT just antivirus
- Behavioral and AI-based monitoring to analyze potential threat indicators
- Defense-in-depth (no single control is a silver bullet)
- Limited use of privileged access and administrative accounts

Because a combination of these lockdown strategies is essential to protecting your network and data, we employ ALL of these for our clients. Effective cyber security should never compromise between choosing this OR that. It should feature every weapon in your arsenal.

Q12 What cyber liability and errors and omissions insurance do you carry to protect me?

Our Answer: Here's something to ask about: if THEY cause a problem with your network that causes you to be down for hours or days, to lose data or get hacked, who's responsible? What if one of their technicians gets hurt at your office? Or damages your property while there?

In this litigious society we live in, you better make darn sure whomever you hire is adequately insured with both errors and omissions insurance, workers' compensation and cyber liability – and don't be shy about asking them to send you the policy to review!

Rest assured, we make it a priority to carry all the necessary insurance to protect you. Simply ask, and we will be happy to share these details.

Q13 If our business was to experience a disaster, pandemic, or other shutdown that impacted routine operations, do you offer solutions for remote access?

Our Answer: If Covid taught us anything, it's that work-interrupting disasters CAN and DO happen when you least expect them. Fires, floods, hurricanes and tornadoes can wipe out an entire building or location. Covid forced everyone into lockdown, and it could happen again.

That's why you want to ask your prospective IT provider how quickly they were able to get their clients working remotely (and securely) when Covid shut everything down. Ask to talk to a few of their clients about how the process went.

Q14 How do you monitor for and detect security threats?

Our Answer: A SOC (pronounced "sock"), or security operations center, is a centralized department within a company to monitor and deal with security issues pertaining to a company's network. What's tricky here is that some IT firms have the resources and ability to run a good SOC in-house. Others cannot and outsource it because they know their limitations.

But the key thing to look for is that *they have one*. Less experienced IT providers may monitor your network hardware, such as servers and workstations, for uptime and patches, but they might not provide security monitoring. This is particularly important if you work with sensitive data (financial information, medical records, credit cards, etc.) and fall under regulatory compliance for data protection.

Rest assured, we do have an in-house or outsourced SOC to provide proactive security monitoring for our clients to better prevent a network violation or data breach.

Backups & Disaster Recovery

Q15 What is the timeline to get my network back up and running in the event of a disaster?

Our Answer: There are two aspects to backing up your data: the first is "fail over" and the other is "fail back." For example, if you get a flat tire, you would fail over by putting on the spare tire to get to a service station where you can fail back to a new or repaired tire.

If you were to have a disaster that wiped out your data and network – you want to make sure you have a solution in place so your employees could continue to work with as little interruption as possible. This fail-over should be in the cloud and locked down separately to avoid ransomware from infecting the backups as well as the physical servers and workstations.

But, at some point, you need to fail back, and that's a process that could take days or even weeks. So, one of the key areas you want to discuss with your next IT provider is how they handle both data backup AND disaster recovery. They should have a plan in place and be able to explain the process for the emergency fail-over as well as the process for restoring your systems.

Regardless of natural disaster, equipment failure or any other issue, your business should ALWAYS be able to be operational with its data within six to eight hours or less, and critical operations should be failed over immediately. We understand how important your data is and how getting your team up and running quickly is essential to your business success.

Q16

Do you INSIST on doing periodic test restores of backups to verify data integrity to ensure that it could be restored in the event of a disaster?

Our Answer: A great IT provider will place eyes on your backup systems every single day to ensure that backups are actually occurring, and without failures. However, in addition to this, your IT company should perform a monthly randomized "fire drill" test restore of some of your files from backups to make sure your data CAN be recovered in the event of an emergency. After all, the WORST time to "test" a backup is when you desperately need it.

If you don't feel comfortable asking your current IT company to test your backup OR if you have concerns and want to see proof yourself, just conduct this little test: Copy three unimportant files onto a thumb drive (so you don't lose them) and delete them from your server. Make sure one was newly created that same day, one was created a week earlier and the last a month earlier. Then call your IT company and let them know you've lost three important documents and need them restored from backups as soon as possible. They should be able to do this easily and quickly. If not, you have a problem that needs to be addressed immediately!

Verifying your backups daily and testing them on a regular basis is a cornerstone of a successful overall IT strategy. These are the lengths we go to for all our clients, including multiple random "fire drill" test restores to ensure ALL your files are safe because they are always backed up.

TIP: ***Ask your IT provider about the "3-2-2" rule of backups, which has evolved from the "3-2-1" rule. The 3-2-1 rule is that you should have three copies of your data: your working copy, plus two additional copies on different media (tape and cloud), with at least one being off-site for recovery.***

That rule was developed when tape backups were necessary because cloud backups hadn't evolved to where they are today. Today, there are more sophisticated cloud backups and BDR (backup and disaster recovery) devices. Therefore, we recommend three copies of your data…

Q17

What about a disaster, pandemic or shutdown that prevented us from being in the office, how would you enable our staff to work from a remote location?

Our Answer: If Covid taught us anything, it's that work-interrupting disasters CAN an d DO happen when you least expect them. Fires, floods, hurricanes and tornadoes can wipe out an entire building or location. Covid forced everyone into lockdown, and it could happen again.

That's why you want to ask your prospective IT provider how quickly they were able to get their clients working remotely (and securely) when Covid shut everything down. Ask to talk to a few of their clients about how the process went.

Q18

Do you offer documentation of our network as part of the plan, and how does that work?

Our Answer: Network documentation is exactly what it sounds like: the practice of maintaining detailed technical records about the assets you own (computers, devices, software, directory structure, user profiles, passwords, etc.) and how your network is set up, backed up and secured.

Why is this important? There are several reasons: First, it shows professionalism and integrity in protecting YOU. No IT person or company should be the only holder of the keys to the kingdom. Because we document your network assets and passwords, you have a blueprint you can give to another IT person or company to take over if necessary. Second, good documentation allows the engineers working on your account to resolve problems faster.

Q19

Show me your process and documentation for onboarding me as a new client.

Our Answer: The reason for asking this question is to see if they HAVE SOMETHING in place. A plan, a procedure, a process. Don't take their word for it. Ask to SEE it in writing. What's important here is that they can produce some type of process. Further, they should be able to explain how their process works.

One thing you will need to discuss in detail is how they are going to take over from the current IT company – particularly if the current company is hostile. It's disturbing to me how many IT companies or people will become bitter and resentful over being fired and will do things to screw up your security and create problems for the new company as a childish way of getting revenge. A solid IT company will have a process in place for handling this. If you consider us as your next IT services firm, we will gladly share our new client onboarding process and documentation.

Other Things To Notice And Look Out For:

Are they good at answering your questions in terms you can understand and not confusing "geek-speak"?

Good IT companies won't confuse you with techno-mumbo-jumbo, and they certainly shouldn't make you feel stupid for asking questions. All great consultants have the "heart of a teacher" and will take time to answer your questions and explain everything in simple terms. As you interact with them in the evaluation process, watch for this.

Our technicians are trained to take time to answer your questions and explain everything in simple terms. Just look at what this one client/these clients had to say:

PRIMECONCEPTS
Creative Marketing Agency

> **"RBS IT Solutions provides an unmatched customer experience with top tier technical talent. IT made easy and painless."**
>
> **- Ford Saeks, President**

Do they and their technicians present themselves as true professionals when they are in your office?

If you'd be embarrassed if YOUR clients saw your IT provider behind your desk, that should be a big red flag. How you do anything is how you do everything, so if they cannot show up on time, are sloppy with paperwork, show up unprepared, forget your requests and seem disorganized in the meeting, how can you expect them to be on point with your IT?

Our team are true professionals who you would be proud to have in your office. They dress professionally and show up on time, and if they cannot be there on time (for some odd, unforeseen reason), we always notify the client immediately. We believe these are minimum requirements for delivering a professional service.

To Schedule Your FREE Assessment,
please visit **www.rbsitsolutions.com** or call our office at 316-365-8701.

See What Other Clients Have To Say…

Health Ministries Clinic
COMMUNITY HEALTH CENTER

"Cybersecurity threats continually transform and mature. RBS IT Solutions delivers the expertise to constantly monitor our environment and help us defend against these threats.

We can feel more confident knowing our technology systems are protected and secure."

- Matthew Schmidt, President

WICHITA FAMILY DENTAL

"Our previous IT provider could not meet our needs in terms of quick response and high level of service. Our office is committed to providing exceptional dental care and we needed and IT partner to support us in this effort.

Since working with RBS IT Solutions, they have filled that role as our long-term partner. This is evidenced in our daily interactions and their willingness to go the extra mile."

– Dr. Charles Pierson, Partner

HUTTON & HUTTON
LAW FIRM, LLC

"It was clear from our first meeting that RBS IT Solutions understood our business needs and had excellent solutions to problems we were having with our systems.

They spend the time to get the details right and put together easy-to-understand solutions that are far more comprehensive than other IT providers we have worked with ."

– Daniel Back, Manager

A Final Word And Free Offer To Engage With Us

1. **We Respond Within 5 Minutes Or Less.** The average amount of time it takes for one of our clients to get on the phone with a technician who can start working on resolving their problem is 3.5 minutes. We know you're busy and we have made a sincere commitment to making sure your computer problems get fixed FAST. And since most repairs can be done remotely using our secure management tools, you don't have to wait for a technician to show up.

2. **No Geek-Speak.** You deserve to get answers to your questions in PLAIN ENGLISH, not in confusing technical terms. Our technicians will also not talk down to you or make you feel stupid because you don't understand how all this "technology" works. That's our job!

3. **100% No-Small-Print Satisfaction Guarantee.** Quite simply, if you are not happy with our work, we'll do whatever it takes to make it right to YOUR standards without charging you for it. And if we can't make it right, the service is free.

4. **All Projects Are Completed On Time And On Budget.** When you hire us to complete a project for you, we won't nickel-and-dime you with unforeseen or unexpected charges or delays. We guarantee to deliver precisely what we promised to deliver, on time and on budget, with no excuses.

5. **Lower Costs, Waste And Complexity With Cloud Solutions.** By utilizing cloud computing and other advanced technologies, we can eliminate the cost, complexity, and problems of managing your own in-house server while giving you more freedom, lowered costs, tighter security and instant disaster recovery.

6. **We Won't Hold You Hostage.** Many IT companies do NOT provide their clients with simple and easy-to-understand documentation that outlines key network resources, passwords, licenses, etc. As a client of ours, we'll provide you with full, written documentation of your network and all the resources, software licenses, passwords, hardware, etc., in simple terms so YOU can understand it. We keep our clients by delivering exceptional service – not by keeping them in the dark.

7. **Peace Of Mind.** Because we monitor all our clients' networks 24/7/365, you never have to worry that a virus has spread, a hacker has broken in or a backup has failed to perform. We watch over your entire network, taking the management and hassle of maintaining it off your hands. This frees you to focus on your customers and running your business, not on your IT systems, security and backups.

To Schedule Your FREE Assessment,
please visit **www.rbsitsolutions.com** or call our office at 316-365-8701.