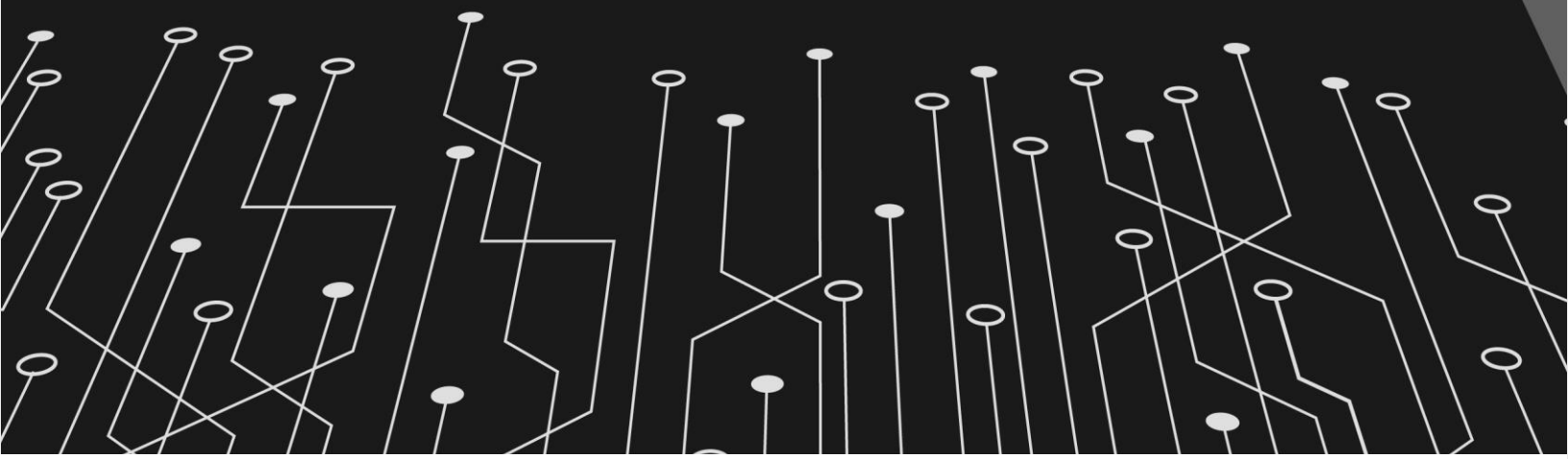
21 Critical I.T. Security Questions



A Free Education Guide By:
Information Systems of Montana
www.infosysmt.com/21questions
(406) 443-8386

21 Questions You Should Ask Your I.T. Services Company Or Consultant Before Hiring Them For I.T. Support

Customer Service:

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

Our Answer: When a client has a problem, we "open a ticket" in our I.T. management system so we can properly assign, track, prioritize, document and resolve client issues. However, some I.T. 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 I.T. issue on the fast track to getting resolved.

Q2 Are they good at answering your questions in terms you can understand and not in confusing "geek-speak"?

Good I.T. 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.

To Request Your FREE Assessment,
please visit **www.infosysmt.com/21questions**
or call our office at (406) 443-8386.

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

Our Answer: Most I.T. 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 one hour or less. A good I.T. firm should also be able to show you statistics from their PSA (professional services automation) software, where all client problems (tickets) get responded to and tracked. Ask to see a report on average ticket response and resolution times.

Q4 Will I be given a dedicated account manager/engineer?

Our Answer: YES! 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 and primary engineer, who will know you, your business and your goals.

Q5 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 I.T. 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 I.T.? 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.

To Request Your FREE Assessment,
please visit **www.infosysmt.com/21questions**
or call our office at (406) 443-8386.

I.T. Maintenance (Managed Services):

Q6 Do you offer TRUE managed I.T. services and support?

Our Answer: You want to find an I.T. company that will proactively monitor for problems and perform routine maintenance on your I.T. 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 I.T. companies fail to explain is what is NOT included in your monthly managed services agreement that will trigger an invoice. Their so-called "all you can eat" option is RARELY true – there are limitations to what's included and you want to know what they are BEFORE you sign.

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

- Do they 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 they charge extra if they have to resolve a problem with a line-of-business application, Internet service provider, phone system, leased printer, etc.? (What you want is an I.T. 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 your employees had to work remote (due to a shutdown, natural disaster, etc.), would they provide support on their home PCs or would that trigger a bill?
- If you 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 you would have to pay for? (Get this IN WRITING. Recovering from such a disaster could take hundreds of hours of time for your I.T. 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 above issues and MORE!

To Request Your FREE Assessment,
please visit **www.infosysmt.com/21questions**
or call our office at (406) 443-8386.

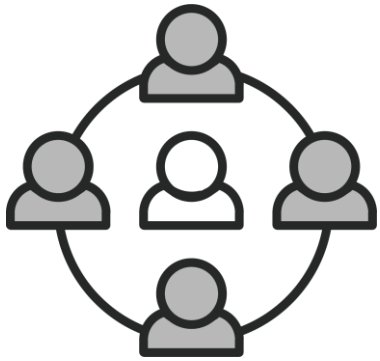
Q8 Is your help desk local or outsourced?

Our Answer: Be careful because smaller I.T. 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 help desk technicians to your account who will get to know you and your company, as well as your preferences and history. When you work with our local help desk technicians, they'll be more capable of successfully resolving your I.T. issues and handling things the way you want.

Q9 How many engineers do you have on staff?

Our Answer: Be careful about hiring small, one-person I.T. firms that only have one or two techs or that outsource this critical role. Everyone gets sick, has emergencies, goes on vacation or takes a few days off from time to time. We have more than enough full-time techs on staff to cover in case one is unable to work.



ALSO: Ask how they will document fixes, changes, credentials for you organization so if one tech is out or unavailable, another can step in and know your network settings, history, previous issues, etc., and how those issues were resolved. This is important or you'll be constantly frustrated with techs who are starting over to resolve a known issue or may screw up something because they don't understand or have a blueprint of your computer network.

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 I.T. company should provide this to you in both written (paper) and electronic form at no additional cost and update it on an agreed upon, periodic basis.

Why is this important? There are several reasons:

First, it shows professionalism and integrity in protecting YOU. No I.T. 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 I.T. 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.

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 I.T. person to have that much control over you and your company. If you get the sneaking suspicion that your current I.T. 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 less or more often as agreed) to provide a "strategic 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 technology budget, critical projects, compliance issues, known problems and cyber security best practices.

Our goal in these meetings is to help you improve operations, lower costs, increase efficiencies and ensure your organizational productivity stays high. This is also your opportunity to give us feedback on how we're doing and discuss upcoming projects.

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 I.T. firms hold their clients hostage with long-term contracts that contain hefty cancellation penalties and will even sue you if you refuse to pay.

We would never "force" a client to stay with us if they are unhappy for any reason. Therefore, we make it easy to cancel your contract with us, with zero contention or fines. Our "easy out" agreements make us work that much harder to exceed your expectations every day so we keep your business.

To Request Your FREE Assessment,
please visit **www.infosysmt.com/21questions**
or call our office at (406) 443-8386.

Cyber Security:

Q13 What cyber security certifications do you and your in-house team have?

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

You can feel confident that our in-house technicians have among the most advanced cyber security training and certifications available, including CompTIA Security+, Cisco Engineer, Sophos Engineer, Sophos Architect and Sophos Technician

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:

- MFA (multi-factor authentication)
- Advanced end-point protection, NOT just antivirus
- Advanced next gen firewall
- 24x7 Managed Detection and Response
- Penetration and Vulnerability Testing

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.

To Request Your <u>FREE</u> Assessment,
please visit **www.infosysmt.com/21questions**
or call our office at (406) 443-8386**.**

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 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 I.T. firm you're hiring has proper insurance to protect YOU.

Rest assured, we make it a priority to carry all the necessary insurance to protect you, including errors and omissions, workers' comp and cyber liability insurances you carry. Simply ask, and we will be happy to show you a copy of our policy.

Q16 Who audits YOUR company's cyber security protocols and when was the last time they conducted an audit?

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

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

You can be confident in the effectiveness of our cyber security because we are audited by CyberStone, Breach SecureNow and Vonahi, and we have just recently been audited in June 2022

To Request Your FREE Assessment,
please visit **www.infosysmt.com/21questions**
or call our office at (406) 443-8386.

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 I.T. firms have the resources and ability to run a good SOC in-house (this is the minority of outsourced I.T. 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 I.T. 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 outsourced SOC 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 I.T. 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 one hour 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 I.T. 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 I.T. 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 I.T. 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 I.T. 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 I.T. 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 I.T. provider about the "3-1-2" rule of backups, which has evolved from the "3-2-1" rule. The 3-2-1 rule was that you should have three copies of your data: your working copy, plus two additional copies on different media (tape/removable drive 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. Note that you need to ask your backup vendor specifically whether they offer a 3-1-2 as shown or if they offer only a 3-1-1 (one copy in the cloud.) Don't accept only a single copy in the cloud – it simply doesn't offer the protection afforded by modern continuity and backup solutions.

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 I.T. consultant how quickly they were able to get their clients working remotely (and securely) when Covid shut everything down. Ask to talk to a few of their clients about how the process went.

Here's how we handled our clients' needs when it seemed everyone needed to work remotely, get laptops and implement security measures almost overnight. During Covid shutdown, we were able easily move our clients to remote work and remote phones because or the NextGen Firewalls we install and the VoIP phone systems we install. Unless it was stated, no one knew that people were working remotely. We have continued to provide that service for any of our clients needing the remote work option.

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 I.T. company – particularly if the current company is hostile. It's disturbing to me how many I.T. 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 I.T. company will have a process in place for handling this.

If you consider us as your next I.T. services firm, we will gladly share our new client onboarding process and documentation. I think you'll be impressed.

To Request Your FREE Assessment,
please visit **www.infosysmt.com/21questions**
or call our office at (406) 443-8386.

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 focus on SMB Clients. The reason we work well with them is because , first, we are a small business oourselves and secondly, one of our core values is the "We Give A Damn!" Here's what a couple of our clients had to say:

"We love ISM for their great support, and they are friendly, easy to talk to, and fun and helpful. We like how we can call or submit a ticket and it is taken can of. They always follow up and never leave us hanging. We get busy and forget but ISM doesn't!"

– Kathy, Office Manager, Exploration & Drilling Enterprise

"Knowing that we are protected from cyber threats, hackers and malicious attacks let's me sleep at night. ISM has our back for our VoIP telephone service; all our computer workstations; our email and protection processing credit cards for clients. ISM has complete coverage for all our technology needs, period. I find that all the staff who I speak with on the phone, email or in person in our business to be very polite, kind and genuinely concerned to understand what we need."

– Lane, President, Concept Salon

"Your Staff Have Become An Extension Of Our Organization Switching to ISM still remains one of the best decisions I have made to improve the corporate operations and field systems operations between the corporate office where the file server resides and the group homes. Yes, it costs money, but it has also saved us a ton of down time and frustrations. From the very beginning ISM has been a great partnership. ISM handles all of our network changes with staff changes with a simple request through the user portal. I would not hesitate to recommend ISM to anyone considering outsourcing their IT function. I always believe that you pay for what you get but in the case of ISM I believe that we get a very solid value for what we pay maybe even more than I initially expected."

- Jen, Executive Director, Non-Profit

The 4 Most Costly Misconceptions About I.T. Services

Misconception #1: My I.T. network doesn't need regular monitoring and cyber security maintenance (managed services).

This is probably one of the biggest and most costly misconceptions that business owners have. Usually this is because they've been fortunate enough to have never encountered a major system failure that caused data loss from human error (or a disgruntled employee), failed hardware or even a ransomware attack, but that's just like someone thinking they don't need to wear a seat belt when driving a car because they've never had an accident.

I.T. networks are complex and dynamic systems that need regular updates and maintenance to stay up, secure, running fast and problem-free – especially now with the proliferation and sophistication of ransomware and hacker attacks. Here are just a FEW of the critical updates that need to be done on a weekly, if not daily, basis:

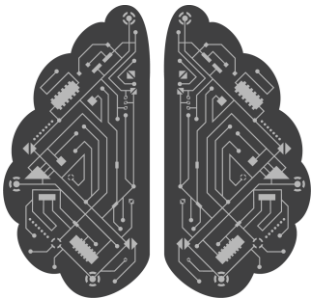
- Cyber security patches, updates and management
- Antivirus updates and monitoring
- Firewall updates and monitoring
- Backup monitoring and test restores
- Spam-filter updates
- Operating system updates, management
- Monitoring hardware for signs of failure
- Application patching including Line of Business applications, accounting, Microsoft, Apple, Adobe, etc (dozens upon dozens more that we monitor and patch)

If your I.T. support tech does not insist on some type of regular, automated monitoring or maintenance of your network, especially for cyber protections, then DO NOT HIRE THEM.

1. Either they don't know enough to make this recommendation, which is a sure sign they are grossly inexperienced and unprofessional, or…
2. They recognize that they are *profiting* from your I.T. problems and don't want to recommend steps toward prevention, which would reduce the number of issues you pay them to resolve.

To Request Your FREE Assessment,
please visit **www.infosysmt.com/21questions**
or call our office at (406) 443-8386.

Misconception #2: My nephew/neighbor's kid/brother-in-law/ office manager knows this I.T. stuff and can take care of our network.



Most people look for a part-time "guru" for one reason: to save a few bucks. But this often comes back to haunt them. We frequently get calls from business owners who desperately need our help to get them back up and running or to clean up a mess that was caused by an inexperienced employee or friend who was just trying to help.

If the person you have working on your I.T. systems does not do I.T. support for a living, there is a good chance they won't have the knowledge or experience to truly help you – they are a hobbyist at best. And do you really want a part-time, inexperienced person responsible for handling something as important as your data and I.T. network? As with everything in life, you get what you pay for. That's not to say you need to go broke to find a great I.T. firm, but you shouldn't be choosing someone based on price alone.

Misconception #3: You shouldn't have to pay "that much" for I.T. services.

We all know you get what you pay for. A cheap hourly rate $120 per hour usually means a cheap job. Like every other profession, **good** I.T. engineers and techs do NOT work cheaply because they are in high demand. **When you see low I.T. services fees, it's because of one of the following:**

1. They are a small shop just getting started. Usually they will have only one to two techs working for them (or they are a solo shop). That size of company may be perfectly fine for a small business that is not regulated, doesn't have sophisticated I.T. requirements and/or has only 10 or fewer PCs to support. This would not be a good choice for a larger organization that needs professional I.T. services for their growing company.
2. They are hiring inexperienced (cheap) college kids or newbie technicians because they will work for next to nothing, OR they allow interns to support your network because they don't have to pay them at all – but what you don't realize is that an inexperienced technician like this can end up costing more because:

   - ✓ They improperly diagnose problems, which means you're paying them to fix the wrong thing and they still won't resolve your issue. Case in point: A few years ago a TV reporter

went undercover to I.T. services companies in LA with a perfectly working PC, but simply disconnected a cable in the back (a fix that the average tech would have caught in minutes with a visual inspection). Several shops improperly diagnosed the problem and wanted to charge them up to $275 to fix it!

- ✓ They could take three to five times as long to do the same repair an experienced technician could fix quickly. Again, you're paying for those extra hours AND you're frustrated and unproductive while you wait for the SAME problem to be fixed!
- ✓ They could do things that put your security and data in jeopardy. True story: An inexperienced engineer of a competitor turned off all security notifications his client's network was producing because it was "too much work" to sift and sort through them. Because of this, the company got hacked and ended up having to pay a ransom to get their data back, not to mention suffered downtime for days while they scrambled to recover. Don't let a cheap, inexperienced tech do this to you!

With your client data, accounting records, e-mail and other critical data at stake, do you REALLY want the lowest-priced shop working on your machine?

We take the view that most people want value for their money and simply want the job done right. You will find that we are not the cheapest, but we don't apologize for that. As the owner, I decided a long time ago that I would rather explain our higher rates ONE TIME than make excuses for POOR SERVICE forever. That said, we're not the most expensive either. We simply feel that we should offer a good service at a fair price. That's why we have been able to stay in business for over 27 years and have over 185 clients who've been with us that entire time.

Misconception #4: An honest I.T. services company should be able to give you a quote over the phone.

I wish this were true, but it isn't. Just like a good doctor, an honest and professional technician will need to diagnose your network before they can quote any price over the phone; consider the example above where all that was needed was to plug in a simple cable. If someone brought that to us, we would just plug it back in and not charge them, but without SEEING the computer, we could have never diagnosed that over the phone.

To Request Your FREE Assessment,
please visit **www.infosysmt.com/21questions**
or call our office at (406) 443-8386.

3 More Recommendations To Find A Great I.T. Company You'll Love

1 Ask to speak to several of their current clients.

Check their references! Don't just take the sales guy's word that they are good – ask to speak to at least three or four clients that are similar to you in size and scope. If they hesitate or cannot provide you with references, don't trust them!

Another good sign is that they have good online reviews and client testimonials on their website. A lack of this may be a sign that they don't HAVE clients who are happy enough to provide a good reference – again, a warning sign.

2 Look for a company that is local

While it is true that many technical issues can be resolved remotely, on-site response time is everything when you are experiencing a nightmare of a technical issue, like network or server down or phone system down. When the inevitable emergency happens, you need help as quickly as possible. So why would you partner with an I.T. Consultant that cannot even get to your location in a reasonable amount of time? Or at all, for that matter.

3 Choose an I.T. consultant who is responsive and cares about your business almost as much as you do

How long do you want to wait for your I.T. Consultant to respond when your systems are down, 1 hour? 2 hours? Longer? Like most people, you probably do not want to wait at all. In the technology world, uptime is money, so unresponsive I.T. could cost your business more than it saves, in a relatively short amount of time. Make sure to check if they have a response time goal or guarantee for their managed clients. This is a sign of a company that is well prepared and able to handle even the most asymmetric of technical issues. If they do not lay out their response times, be prepared to play the waiting game, and possibly pay for it, too. Two of our core values are "We Give A Damn" and "Results", and we can SHOW you!

To Request Your FREE Assessment,
please visit **www.infosysmt.com/21questions**
or call our office at (406) 443-8386.

A Final Recommendation

I hope you have found this guide to be helpful in shedding some light on what to look for when outsourcing I.T. for your company. As I stated in the opening of this report, my purpose in providing this information was to help you make an informed decision and avoid getting burned by the many incompetent firms offering these services.

If you are looking for someone you can trust to take over the care and maintenance of "all things digital" in your office, we'd love the opportunity to EARN your business. To that end, we'd like to offer you a…

FREE Cyber Security Risk Assessment And I.T. Systems Checkup.

*This is **completely free**, and with no expectations for you to hire us unless you feel that is the right thing for you to do.*

Here's how this works…

We'll meet by phone (or Zoom) to have a brief conversation about your current situation; what you are frustrated by, looking for in an I.T. company and any concerns and questions you have. We'll ask you a few questions that you should easily be able to answer. Depending on what we discover, we can move to the next step, which is to conduct a quick, non-invasive, CONFIDENTIAL investigation of your computer network, backups and security protocols.

Your current I.T. company or team DOES NOT NEED TO KNOW we are conducting this assessment, or we can involve them. (The choice is yours, but we recommend NOT letting them know this inspection is happening so we can get a truer read of how secure you are. After all, the cybercriminals won't tip you off that they're about to hack you.)

Your time investment is minimal: under 30 minutes for the initial phone consultation, 30 minutes to show an engineer around (or have one of your staff do it) and about one hour in the second meeting to go over what we discover. When this Risk Assessment is complete, here's what you will know:

- If your I.T. systems and data are truly secured from hackers, cybercriminals, ransomware and even sabotage by rogue employees.
- If your current backup would allow you to be up and running again fast if ransomware locked all your files – 99% of the computer networks we've reviewed failed this test.
- If you and your employees' login credentials are being sold on the dark web right now and what to do about it. (I can practically guarantee they are, due to a recent 8.4 billion credentials being sold on the dark web. What we find will shock you.)
- Answers to any questions you have about a recurring problem, an upcoming project or change or about the service you are currently getting.

When done, we'll provide you with a **"Report Of Findings"** and Network Health Score that will show you where you are vulnerable to cyber-attacks, problem devices, backup issues, etc. We'll also provide you with an Action Plan, for free, on how to remediate any less than favorable situation or problem we discover – and if you choose, we can assist you in its implementation.

After doing this for over 27 years, I can practically guarantee I will find significant and preventable security loopholes in your network and problems with your backups. Like Sherlock Holmes, we never fail. If nothing else, our Risk Assessment is an easy and free way to get a valid third party to verify your security and give you peace of mind.

Dedicated to your peace of mind,

Michael Marlow, President
Information Systems of Montana

To Request Your <u>FREE</u> Assessment,
please visit **www.infosysmt.com/21questions**
or call our office at (406) 443-8386**.**

Other Things To Notice And Look Out For:

How is a ransomware attack handled

Our Answer: Recovering from a cyber-attack could take HOURS of high-level I.T. expertise. Will your IT people work hand-in-hand with your advanced cyber security experts, ransom negotiators, your insurance company, the local police and the F.B.I.? Do they have a written cyber incident response plan? Do they have any experience in this realm? Be sure you're clear on this before you sign, because surprising you with a lot of "I don't know's" is totally and completely unacceptable.

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

Our Answer: Any good IT company will answer their phones LIVE (not voice mail or phone trees) and respond from 8:00 a.m. to 5:00 p.m. every weekday. But many CEOs and executives work outside normal "9 to 5" hours and need I.T. support both nights and weekends. If this is an additional service you need, not only can you reach our after-hours support any time and any day, we GUARANTEE a response time of two hours or less for normal problems, and within 60 minutes for problems marked "emergency," such as a network being down or a critical problem that is significantly impacting your ability to work.

To Request Your FREE Assessment,
please visit **www.infosysmt.com/21questions**
or call our office at (406) 443-8386.

Read On To Hear What Our Clients Have To Say:

ISM is always available to us when we need them. We can email them at any time and get a response back in no time at all. They schedule time to help as quickly as possible and they put in extra effort to always ensure our issues are resolved even if it means bringing in another staff member for assistance. There is no problem too big or small for them.

– Emily, Executive Director, Regional Non-Profit

I believe every company needs active monitoring. A smaller subsidiary company of ours was not using option and they suffered a devastating virus attack. Again, this is peace of mind for me knowing I don't need to worry about this. I can concentrate on our business and leave the IT issues to someone whom I completely trust.

– Colleen, Union Business Manager

ISM's service has been great! I'm very glad we have moved to the new and improved program and pay the extra money. It really has eased all our minds knowing that your engineers and your team are watching what is going on. I love the quick response too, and the team is great about showing me things, so I feel like I'm still learning and growing, but I don't feel the pressure of making sure I MUST do it!

– Julie, IT Manager, Credit Collection Agency

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do

How To Request Your <u>FREE</u> Assessment:

Visit **www.infosysmt.com/21questions**

or call our office at (406) 443-8386.