DLC Technology

IT Buyers Guide
What Every Business Owner MUST Know About IT Support Services and Fees

What You Should Expect To Pay For IT Support And How To Get Exactly What You Need

DLC Technology

The Southern New Jersey CEOs Guide To IT Support And Services

What You Should Expect To Pay For IT Support For Your organization

(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.
- ✓ 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:
Darren Crane President
DLC Technology Solutions, Inc.
777 Route 70 E, Suite G-104
Marlton, NJ
856-983-2001,
dlctechnology.com, dcrane@dlctechnology.com

Never Ask An IT Services Company, "What Do You Charge For Your Services?" Instead You Should Ask,

"What Will I *Get* For My *Money*?"

From The Desk Of: Darren Crane
President, DLC Technology Solutions, Inc.

Dear Colleague,

If you are the CEO of a organization in Southern New Jersey that is currently looking to outsource some or all of the IT support for your healthcare 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 Darren Crane, President of DLC Technology Solutions, Inc. We've been providing IT services to businesses in the Southern New Jersey area for over 34 years now. If fact, my business partner and I have been in healthcare IT our entire career – and we have the grey hairs to prove it. You may not have heard of us before, but I'm sure you're familiar with one or more of the other healthcare organizations who are clients of ours. A few of their comments are enclosed.

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 three 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 services contracts and SLAs (service level agreements) that almost no CEOs 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,
Darren Crane

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. This service also has the unique advantage of typically including technology leadership at the top-tier of your company to help ensure alignment with your business needs.

- **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 healthcare organization.

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 two very important, fundamental reasons:

1. you'll ultimately end up paying for a pound of "cure" for problems that could have easily been avoided with an "ounce" of prevention.
2. The burden of guiding your technology in terms of business alignment, cybersecurity compliance, future budget planning, preventative maintenance and more remains on your plate as the business owner. Likely, you already have enough to do and are not a full time technology and compliance expert.

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, well-run and richly funded operations employing *literal armies* 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. Risks even extend to other exposures, as most insurance companies are now requiring various cyber protections, written information security policies and procedures, and proof they are implement via an annual third-party audit.

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).

Hint: IT and cybersecurity companies are aware that some of you didn't have the right protections in place, so when you call them after a bad event happens – you guessed it – their rates are much, much higher. Emergency IT services after a cyber event are called "Incident Response Services" and typically start around $400 per hour with some mandatory minimums.

Should You Just Hire A Full-Time IT Manager?

In most cases, it is not cost-effective for companies with under 50 or even 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 person. 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.

I know you've heard about current unemployment rates, and you're tempted to believe there are candidates out there; but let me tell you as someone who's been hiring technical staff since the mid 1990's – there is essentially no unemployment for qualified and quality IT or cybersecurity staff!

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. An internal IT department typically doesn't make sense until you have beyond 100 employees OR you have unique circumstances and need specialized skills, a developer, etc., but not for day-to-day IT support, management and maintenance.

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. 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). You can try questioning every invoice but do you really have the time for all that management?

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

Not to mention – who is doing the future planning? Nothing like thinking there is a quick fix only to find out you need an emergency server replacement for five figures.

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.

Hourly Break-Fix Fees: Most competent IT services companies selling break-fix services charge between $150.00-$275.00 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.

Red flag: Being too cheap

There are IT service companies out there charging far lower rates than this. They claim they have lower overhead and can make the pricing possible. In reality, they are likely understaffed (sometimes only 1 or 2 people!), lacking insurance and proper back-end systems to secure and manage your data. If the person gets sick or has an urgent disaster at two customers at the same time you may be left in the cold when you need them the most! See our 21 questions later in this document for details on how to spot one of these companies.

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 on 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.

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 New Jersey, that fee is somewhere in the range of $250.00 - $550.00 per server, $100.00 - $300.00 per desktop and approximately $10.00 - $30.00 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 (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
- Monitoring workstations and servers for signs of failure
- Optimizing systems for maximum speed
- Documentation of your network, software licenses, credentials, etc.
- Technology Management and Planning services (sometimes called “Virtual CIO”)

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!

- Advanced Cybersecurity services and solutions such as vulnerability management, penetration testing, managed detection and response by a security operations center (SOC), etc.
- Compliance Consulting for compliances such as HIPAA, ISO27001, SOC2, etc.
- Hardware, such as new servers, PCs, laptops, etc.
- Software licenses
- Special projects

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" 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 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 making a decision about who the right provider is for you, then make sure you get this IN WRITING.

21 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, 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: Most good IT companies will answer their support hotline telephones LIVE (not voice mail or phone trees) from 8:30 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 any time and any day, we GUARANTEE a response time of 60 minutes or less for problems marked "emergency," such as a network being down or a critical problem that is significantly impacting your ability to work. Need faster response? Based on your needs our response times are customizable.

Q3: Do you have a written, guaranteed response time for working on resolving your 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. Our written, guaranteed response time is 60 minutes or less. 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 times.

Q4: 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.

Q5: 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. 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 (Managed Services):

Q6: 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.

Q7: 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.

But here's a question you need to ask: If you were hit with a costly ransomware attack, would the recovery be EXTRA or included in your contract? Recovering from a cyber-attack could take HOURS of high-level IT expertise. Who is going to eat that bill? Be sure you're clear on this before you sign, because surprising you with a big, fat bill is totally and completely unacceptable.

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 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 and covers the content listed above.

Q8: 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 dedicated group of technicians to your account who will get to know you and your company, as well as your preferences and history. Beyond help desk, each of our managed services customers is assigned a dedicated Virtual CIO and dedicated Solutions Engineer ensuring laser-like focus on your needs. Our support team is all locally based, and never outsourced. When you work with our local help desk, they'll be more capable of successfully resolving your IT issues and handling things the way you want.

Q9: How many technicians and engineers do you have on staff? Who performs what role?

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 and engineers on staff to cover in case one is unable to work.

When providing managed IT services, it is about much more than just help desk (in other words, getting support when you need it). It also includes planning, design, complex implementations and integrations, budgeting, and education. This requires more than a help desk team, but also an engineering or architecture team, and a leadership or Virtual CIO team. Ask to see their internal org chart or at least understand how they staff each of these critical functions.

Also ask about experience level of the person answering the phone. Do they have “Level 1 Techs” that answer the phone with minimal experience? If so, what types of things can they resolve on that initial call,

and what needs to get escalated? We employ NO Level 1 techs, and instead require at least 7 years IT experience to answer the phone. The result is a very capable human at the other end of the phone call ready to solve your issue.

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.

Q10: 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 upon request in both written (paper) and electronic form at no additional cost and update it on a continual 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. We recommend keeping this data in a safe or other secure location so you have it when you need it.

Note: The principle of least privilege (a cyber security thing) does not allow you to be the 'admin' level user on a day to day basis (which if you are doing your own IT today – you may be!). Therefore we restrict all users from being an admin and create unique, specialized admin accounts at the start. However the credentials to the admin level user accounts are documented and included in the documentation set for your use in any 'break glass' scenarios.

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 perform a continual update on this material and can make available fresh copies of the information at any time upon request, giving you complete control over your network at all times.

Note: You should NEVER allow an IT person to have that much control over you and your company. 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 (and we can help to make sure you don't suffer ANY ill effects). This is

downright unethical and dangerous to your organization, so don't tolerate it! [We've helped rescue customers from situations like this in the past. Let us know and we can help!]

Q11: 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 upgrades you'll be needing soon or sometime in the near future. 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.

Depending on your needs and business planning cycle, we can also include multi-year technology budget forecasts that include all of your technology expenses – not just those purchased through us!

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.

Q12: If I need or want to cancel my service with you, how does this happen and how do you offboard us?

Our Answer: Make sure you carefully review the cancellation clause in your agreement. Many IT firms hold their clients hostage with long-term contracts that contain hefty cancellation penalties and will even sue you if you refuse to pay. Also be sure to ask about offboarding or transitioning to another IT provider at the end of the contract. Typically these are paid projects and are not included in your monthly fees.

We would never "force" a client to stay with us if they are truly unhappy. Therefore, after a period of trying to 'make it right' and resolve whatever issues may exist, we will make it easy to cancel your contract with us, with zero contention or artificial fines.

Regardless of the reasons why, when it comes time to offboard a customer we work in a collaborative manner with your new IT provider to ensure they have everything they need to ensure your needs are addressed.

DLC Technology

Cyber Security:

Q13: What cyber security tools and services are included in your offering, and how did you determine these were the most appropriate for your customers?

When building a cybersecurity focused managed IT offering there are many components involved. I like to call them the 'layers of the onion' but most IT providers call them "the stack." For each of these layers there are dozens of vendors that offer a solution. The challenge for all of us – given the fact that cybersecurity is so critically important these days – is which vendor and solution is the best? In terms of creating a managed offering it is also critical that all the various layers are connected in some way. They must integrate to each other and all flow back to a centralized place – ideally to a Security Operations Center (SOC) – for correlation, analysis and (if required) response.

Ask the IT provider to outline all the components and vendors in their "stack" and ask them to explain how they relate to each other. For example, if a questionable activity is happening on a desktop, and another is happening in your Office365, how are they viewed simultaneously to understand if they are related and perhaps an indication of something really bad happening or about to happen?

Our Answer: Building our comprehensive offering is a constant task of evaluation and re-evaluation of vendors and products. This is because firms are bought and sold, new products emerge, and new threats emerge. It is a constantly changing soup of problems and solutions. We review all the components inside our managed cybersecurity offering no less than every 90 days. When new vendors or solutions are available we vet them internally, scrutinize their integration into the rest of the 'stack' and evaluate the cost/pricing dynamic. We are always looking for better solutions that not only provide enhanced protections and compliance, but hopefully more cost-effective solutions for our customers.

Internally we have created a dedicated team (called our Continual Process Improvement (CPI) team) which analyzes and determines the various vendors and products used in our offerings. Once the product testing, vetting, financial analysis and integration testing is completed it is our CPI team that renders the final decision on if this is incorporated into our offering.

Because of this constant evolution, our managed offerings are versioned with the year and quarter that they were released. We allow no customer to stay on a version that is more than 2 years old to ensure the most modern of cybersecurity protections.

Q14: 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
- Managed Detection and Response (called MDR) backed by a SOC (Security Operations Center)
- Removal of "Admin" rights from all users (no user needs this, although they think they do!)
- Zero trust solutions

Because a combination of these lockdown strategies is essential to protecting your network and data, we employ ALL of these for our clients depending on the situation and need. Effective cyber security should never be composed of a single solution, but a series of solutions all working in harmony.

Q15: 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 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!

If you get hit with ransomware due to their negligence, someone has to pay for your lost sales, the recovery costs and the interruption to your business operations. If they don't have insurance to cover YOUR losses of business interruption, they might not be able to pay, and you'll have to end up suing them to cover your costs. If sensitive client data is compromised, who's responsible for paying the fines that you might incur and the lawsuits that could happen? No one is perfect, which is why you need them to carry adequate insurance.

True story: A few years ago, a company that shall not be named was slapped with several multimillion-dollar lawsuits from customers for bad behavior by their technicians. In some cases, their techs were accessing, copying, and distributing personal information they gained access to on customers' 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 IT firm you are hiring has proper insurance to protect YOU.

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.

Q16: Who assesses YOUR company's cyber security protocols and when was the last time they conducted an review?

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 cyber security practices.

There are many companies that offer this service, so who they use can vary (there's a number of good ones out there). If they don't have a professional cyber security firm doing this for them on at least a annual basis, or if they tell you they get their peers to audit them, DO NOT hire them. That shows they are not taking cyber security seriously.

You can be confident in the effectiveness of our internal cybersecurity for the following reasons:

- We are a HIPAA Business Associate to many organizations and therefore abide by HIPAA internally. This includes the HIPAA required annual risk assessment (performed by a third-party).

- We have a third-party perform penetration testing on our systems no less than annually, and vulnerability scanning no less than monthly.

Q17: 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 of limitations or an intentional desire to not perform those services internally. (This is 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 have specialized Outsourced SOC partner to provide proactive security monitoring for our clients to better prevent a network violation or data breach.

Backups And Disaster Recovery:

Q18: 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 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 – 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-premise 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.

In this day and age, 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 almost immediately. However these types of disaster recovery solutions come with a cost.

Some providers will give you multiple options – where longer restoration or failover times come at a lower monthly cost – and this is OK. However you must carefully weigh the options and understand the impact of a 4 hour failover vs a 48 hour failover to your business.

We understand how important your data is and how getting your team up and running quickly is essential to your business success. Therefore, with our backup/disaster recovery solution in the event of any disaster, we can confidently get your systems back up and available in 4 hours or less.

Q19: 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 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.

TIP: As your IT provider about Ransomware Protection for your backup data. Is the data stored in a location or in a way that it is immune from a ransomware outbreak? This is also called having an 'immutable copy' of your data. Our solution is designed to be isolated from your network in a way that makes it immune from ransomware on your network along with an additional immutable cloud copy.

Q20: 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.

That's why you want to ask your prospective IT consultant how quickly they were able to get their clients working remote (and securely) when Covid shut everything down. Ask to talk to a few of their clients about how the process went. We implemented remote worker scenarios at scale immediately for our customers during early Covid. With access to our own world-class data center as well as leveraging Microsoft Azure cloud we were able to achieve and implement remote worker solutions within days.

Q21: 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 new client onboarding process and documentation. I think you'll be impressed. We take our time to both onboard and assess your technology environment during the initial days of the agreement. You will see a lot of us as we get to know you, your company, and your employees and become part of your team.

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, engineers, architects, and consultants are trained to take time to answer your questions and explain everything in relatable terms.

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

If you'd be embarrassed if YOUR clients saw your IT consultant 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 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.

Our technicians 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. We have a written dress code for client visits which we are happy to show you. All our employees wear a photo ID badge so you are comfortable the person is genuine and authorized.

Do they have expertise in helping clients similar to 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 many healthcare organization clients. The reason we work well with them is because we are veteran healthcare IT experts with over 20 years of expertise in designing, implementing and managing the complex integration and compliance needs of various HIPAA covered entities and business associates.

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 manage your IT. 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 856-552-3535 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 proprietary multi-point 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 *actually* being backed up in a manner that would allow you to recover it 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:

www.dlctechnology.com/initial-consultation/

Call me direct: 856-552-3535

With appreciation,

Darren Crane
President DLC Technology Solutions, Inc.
Office: 856-983-2001 Direct: 856-552-3535 Web: dlctechnology.com

See What Other Business Owners Are Saying:

Essential IT Partner Ensuring Compliance and Efficiency in Healthcare

"DLC's understanding of our operations and culture allows them to implement projects tailored to our needs, helping us deliver exceptional healthcare services. We value DLC's critical services and their commitment to staying informed about industry updates and risk factors. DLC has been an invaluable ally, consistently delivering efficient, cost-effective, and compliant services. Their leadership and staff are always available for discussions and addressing concerns, providing instrumental support for our success."

- Geraldine Martinez
Chief Executive Officer
Project H.O.P.E.

Reliable, Compliant IT Services that Enhance Performance and Security

Since moving to DLC for our IT services, the single biggest benefit has been reliability. Everything always works. DLC's knowledge of the medical space where we operate ensures we stay ahead of the competition in terms of system integration while remaining compliant and protected from bad actors and malware. The services they provide not only ensure we don't lose valuable work time for our employees but also assist in identifying and implementing efficiencies in performance.

-Bill Lobosco
President
Sunmed Medical Systems

DLC Technology

The Top Reasons Why You'll Want To Outsource Your IT Support and Management To Us:

1. **We have grey (or no) hair**. [Ok, I added this to see if anyone got this far in reading this whitepaper!] **But seriously, all of our staff are seasoned veterans of IT from various industries. We hire NO "Level 1" staff. We require our junior most team members to have at least 7 years IT experience. While this may cost a little more, the value gained for you, the customer, is palpable.**

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. **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.**

4. **We stand behind our work and our products, and we represent you. We spend a lot of internal time vetting products, vendors and solutions. Our job is to bring those solutions to bear to address your business needs and help you achieve enhanced performance. Despite our efforts sometimes the product doesn't work as advertised, a vendor goes out of business, or other unforeseen issue occurs. In those cases we represent you and your interests, and work tirelessly until the situation is made right.**

5. **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 clients "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.**

6. **Peace Of Mind. Because we monitor all of 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.**