T. Daniels Consulting

The Small Business Guide
To IT Support Services And Fees

What You Should Expect To Pay For IT Support For Your Small 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 3 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 that you didn't anticipate.
- ✓ 20 revealing questions to ask your IT support firm BEFORE giving them access to your computer network, e-mail, and data.

Provided as an educational service by:
Timothy D. Ricketts, President
T. Daniels Consulting
107 S. Walnut, Fenton, MI 48430
810-629-0131

T. Daniels Consulting

From the Desk of: Timothy D. Ricketts
President, T. Daniels Consulting

Dear Colleague,

If you own or manage a business that is currently looking to outsource some or all of the 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**.

One of the most commons questions we get from new prospective clients calling our office is "What do you guys charge for your services?" Since this is such a common question — and a very important one to address — I decided to write this report for 3 reasons:

1. I wanted 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. I wanted to bring to light a few "industry secrets" about IT service contracts and SLAs (service level agreements) that almost no business leader thinks about, understands, or knows to ask about when evaluating IT service 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. I wanted 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, my purpose is to help you make the most informed decision possible so you end up working with someone who understands your unique business requirements, 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,

Timothy D. Ricketts, President

T. Daniels Consulting

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 to another, you need to understand the 3 predominant service models most of these companies fit within. Some companies offer a blend of all 3, while others are strict about offering only one service plan. The 3 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 removing a virus), or it may encompass a large project like a computer 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.

- **Preventative IT Services.** Traditionally referred to as Managed Services (MSP), it is a model where an IT services company takes the role of your "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, security, backup, and a host of other services to monitor and maintain the health, speed, performance, and security of your computer network.

  With cybercriminal activity on the rise, many business owners are taking advantage of a specialized form of an MSP which is the Managed Security Service Provider (MSSP). A MSSP has highly trained security engineers to provide outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services.

- **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 "Preventative IT Services" and "break-fix" models.

Therefore, let's dive into the pros and cons of these two options, and then their typical fee structures.

Preventative IT 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 the Preventative IT Services approach is, by far, the most cost-effective, smartest option for any business. 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 or expertise to implement (such as a network upgrade, installing a backup solution, 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 Today's Computer Networks

The fact of the matter is computer networks absolutely, positively need ongoing maintenance and monitoring to stay secure. Newer technology such as automated sign-ins, mobile devices such as iPads for client record access, and contactless payment all improve the customer experience but bring along with them a need for specialized support. Bottom line is the ever-increasing dependency we have on IT systems and the data they hold has given rise to very smart and sophisticated cybercrime organizations and who work around the clock to do one thing: compromise your network for illegal activities.

In most cases their intent is to access financial information and passwords to rob you (or your customers), create fake identities for credit card fraud, etc. In other cases, they may want to use your computer network to send illegal spam, host pirated software, spread viruses, etc. And some do it just for the "fun" of being able to make computer systems inoperable. These criminals work around the clock in teams, constantly finding and inventing new ways to get around your antivirus software and firewalls; that's why you have to remain ever vigilant against their attacks.

Of course, this doesn't even take into consideration other common "disasters" such as rogue employees, lost devices, hardware failures (which are the #1 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. We also can't forget the regulatory compliance that exists for any business that is hosting or touching credit card or financial information.

Preventing these problems and keeping your systems up and running (which is what Preventative IT Services is all about) is a LOT less expensive and damaging to your business 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 300 employees (sometimes more or less depending on the individual company's needs) to hire a full-time IT person (someone other than your office or finance manager pulling double duty as your "IT" person) because you can outsource this function of your business far cheaper and with a lot less work; but you DO want to hire a professional to perform basic maintenance just as you would hire an attorney to handle your legal matters or an accountant to prepare your taxes. **And if you truly understand the cost of your TIME and factor in employee productivity, the Preventative IT services model is considerably less expensive over time than the "break-fix" model.**

Why "Break-Fix" Works Entirely In the Consultant's 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 stabilize your computer network or to resolve problems quickly because they are getting paid by the hour; 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 consultant can take the liberty of assigning a junior (lower-paid) technician to work on your problem who may take two to three times as long to resolve an issue that a more senior (and more expensive) technician may have resolved 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 to 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 to Look For In a Preventative IT Services Agreement and What You Should 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.

Hourly Break-Fix Fees: Most IT services companies selling break-fix services charge between $100 to $200 plus per hour with charges equal to one to several hours minimum. In most cases, they will give you some type of discount 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 would suggest you demand the following:

- **A very detailed scope of work that specifies what "success" is.** Make sure you detail what your expectations are in performance, work flow, costs, security, access, etc. The more detailed you can be, the better. Detailing your expectations up front willgo a long way in avoiding miscommunications and additional fees later on to give youwhat you REALLY wanted.

- **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 consulting firm'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 consultant underestimating a job or for their inefficiencies. A true professional knows how to take into consideration those contingencies and bill accordingly.

Preventative IT Services: Most Preventative IT Services firms will quote you a MONTHLY fee based on the number of devices they need to maintain, back up and support.

If you hire an IT consultant and sign up for a Preventative 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
- Spam-filter installation and updates
- Spyware detection and removal
- Monitoring disk space on workstations and servers
- Monitoring hardware for signs of failure
- Optimizing systems for maximum speed
- Web-Protection and monitoring

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

- Hardware, such as new servers, PCs, laptops, etc.
- Software licenses
- On-site support for special projects (for example: upgrading/replacing hardware to upgrade from Windows 7 to Windows 10)

Warning! Gray areas of “all-inclusive” service contracts. In order to truly compare the “cost” of one Preventative IT Services contract to another, you need to make sure you fully understand what IS and ISN’T included AND the “SLA” or “service level agreement” you are signing up for. It’s VERY easy for one IT services provider to appear far less expensive than another UNTIL you look closely at what you are getting.

- The following are 20 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.

20 Questions You Should Ask Your Preventative IT Services Company Before Hiring Them To Support Your Network

General:

Q1: Do they answer their phones live or do you always have to leave a voice mail and wait for someone to call you back?
Any reputable IT company will answer their phones live from at least 8:00 am to 5:00 pm and give all clients an emergency after-hours number they may call if a problem arises, including weekends. Why? Because in today's business world, many people work outside normal hours and find it to be the most productive time they have. If they cannot access their computer network AND can't get hold of anyone to help them, it's incredibly frustrating.

Q2: Do they have a written, guaranteed response time to your calls?
They must guarantee to have a qualified technician working on your problem within a certain timeframe after you call. If they can't guarantee a certain response time, then be prepared to work on their timeframe and not yours when a problem does arise. A written guaranteed response time should be standard in every service agreement you sign.

Q3: Do they take the time to explain what they are doing and answer your questions in terms that you can understand (not geek-speak), or do they come across as arrogant and make you feel stupid for asking simple questions?
Good IT staff are trained to have the 'heart of a teacher' and will take the time to answer your questions and explain everything in simple terms.

Q4: Do they consistently (and proactively) offer new ways to improve your network's performance, or do they wait until you have a problem to make recommendations?
They should conduct **"Technology Business Review"** meetings with you 2-4 times per year to look for new ways to help improve your operations, lower costs, increase efficiencies and resolve any problems that may be arising. The goal of these meetings should be to help you be more profitable, efficient, and competitive.

Q5: If using cloud-based services like Microsoft 365 or Azure, is it clear that you own YOUR data?
One among the many benefits of leveraging the cadre of Microsoft cloud solutions is that they are governed by strict standards related to data ownership and privacy. You should confirm that you have 24/7 access to your data. Also, upon termination, of any hosting service, Microsoft will retain your data for 90 days which is more than sufficient to plan for and execute on a data migration plan. Your data should never be held hostage by an IT provider.

Q6: Do they provide detailed invoices that clearly explain the work performed?

Do you hate it when any vendor sends you a bill and you have no idea what work was done? This is completely unacceptable behavior. You should demand that your IT company provides you with detailed descriptions that show what work was done and when so you never have to guess what you are paying for.

Q7: Do they have adequate errors and omissions insurance as well as workers compensation insurance to protect YOU?

Here's something to consider: if THEY cause a problem with your network that causes you to be down for an unreasonable amount of time or to lose data, who's responsible? Here's another question to consider: if one of their technicians gets hurt at your business, who's paying? In this litigious society we live in, you better make darn sure whomever you hire is adequately insured with both errors and omissions insurance AND workers compensation – and don't be shy about asking to see their latest insurance policies!

True Story: A few years ago, Geek Squad was slapped with multi-million dollar lawsuits from customers for the bad behavior of their technicians. In some cases, their techs were accessing, copying, and distributing personal information they gained access to on customer's PCs and laptops brought in for repairs. In other cases, they lost a client's laptop (and subsequently all the data on it) and tried to cover it up. Bottom line make sure the company you are hiring has proper insurance to protect YOU.

<u>Maintenance of Your Network</u>:

Q8: Do they insist on remotely monitoring your network 24-7-365 to keep critical security settings, virus definitions and security patches up-to-date and PREVENT problems from turning into downtime, viruses, lost data, and other issues?

A remote network monitoring system watches over your network to constantly look for developing problems, security issues, and other problems so they can be addressed BEFORE they turn into bigger problems and network downtime.

Q9: Do they provide you with a weekly report that shows all the updates, security patches, and status of every machine on your network so you know for SURE your systems have been secured and updated?

Demand a detailed weekly report that shows an overall health score of your network and the updates to your antivirus, security settings, patches, and other important network checks (like hard drive space, backups, speed, and performance, etc.). Even if you don't read through the report every week, it's important to know that this is happening.

Q10: Is it standard procedure for them to provide you with written, network documentation detailing what software licenses you own, critical passwords, user information, hardware inventory, etc., or are they the only person with the "keys to the kingdom?"
Every business should have this in written and electronic form at no additional cost. Your IT company should also provide the information with the Technology Business Review mentioned earlier in this report and you should make sure your key people have this information and know how to use it, giving you complete control over your network.
Side Note: You should NEVER allow an IT person to have that much control over you and your business. If you get the sneaking suspicion that your current IT person is keeping this under their control as a means of job security, get rid of them. This is downright unethical and dangerous to your organization, so don't tolerate it!

Q11: Do they build internal knowledge around your specific network?
While most IT companies assign a "primary technician" to support your network, it is important that multiple team members that are trained on the nuances of your specific organization so that if someone goes on vacation or leaves, there will be no slowdown or disruption in the support of your network.

Q12: If they offer an "all-inclusive" support plan, is it TRULY all-inclusive, or are their "gotchas" hidden in the fine print?
The most advanced IT engineering firms today offer an "all-inclusive" or "all-you-can-eat" Preventative IT Services plan. These are actually a good thing because they'll save you a lot of money in the long run – HOWEVER, make sure you REALLY understand what is and isn't included. Some things to consider are:

- Is phone/e-mail help desk included, or extra?
- What about network upgrades, moves, or adding/removing users?
- Is hardware and/or software included?
- What about 3rd party software support such as your industry specific software?
- What are the costs/consequences of early cancellation?
- What if you're not happy with their services? Do they offer a money-back guarantee?
- If the hardware and software are included, what happens if you cancel thecontract?
- Are offsite backups included? To what degree?
- If you have a major disaster, is restoring your network included or extra?
- What about onsite support calls?
- Are home PCs used to access the company's network included or extra?

Backups and Disaster Recovery:

Q13: Do they INSIST on monitoring an offsite as well as an onsite backup, or are they letting you rely on outdated backup practices?
I would never allow any business these days to have onsite backup as their only form of backup because it leaves them incredibly vulnerable to ransomware as it is specifically designed to impact all aspects on an onsite network. We recommend a multi-layered approach using both on-site and off-site backup providing for both fast access on-site recovery and necessary redundancy in the event of a ransomware attack, fire, natural disaster, etc…

Q14: Do they INSIST on doing periodical test restores of your backups to make sure the data is not corrupt and could be restored in the event of a disaster?
They should perform minimally a quarterly "fire drill" and perform a test restore from backup 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. *I have gone into situations many times where the potential client has reached out to us because their existing IT provider cannot restore the data because the backup was not good*.

Q15: Do they insist on backing up your network BEFORE performing any type of project or upgrade?
This is a simple precaution in case a hardware failure or software glitch causes a major problem.

Q16: If you were to experience a major disaster, do they offer a written plan for how your data could be restored FAST and/or enable you to work from a remote location?
At a minimum, you should have a simple disaster recovery plan for your data and network. I would also encourage you to do a full disaster recovery plan for your business, but at a minimum, your computer network will be covered should something happen.

Technical Expertise and Support:

Q17: Are they able to support ALL aspects of your network?
A good example of this is a VoIP system. To avoid problems like dropped calls, echoing and to ensure a secure system to prevent hacks, your IT company needs to be specifically trained in VoIP. Most VOIP systems are cloud based which means your provider must also be an expert in cloud infrastructure as well.

Q18: Do their technicians maintain current vendor certifications and participate in on-going training – or are they learning on your dime?
Any technician working on your network should be up to date on the vendor certifications on your network. Our experience is that the vast majority of technicians out there these days are woefully undertrained. Also, look for a company that is "Certified". This ensures the company has multiple engineers with certifications and the company has additional access to live support and product resources that "non-Certified Partners" do not have. For example,

our company is a **<u>Microsoft Partner with Silver Cloud Platform and Silver Small and Midmarket Cloud Solutions certifications.</u>** This ranks us in the top 5% of all Microsoft Partners worldwide.

Q19: Do their technicians arrive on time and dress professionally?
Any technician working on your network is a part of your staff while they are there. Are they true professionals that you would be proud to have in your business? Do they dress professionally and show up on time? You have spent a lot of time and money building your business' image so it's important to make sure your IT vendors adhere to it!

Q20: Are they familiar with (and can they support) your unique line of business applications?
They should own the problems with all of your line of business applications. That doesn't necessarily mean that they can fix faulty software – but they SHOULD be the liaison between you and your vendor to resolve problems you are having and make sure these applications work smoothly for you. If they have experience working with your applications, they understand the nuances and can get your business back on track faster eliminating disruptions and enhancing a positive customer experience. For example, knowing a special setting in the browser your line of business software needs or how a printer setting can make a difference on how it works. I can give you multiple stories where companies had problems for months and longer before our company came on the seen because the previous IT vendor could not resolve a particular problem like the aforementioned. The company had just accepted that they had to live with it. Because we have experience and understand how your line of business applications work, we save you time and increase employee satisfaction, productivity and it results in greater customer satisfaction ratings, an important KPI you strive for.

A Final Word and Free Assessment Offer to Review Your Current Network Security Proficiency

I hope you have found this guide helpful in shedding some light on what to look for when hiring a professional firm for outsourced IT security and/or support. As I stated in the opening of this report, my purpose in providing this information was to help you make an informed decision and avoid getting burned by incompetent or unethical firms luring you in with cheap prices.

T. Daniels Consulting

If you are worried about whether or not your current backup and security processes are up to par, I'd like to offer you, for a limited time, a free Network Assessment and PEN Test (a value of $1,945) as a means for introducing our services to you. Our test will inform you of your **vulnerability and risk of an attack.** The PEN Test simulates a cyberattack to identify your security weaknesses. Why do we do this? Simply because I know how confusing and difficult it can be to find a good IT support company that is responsive, easy to work with and actually knows what they're doing.

Just about anyone can say they are an "IT expert." And since most business owners and managers don't have the ability to evaluate whether or not their IT is secure as it needs to be and running as efficiently as possible, we find that offering this assessment is a no-risk way of demonstrating how we can help you. At the very least, you'll get a free, qualified 3rd party evaluation of your network security, current backup, and voice communications profile and score which is extremely valuable even if you don't choose to hire us.

At no charge, one of our security specialists will …

- Audit your current data security and protection policy, including backup and restore procedures. Validate if ALL of your data is actually being backed up in a format that could quickly be restored. We often discover data on drives, laptops or PCs that is overlooked.

- Confirm if your current backup is working as expected, if you would be able to get your data and systems back up and running, and if so, would it be in a reasonable time frame (hours, days, weeks)? Many of the companies we've reviewed are shocked to learn the backup would NOT survive a ransomware attack.

- Assess if your IT systems and data are **truly secured** from hackers, cybercriminals, viruses, worms and even sabotage by rogue employees. If you're not getting weekly security updates, your systems probably aren't secure. You should also know that antivirus software and most firewalls are grossly inadequate against the sophisticated attacks happening in 2021.

- Evaluate your VoIP system. If you utilize VoIP, it is important to know that with today's technology, VoIP needs to be configured correctly to work seamlessly with your computer network. If not, it will not work right (static, dropped calls etc.) and is an open invitation for cybercriminals to hack your business.

- Run a Dark Web Assessment– **9 out of 10 times** we find compromised company credentials/passwords are available on the Dark Web**.** This alone is a reason to consider this limited offer.

Depending on what we discover, we'll either give you a clean bill of health or reveal gaps in your network that could prove disastrous. If it's appropriate, we'll provide you with an action plan for further securing your data.

How To Request Your Data Security Assessment and PEN Test?

To request your assessment, simply do one of the following:

1. Call our office at 810-629-0131
2. Send us an e-mail to: info@tdaniels.com
3. Go online to: https://www.tdaniels.com/security-assessment/

As soon as we receive your request, we'll call to schedule a convenient time for us to meet with you and to conduct the assessment. Again, you are under no obligation to do or buy anything. Even if you choose not to hire us for any additional work, you'll at least get a free, 3rd party evaluation of your company's data backup and security.