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

Lumen21

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 that you didn't anticipate.
- 21 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:

Eduardo Don Jr. President | ed.don@lumen21.com

Lumen21 Inc.

711 West Kimberly Ave., Suite 110 | Placentia, CA | 7148622171

Never Ask an IT Services Company, "What Do You Charge for Your Services?" Instead, **You Should Ask, "What Will I Get for My Money?"**

Dear Colleague,

If you are the Business Owner of a Small Business in Southern California that is currently looking to outsource some or all the IT support for your Healthcare Organization or any other organization, this report contains important information that will be extremely valuable to you as you search for a competent firm you can **trust**.

My name is Eduardo Don Jr., President of Lumen21 Inc. We've been providing IT services to businesses in the Southern California area for over 18 years now. You may not have heard of us before, but I'm sure you're familiar with one or more of the other Healthcare Providers who are clients of ours. A few of their comments are enclosed.

One of the most common questions we get from new perspective 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 three reasons:

1. I wanted an easy way to answer this question and educate all prospective clients who come to us in 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 services contracts and SLAs (service level agreements) that almost no Business Owners 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. I wanted to educate <<business owners>> 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 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,

Eduardo Don Jr.

President, Lumen21 Inc.

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:

1 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.

2 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.

3 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.

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 **midsize 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.

"An ounce of prevention is worth a pound of cure."

Benjamin Franklin

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. 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 hackers make millions of tax-free 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?

Size, need and cost are all factors that come into this decision. Certainly, for companies with under 50 employees to **hire a full-time IT person maybe challenging for a couple of reasons.**

First, 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 person. You need someone with help-desk expertise as well as a network engineer, a network administrator, an IT lead at times referred to as CIO (chief information officer or Director of IT), and a Security lead, also known as 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.

Often, 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. **We find that a strong case is also made for a blend of in-house and the outside IT Service as it allows you to provide the right blend of skill, coverage optimize cost.**

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 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 consultant 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. 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?

Hourly Break-Fix Fees

Most IT services companies selling break-fix services charge between $125.00per hour on the lower end to higher depending on the skill set required, 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 detail what your expectations are in 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 miscommunications and additional fees later to give you what 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.

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.**

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 Southern California, that fee is somewhere in the range of $250.00 per server to $300 per server, $150.00 per desktop and approximately $75.00 per smartphone or mobile device.

If you hire an IT consultant and sign up for a **managed IT services contract**, here are **some things that SHOULD be included** and intended frequency:

- 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
- 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 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.
- Setting up new equipment
- Software licenses
- Special projects

Warning! Beware the gray areas of "all-inclusive" service contracts. 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 "SLO" or "service level objectives" 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 21 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 deciding about who the right provider is for you, then make sure you get this IN WRITING.

20 Questions You Should Ask Your IT Services Company Or Consultant Before Hiring Them for IT Support

Customer Service

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

Our Answer: When a client has a problem, we "open a ticket" in our IT management system so we can properly assign, track, prioritize, document and resolve client 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, not yours. Trust me, this will become a giant inconvenience and thorn in your side. While a portal is a good option, it should never be your ONLY option for requesting support.

Also, make sure they HAVE a reliable system in place to keep track of client "tickets" and requests. If they don't, I can practically guarantee 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, chat, for example.

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 8:00 a.m. to 5:00 p.m. every weekday. But many CEOs and executives work outside normal "9 to 5" hours and need IT support both nights and weekends. Not only can you reach our after-hours support at any time and any day, but we also CONSISTENTLY respond in 5-10 minutes or less to communicate with you regarding the situation. The issue is critical to you and needs attention sooner than later and that triggers other activity in talking with our support team to help resolve the issue in question at that time. If your issue can wait it will be assigned accordingly first thing in the morning based on the data that was collected so it can be acted upon then.

Q3 Will I be given a dedicated account manager?

Our Answer: Smaller firms may not offer this due to staff limitations, and the owner may tell you they will personally manage your account. While that sounds like great customer service, the owner is usually so busy that you'll only be given reactive support instead of proactive account management. Rest assured, from initial call to final resolution, you will work with our SAME dedicated account manager who will know you, your business, and your goals.

Q4 Do you have a feedback system in place for your clients to provide "thumbs up" or "thumbs down" ratings on your service? If so, can I see those reports?

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

IT Maintenance (Managed Services)

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 IT 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 system watches over your network to constantly look for developing problems, security issues and other problems 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.

Other things to inquire about are:

- 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 must 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.)

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. This can be frustrating and lead to the same problems cropping up again, longer resolution time.

Q8 How many engineers do you have on staff?

Our Answer: Be careful about hiring small, one-person IT firms that only have one or two techs or that outsource this critical role. 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 in case one is unable to work.

ALSO: Ask how they will document fixes, changes, credentials for you organization so 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 computer network.

Q9 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. Every IT company should provide this to you in both written (paper) and electronic form at no additional cost and update it on a quarterly basis.

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 because they don't waste time fumbling their way around your network trying to find things and uncover accounts, hardware, software licenses, etc. Third, if you had to restore your network after a disaster, you'd have the blueprint to quickly put things back in place as they were.

Finally, and most important, if you ever need to switch IT providers, your replacement company will be able to take over quickly because the network has been documented properly.

All our clients receive this in written and electronic form at no additional cost. We also provide an update on this material as it happens with the tools we use.

Side note: You should NEVER allow an IT person to have that much control over you and your company that you don't have access to if needed. It's your data. This is downright unethical and dangerous to your organization, so don't tolerate it!

Q10 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 (sometimes more often) 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. We also make recommendations for new equipment and upgrade you'll be needing soon or sometime soon. Our quarterly meetings with you are C-level discussions (not geek-fests) 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, lower costs, increase efficiencies, and ensure your organizational productivity stays high. This is also your opportunity to give us feedback on how we're doing and discuss upcoming projects.

Q11 If I need or want to cancel my service with you, how does this happen and how do you offboard us?

Our Answer: If a client is leaving us, we will collaborate with the entity that will be involved going forward in providing all needed documentation related to your account. Our agreement includes notice period for renewal of the contract period allowing you to plan on how to proceed once the agreement comes to an end, in our case it is 90 days' notice. Lots goes into this issue of cancelation often time there are pricing considerations that may have been provided, rates, etc. Just be clear on what a given contract calls for so there are no surprises.

Q12 What cyber security certifications do you and your in-house team have?

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 and tools capabilities. Lack of this capability is a red flag. Some business owners won't invest in training and give this excuse: "What if I spend all this money on training my employees and then they leave us for another job?" Our response is, "What if you DON'T train them and they stay?" Having said that our SOC service is made up of folks that have some of these certifications; Security+, Pentest+, SANS/GIAC GSEC, SANS/GIAC GCIF, SANS/GIAC GCIH, SANS/GIAC GIME to name a few.

Q13 How do you lock down our employees' PCs and devices to ensure they're not compromising 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
- Network change detection

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.

Q14 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 show you a copy of our policy.

Q15 Who audits YOUR company's cyber security protocols and when was the last time they conducted an audit?

Our Answer: Nobody should proofread their own work, and every professional IT consulting firm will have an independent third party reviewing and evaluating their company for airtight cyber security practices.

There are many companies that offer this service, so whoever they use can vary (there's several good ones out there). If they don't have a professional cyber security auditing firm doing this for them on at least a quarterly basis, or if they tell you they get their peers to audit them, DO NOT hire them.

You can be confident in the effectiveness of our cyber security because we are audited by Galactic, Withum for our SOC2 Type Yearly Certification, and we have just recently been audited.

Q16 Do you have a SOC, and do you run it in-house or outsource it? If outsourced, what company do you use?

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 (this is the minority of outsourced IT firms out there). Others cannot and outsource it because they know their limitations (not entirely a bad thing).

But the key thing to look for is that they have one. Less experienced IT consultants 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 host sensitive data (financial information, medical records, credit cards, etc.) and fall under regulatory compliance for data protection.

Rest assured, we do provide proactive security monitoring for our clients to better prevent a network violation or data breach via our SOC and its service offerings.

Q17 Can you provide a timeline of how long it will take 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 that most business owners aren't aware of. The first is "fail over" and the other is "fail back." For example, if you get a flat tire, you will 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 – be it a ransomware attack or natural disaster – you want to make sure you have a fail-over 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 to your on-premises network, and that's a process that could take days or even weeks. If the backups aren't done correctly, you might not be able to get it back at all.

So, one of the key areas you want to discuss with your next IT consultant or firm 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 network and data with a timeline.

Currently, 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 immediately.

We understand how important your data is and how getting your team up and running quickly is essential to your business success. This area should be discussed and be part of the agreement of what you may need or expect and what must be in place and regularly tested as part of the agreement. Keep in mind these types of things are important and, in some cases, carry added cost but they're worth spending. Therefore, in the event of any disaster, you can confidently get your network back up and running as quickly at a time as possible. And needed.

Q18 Do you INSIST on doing periodic test restores of my backups to make sure the data is not corrupt and could be restored in the event of a disaster?

Our Answer: A great IT consultant will place eyes on your backup systems every single day to ensure that backups are 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.

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.

Q19 If I were to experience a location disaster, pandemic shutdown or other disaster that prevented me from being in the office, how would you enable me and my employees to work from a remote location?

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.

We could experience a terrorist attack, civil unrest or riots that could shut down entire cities and streets, making it physically impossible to get into a building. Who knows what could be coming down the pike? Hopefully NONE of this will happen, but sadly it could.

Q20 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. (Sadly, it's more common than you think.) A good 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 client onboarding process and documentation. I think you'll be impressed, particularly with some of the discovery tools and processes we use to best assess your situation and where there may be gaps if any. We do this based on comparisons to industry frameworks for security and compliance.

Other Things to Notice and Look For

Are they good at answering your questions in terms you can understand and not in arrogant, 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.

Do they and their technicians present themselves as true professionals when they are in your office? Presentable and show up on time?

How you do anything is how you do everything, so if they cannot show up on time for appointments, are sloppy with paperwork, show up unprepared, forget your requests and seem disorganized in the meeting, how can you expect them to be 100% on point with your IT? You can't. Look for someone else.

Do they have expertise in helping clients like you?

Do they understand how your business operates the line-of-business applications you depend on? Are they familiar with how you communicate, get paid, service your clients or patients and run your business? We have several Healthcare Providers clients and several in regulated high value data organizations. The reason we work well with them is because We are a healthcare experience organization that specializes in assisting healthcare companies with their cyber security and IT regulatory compliance for over 18 years.

A Final Word and Free Offer to Engage With Us

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

The next step is simple: **call my office at 714-862-2171 and reference this letter to schedule a brief 10- to 15-minute initial consultation.**

On this call we can discuss your unique situation and any concerns you have and, of course, answer any questions you have about us. If you feel comfortable moving ahead, we'll schedule a convenient time to conduct our assessment.

This Assessment can be conducted 100% remote with or without your current IT company or department knowing (we can give you the full details on our initial consultation call). At the end of the Assessment, you'll know:

- Where you are overpaying (or getting underserved) for the services and support you are currently getting from your current IT company or team.
- Whether or not your systems and data are truly secured from hackers and ransomware, and where you are partially or totally exposed.
- If your data is being backed up in a manner that would allow you to recover quickly in the event of an emergency or ransomware attack.
- Where you are unknowingly violating data breach or compliance regulations.
- How you could lower the overall costs of IT while improving communication, security, and performance, as well as the productivity of your employees.

Fresh eyes see things that others cannot – so, at a minimum, our free Assessment is a completely cost- and risk-free way to get a credible third-party validation of the security, stability, and efficiency of your IT systems.

To Schedule Your Initial Phone Consultation Call: 714-862-2171

See What Other Business Owners Are Saying

"Since partnering with them, we have seen improved uptime, faster resolution times, and greater overall stability."

A Reliable IT Partner We Can Truly Count On
"The biggest benefit of working with Lumen21 has been having a reliable, consistent IT partner we can count on. Their support allows us to stay focused on strategic initiatives, knowing our infrastructure and day-to-day needs are in capable hands. Since partnering with them, we've seen improved uptime, faster resolution times, and greater overall stability.
What sets Lumen21 apart is their responsiveness and technical depth. Even with complex cloud-related issues, their escalation paths are clear, and resolution is always prioritized. The combination of strong customer care and deep technical expertise is truly exceptional.
If someone were on the fence, I'd tell them Lumen21 is a dependable, committed partner. They listen, adapt, and deliver with a customer-first mindset. When it matters most, you won't be left in the dark."

Greg Robinson, CTO
Titan Health Solution

"Their Service just keeps getting better."

"Working with Lumen21 has been a flexible, evolving experience -- their service just keeps getting better. If you want a team that truly cares about doing things right and keeping you happy, Lumen21 is it."

Wendy Kim, Chief Financial Officer
BioVie Pharma

"The biggest benefit of working with Lumen21 has been the added security against cyber threats."

"The biggest benefit of working with Lumen21 has been the added security against cyber threats. Their knowledgeable technicians are quick to step in during the workweek whenever an issue comes up, and they resolve problems in a reasonable timeframe. What I value most is how Lumen21 has been a trusted partner for years, always evolving with the ever-changing world of technology. I'd recommend them to any business looking for both expertise and reliability."

Melissa Scott, COO
Golf Energy Bar

The Top Reasons Why You'll Want to Outsource Your IT Support To Us

1. **We Respond Within 5 Minutes or Less.** We know you're busy and 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 around 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. By keeping that to themselves, IT companies hold their client's "hostage" to scare them away from hiring someone else. This is both unethical and unprofessional. 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. We watch over your entire network, taking the management and hassle of maintaining it off hand. This frees you to focus on your customers and running your business, not on your IT systems, security and backups.

Lumen21

Lumen21, Inc. | sales@lumen21.com | www.lumen21.com

Lumen21 specializes in IT security and compliance. It offers a range of solutions and services for organizations that enable them to leverage the latest technologies and meet their regulatory and security responsibilities. Lumen21 facilitates the compliance process and enables companies to measure, monitor, report, and improve it. Lumen21 offers its O365+ Compliance Service, which leverages Microsoft products such as O365 Enterprise, Enterprise Mobility, Device Management, and Azure Storage, implementing the necessary controls, configuring and monitoring them to meet regulatory standards. Therefore, at Lumen21, we believe that regulatory compliance is not a simple declaration, but a continuous, verified, and certified process. You can learn more about our solutions that help you comply with regulations in your IT operations and improve your security. To do so, please contact us at sales@lumen21.com or visit us at www.lumen21.com