1619 Bypass Rd. STE 122
Winchester, KY 40391
Phone: 859-200-0428
Email: info@isafecomplete.com

The Central Kentucky Healthcare Owners Guide To IT Support Services & HIPAA Compliance

What You Should Expect To Pay For IT Support For Your Healthcare 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:
Bob Stamper
iSAFE Complete Managed Services
Richmond, KY 40475
859-200-0428
bob@isafecomplete.com

1619 Bypass Rd. STE 122
Winchester, KY 40391
Phone: 859-200-0428
Email: info@isafecomplete.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: Bob Stamper
Owner, iSAFE Complete Managed Services

If you are the owner or manager of a healthcare organization in Central Kentucky that is currently looking to outsource some or all of the IT support for your practice, 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 Bob Stamper, Owner of iSAFE Complete Managed Services and author of Small Business Technology Simplified. We've been providing IT services to businesses in the Lexington, KY area for over 20 years now. You may not have heard of us before, but I'm sure you're familiar with one or more of the other local businesses that 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 owners or managers think 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, Bob Stamper.

1619 Bypass Rd. STE 122
Winchester, KY 40391
Phone: 859-200-0428
Email: info@isafecomplete.com

About The Author

Bob Stamper started iSAFE (formerly iSTAM Computer Services) in 1998 shortly after graduating from EKU. iSAFE became well known in central Kentucky as the place for computer repair, upgrades and business support services.

By 2012 the home user computer repair market was almost completely dissolved by low cost new computers distributed by major retailers such as Wal-mart and Best Buy. In response to the industry shift, Bob led the business forward toward business support and cybersecurity services.

Bob went on to write a book entitled Small Business Technology Simplified to address many of the concerns and issues that small businesses face with technology and answer many questions that he had been asked over the years.

In 2020 he developed solutions to accommodate work at home and hybrid work environments for businesses struggling to stay productive and secure during the COVID lockdowns. In spite of a 600% spike in cybersecurity attacks in 2020 not a single iSAFE client experienced a breach or malware infection.

As Zoom and other remote work and communication platforms fell under attack, local news outlets such as ABC (Channel 36) and KY Media turned to Bob for expert advice on how to keep their network and meetings secure.

iSAFE now focuses on helping healthcare companies achieve HIPAA compliance while maintaining productivity and efficiency utilizing technology solutions.

Mission and Values

Our mission is to help people use technology to accomplish their goals while protecting their information and hardware through education, proactive support, and software solutions. Our core values are honesty, integrity, relevance, excellence, and relationships.

iSAFE
We Make Technology Work For You

1619 Bypass Rd. STE 122
Winchester, KY 40391
Phone: 859-200-0428
Email: info@isafecomplete.com

Comparing Apples To Apples: The Predominant IT Service Models Explained

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

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

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

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

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

1619 Bypass Rd. STE 122
Winchester, KY 40391
Phone: 859-200-0428
Email: info@isafecomplete.com

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 provider or organization that falls under the HIPAA security rule.

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 at a discounted rate. 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.

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.

1619 Bypass Rd. STE 122
Winchester, KY 40391
Phone: 859-200-0428
Email: info@isafecomplete.com

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

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

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

Should You Just Hire A Full-Time IT Manager?

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

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

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

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

More often than not, the hard and soft costs of building an internal IT department for general IT support just don't provide the best return on investment for the average small to midsize business. An internal IT department typically doesn't make sense until you have closer to 100

1619 Bypass Rd. STE 122
Winchester, KY 40391
Phone: 859-200-0428
Email: info@isafecomplete.com

employees OR you have unique circumstances and need specialized skills, a developer, etc., but not for day-to-day IT support 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).

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

What Should You Expect To Pay?

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

Hourly Break-Fix Fees: Most IT services companies selling break-fix services charge between $100 and $250 per hour with a one-hour minimum. In most cases, they will give you a

1619 Bypass Rd. STE 122
Winchester, KY 40391
Phone: 859-200-0428
Email: info@isafecomplete.com

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 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 or users they need to maintain, back up and support. In Lexington KY, that fee is somewhere in the range of $225 to $325 per server, $70 to $120 per desktop or between $100 and $250 per user if they are using a per using pricing like iSAFE.

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):

- EDR Antivirus Protection (Enhanced Detection and Response)
- Monitoring workstations and servers for signs of failure
- Web Filtering
- Patch Management
- Daily Backups, Management & Remediation
- Monthly Reporting
- Documentation and Compliance Support
- Optimizing systems for maximum speed
- Lifecycle Management for hardware and software
- End User Training and phishing simulation
- End User Support

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!

1619 Bypass Rd. STE 122
Winchester, KY 40391
Phone: 859-200-0428
Email: info@isafecomplete.com

- Hardware, such as new servers, PCs, laptops, etc.
- Software licenses
- Special projects
- On-Site Support

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 only allow you to submit a ticket through their portal 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 great 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 they answer their phones live or do you always have to leave a voice mail and wait for someone to call you back?

1619 Bypass Rd. STE 122
Winchester, KY 40391
Phone: 859-200-0428
Email: info@isafecomplete.com

Our Answer: We do our best to answer every call live from 9:00 a.m. to 5:00 p.m. and we have an emergency after-hours call system that will email and text our on-call technician. Why? Because many of the CEOs and executives we support work outside normal hours and find it the most productive time they have. If they cannot access their computer network AND can't get hold of anyone to help them, it's incredibly frustrating.

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

Our Answer: We guarantee to have a technician working on a problem within 2 hours or less of your call and ticket submission for business emergencies. This is written into every service agreement we give to our clients because it's standard procedure.

Q4: Do they provide detailed invoices that clearly explain what you are paying for?

Our Answer: All of our invoices include the ticket number and the explanation of work completed. Our managed services invoices are all available from your account one our web site. You can also access and download any of your invoices from there any time as well as review any charges, add or cancel subscriptions, etc.

IT Maintenance (Managed Services):

Q5: Do they consistently (and proactively) offer new ways to improve your network's performance, or do they wait until you have a problem to make recommendations?

Our Answer: We conduct quarterly review meetings with our clients to look for new ways to help improve their operations, lower costs, increase efficiencies and resolve any problems that may be arising. Our goal with these meetings is to help our clients be more profitable, efficient and competitive.

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.

1619 Bypass Rd. STE 122
Winchester, KY 40391
Phone: 859-200-0428
Email: info@isafecomplete.com

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 unlimited support for line of business applications, adding new users (up to 5 per month), adding new computers (up to 5 per month), on-site support, remote support, vendor management (we call the ISP for you) and more.

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

Our Answer: Yes, 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.

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

Our Answer: Every month we send you a detailed Executive Summary report that shows an overall health score of their network and the updates to their antivirus, security settings, patches and other important network checks (like hard-drive space, backups, speed and performance, etc.).

1619 Bypass Rd. STE 122
Winchester, KY 40391
Phone: 859-200-0428
Email: info@isafecomplete.com

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 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 perform a quarterly update on this material and make sure certain key people from your organization have this information and know how to use it, giving you complete control over your network.

Side note: You should NEVER allow an IT person to have that much control over you and your 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!

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.

1619 Bypass Rd. STE 122
Winchester, KY 40391
Phone: 859-200-0428
Email: info@isafecomplete.com

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: Do they have other technicians on staff who are familiar with your network in case your regular technician goes on vacation or gets sick?

Our Answer: Yes; and since we keep detailed network documentation (basically a blueprint of your computer network) and updates on every client's account, any of our technicians can pick up where another one has left off.

Q13: When they offer an "all-inclusive" support plan, is it TRULY all-inclusive, or are their "gotchas" hidden in the fine print?

Our Answer: Our "Complete Managed Support" plan is just that – all-inclusive. One of the more popular service plans offered by consulting firms today is an "all-inclusive" or "all-you-can-eat" managed services plan. These are actually a good thing because they'll save you a lot of money in the long run – HOWEVER, make sure you REALLY understand what is and isn't included. Some things to consider are:

- Is phone/e-mail help desk included or extra? (Our Answer: Yes)
- What about network upgrades, moves or adding/removing users? (Our Answer: Yes)
- What about 3rd-party software support? (Our Answer: Yes)
- What are the costs/consequences of early cancellation? (Our Answer: 50% of Term)
- What if you aren't happy with their services? Do they offer a money-back guarantee? (Our Answer: Full for 60 days, 1 month after 60 days)
- Are off-site backups included? To what degree? (Our Answer: Unlimited Storage)
- What about on-site support calls? Or support to remote offices? (Our Answer: Yes)
- Are home PCs used to access the company's network after hours included or extra? (Our Answer: Included)
- Can they provide a detailed list of "Project" examples? (Our Answer: Yes)

100% of your line of business technology support is available in one simple, affordable monthly plan.

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
- Principle of least access
- Non-Administrative local user accounts
- 24/7/365 Monitoring, Detection & Response via SOC

1619 Bypass Rd. STE 122
Winchester, KY 40391
Phone: 859-200-0428
Email: info@isafecomplete.com

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.

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 darn sure whomever you hire is adequately insured with errors and omissions insurance, and don't be shy about asking them to send you the policy to review!

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.

Q16: Do their technicians participate in ongoing training – or are they learning on your dime?

Our Answer: Our technicians are required to keep up with the most current technology standards in all the software we support. We also pay for continuing education for our employees as a benefit of employment and reward them for achieving new skills and certifications. Plus, our hiring process is so stringent, 90% of the technicians who apply don't make it through (guess who's hiring them?).

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 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.

1619 Bypass Rd. STE 122
Winchester, KY 40391
Phone: 859-200-0428
Email: info@isafecomplete.com

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 immediately.

We understand how important your data is and how getting your team up and running quickly is essential to your business success. Therefore, in the event of any disaster, we can confidently get your network back up and running in six 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

1619 Bypass Rd. STE 122
Winchester, KY 40391
Phone: 859-200-0428
Email: info@isafecomplete.com

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.

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.

Here's how we handled our clients' needs when it seemed everyone needed to work remote, get laptops and implement security measures almost overnight. Up until the lockdowns occurred I was convinced that it wouldn't happen. However, as a remote worker organization ourselves, when it did happen, we had all the tools in place and had experience operating as a remote organization. We applied these same tools, and provided training for our clients so they could work remotely almost overnight.

We provided free Anti-Virus protection and monitoring for our client's home computers for several months to make sure they were virus free and working well. We helped them utilize Microsoft Teams to move critical documents to the cloud and trained them on how to utilize Teams of Zoom to conduct meetings and video calls. Finally, we provided a secure RemotePC software client that allowed them to connect directly to their work computer from home if necessary to run certain applications and access files that couldn't be moved to the cloud.

All of our clients that remained open were functional and productive through out the lockdown period and in spite of a 1200% increase in cyberattacks, we didn't have a single breach or infection. Even local news outlets sought out our expertise regarding the security of Zoom for business meetings.

1619 Bypass Rd. STE 122
Winchester, KY 40391
Phone: 859-200-0428
Email: info@isafecomplete.com

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.

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? 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.

1619 Bypass Rd. STE 122
Winchester, KY 40391
Phone: 859-200-0428
Email: info@isafecomplete.com

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 several healthcare clients that depend on their EMR and are required to meet HIPAA and HITECH security controls. The reason we work well with them is because we've had years of experience serving this industry and my wife has worked in healthcare for many 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 859-200-0428 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 27 point IT Security and compliance review.

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 HIPAA or HITECH regulatory controls.
- 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.

1619 Bypass Rd. STE 122
Winchester, KY 40391
Phone: 859-200-0428
Email: info@isafecomplete.com

To Schedule Your Initial Phone Consultation, visit the URL Below.

https://www.isafecomplete.com/initial-consultation/
Or Call: 859-200-0428

With appreciation,

Bob Stamper, President/CEO
iSAFE Complete Managed Services
Phone: 859-200-0428
E-mail: bob@isafecomplete.com
Web: https://www.isafecomplete.com/

1619 Bypass Rd. STE 122
Winchester, KY 40391
Phone: 859-200-0428
Email: info@isafecomplete.com

See What Other Healthcare Providers Are Saying:

Shem Beard
Eriksen Chiropractic

Always quick to answer any questions...

Nothing but great things to say about iSAFE and Bob Stamper. He installed a VOIP phone system in our office that saves us a couple thousand a year over traditional phone service. Install was clean, professional, and problem free. He's always been quick to answer any questions we have. Highest recommendation possible.

Dana Clay
Dr. Fulkerson

Accounting Software Working Again!

I can always count on iSAFE to take care of any of my computer problems… I stopped worrying long ago about computer issues because I know all I have to do is call. When we had to upgrade our accounting software, iSAFE found a way to make it work with our existing systems and they always respond quickly.

Donna Horn
Horn Therapy & Associates

Smooth Office 365 Data Migration.

When we need technical support, iSAFE is always quick to respond. They have helped us manage remote access and remote worker setup for over 40 Therapists, and they are assisting us with migrating to cloud based email and data services through Office 365.

iSAFE
We Make Technology Work For You

1619 Bypass Rd. STE 122
Winchester, KY 40391
Phone: 859-200-0428
Email: info@isafecomplete.com

The Top 5 Reasons Why You'll Want To Outsource Your IT Support To Us:

1. **Our Complete Managed Services package includes "Unlimited" support.** We refuse to "nickel and dime" our customers out of more money every time they actually need support. Anything that is required for you to continue business as usual, is included in your monthly support package. You will be surprised at what the "other guys" consider a "project" and will bill you for in addition to your regular package. You will also be surprised at what we "cover" and DO NOT charge extra for.

2. **You can expect a response in LESS than 2 hours for business emergencies, Guaranteed.** Unlike most IT firms whose average response time is 4-6 hours, we guarantee that we will respond to any "Urgent" ticket within two hours or less, and we put it in writing. If for any reason we don't exceed that expectation, we credit your account for the actual service time spent at our "Project" rates.

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 and we'll refund your money for up to 60 days after the initial agreement.

4. **We provide clear, understandable documentation and guarantees in writing.** Most IT companies will not put their response times or other "guarantees" in writing. We do our best to make sure every promise and service provided is clearly written and easy to understand.

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