21 Key Questions for Hiring an IT Consultant

This Business Advisory Guide Will Arm You With 21 Critical Questions You Should Ask Any IT Consultant Or Company Before Giving Them Access To Your IT Systems!

CNS
Your Partner in Technology

(916) 366-6566 | callcns.com

Table of Contents

Read this guide and you'll discover:

- The "dirty little secret" of the IT support industry that most people don't know and will never be told by their IT guy (this will surprise you).
- 21 revealing questions that will help you instantly spot an unethical or grossly incompetent IT support technician in minutes.
- 4 costly misconceptions most business owners have about IT services – and what you need to consider when selecting an IT firm.
- Hackers, ransomware and data theft: what you REALLY need to know to protect yourself from a costly, devastating ransomware attack.

An Open Letter To All Business Owners And Leaders Who Outsource IT Support

Dear Fellow Business Owner or Executive,

Choosing the right IT company is a daunting task. Pick the wrong one and you could end up locked into a contract where frustrations and costs mount as you get hammered with constant IT problems and horrible service.

Pick the right one and you'll breathe a sign of relief as your IT problems disappear and you gain complete peace of mind that your data and company are protected. Problem is, they all sound good and promise to be proactive, responsive and professional, but how can you really know who the good guys are until you sign a contract and turn over the "keys" to your company's network?

You can't, and that's why we wrote this executive guide. We want to help business owners avoid the frustration and losses that can result in hiring the wrong IT firm by asking the right questions and knowing what to look for in advance. There are signs, but you have to know what to look for.

Sadly, there's no shortage of horror stories about incompetent IT "gurus" bungling jobs and causing MORE problems as a result of their gross incompetence, lack of qualified staff and poor cyber security skills. I'm sure if you talk to your friends and colleagues you will get an earful of the unfortunate experiences they have encountered in this area.

Part of the problem is that the IT services industry is not regulated like most other professions, which means ANYONE can claim they are an "IT expert." **This means you, the consumer, must be far more diligent about who you choose to do IT support and arm yourself with the information contained in this report.**

From misleading information and unqualified technicians to poor management and terrible customer service, we've seen it all…and we know they exist in abundance because we have had a number of customers come to us to clean up the disasters they have caused.

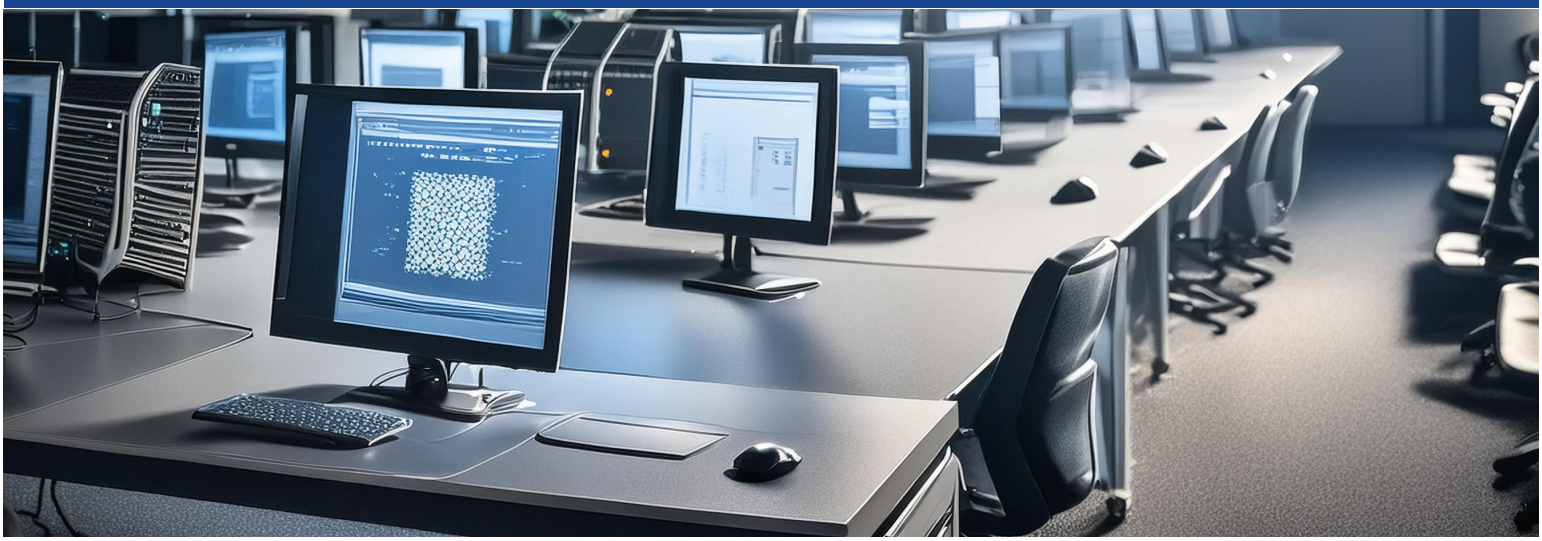
The information in this guide is provided to help raise standards within the IT support industry and to give YOU useful information to help you guard against the lack of ethics or incompetence of some IT companies and technicians.

Dedicated to serving you,

John Guarienti
Vice President

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, all their employees have access to call our help desk for immediate support or simply send an email. We "open a ticket" in our IT management system so we can properly assign, track, prioritize, document and resolve client issues. However, some IT firms force you to log in to submit a ticket and won't allow you to call or e-mail them. This is for THEIR convenience, not yours. Trust me, this will become a giant inconvenience and thorn in your side. While a portal is a good option, it should never be your ONLY option for requesting support.

Also, make sure they HAVE a reliable system in place to keep track of client "tickets" and requests. If they don't, I can practically guarantee your requests will sometimes get overlooked, skipped and forgotten.

Requesting support should also be EASY for you. So be sure to ask how you can submit a problem to their support desk for resolution. We make it easy. Calling or e-mailing, puts your IT issue on the fast track to getting resolved.

Q2: Do you offer after-hours support, and if so, what is the guaranteed response time?

Our Answer: Any good IT company will answer their phones LIVE (not voice mail or phone trees) and respond from 5:00 a.m. to 5:00 p.m. PST every weekday. But many CEOs and executives work outside normal "9 to 5" hours and need IT support both nights and weekends. Not only can you reach our after-hours support any time and any day, we GUARANTEE a response time of one hour or less for normal problems.

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

Our Answer: Most IT firms offer a 60-minute or 30-minute response time to your call during normal business hours. Be very wary of someone who doesn't have a guaranteed response time IN WRITING – that's a sign they are too disorganized, understaffed or overwhelmed to handle your request. Our written, guaranteed response time is one hour or less. We offer immediate phone support for all employees with an average wait time of 90 SECONDS. Or for non-urgent issues you can email us with an average of a 90 minute response time. A good IT firm should also be able to show you statistics from their PSA (professional services automation) software, where all client problems (tickets) get responded to and tracked. Ask to see a report on average ticket response and resolution times.

Q4: Will I be given a dedicated account manager?

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

Q5: Do you have a feedback system in place for your clients to provide "thumbs up" or "thumbs down" ratings on your service? If so, can I see those reports?

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

IT Maintenance (Managed Services)

Q6: Do you offer true managed IT services and support?

Our Answer: You want to find an IT company that will proactively monitor for problems and perform routine maintenance on your IT systems. If they don't have the ability to do this, or they don't offer it, we strongly recommend you look somewhere else. Our remote network monitoring system watches over your network to constantly look for developing problems, security issues and other problems so we can address them BEFORE they turn into bigger problems.

Q7: What is NOT included in your managed services agreement?

Our Answer: Another "gotcha" many IT companies fail to explain is what is NOT included in your monthly managed services agreement that will trigger an invoice. Their so-called "all you can eat" option is RARELY true – there are limitations to what's included and you want to know what they are BEFORE you sign.

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

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

Our Answer: We cover the restore.

Other things to inquire about are:

- Do you offer truly unlimited help desk? (Make sure you are not nickel-and-dimed for every call.)

  Our Answer: CNS covers unlimited help desk support and the set up for new employees and their computers.

- Does the service include support for cloud services such as Microsoft 365?

  Our Answer: CNS covers supporting our customers cloud applications just like the business applications being used on a server.

- 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.)

  Our Answer: CNS covers supporting our customer's business applications

- What about support to remote offices?

  Our Answer: CNS covers supporting our customers working from remote or home offices from the company managed device.

- 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?

  Our Answer: CNS covers supporting our customers working from remotely and did so in the recent COVID pandemic.

Q8: Is your help desk local or outsourced?

Our Answer: Be careful because smaller IT firms may outsource this critical function. As a result, you may get a tech who is not familiar with you, your network, previous problems, and personal preferences. Or worse, they may not be as qualified. This can be frustrating and lead to the same problems cropping up over and over, longer resolution time and you having to spend time educating the tech on your account.

Fortunately, we provide a dedicated technician 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 technician, they'll be more capable of successfully resolving your IT 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 IT firms that only have one or two techs or that outsource this critical role. Everyone gets sick, has emergencies, goes on vacation, or takes a few days off from time to time. We have more than enough full-time techs on staff to cover in case one is unable to work.

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

Q10: Do you offer documentation of our network as part of the plan, and how does that work?

Our Answer: Network documentation is exactly what it sounds like: the practice of maintaining detailed technical records about the assets you own (computers, devices, software, directory structure, user profiles, passwords, etc.) and how your network is set up, backed up and secured. Every IT company should provide this to you in both written (paper) and electronic form at no additional cost and keep it updated.

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 electronic form at no additional cost. We also maintain the portal in real time as items are changed.

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 have strategic virtual Chief Information Officer (vCIO) meetings with your clients as part of your managed services agreement?

Our Answer: To us, there's nothing more important than consulting with our clients. Therefore, we make it a priority to meet with all our clients at least annually (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 strategic vCIO meetings with you are C-level discussions (not geek-fests) where we openly discuss your business goals, including your IT budget, critical projects, compliance issues, known problems and cyber security best practices.

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

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

Our Answer: Make sure you carefully review the cancellation clause in your agreement. Many IT firms hold their client's hostage with long 3-year term contracts that contain hefty cancellation penalties and will even sue you if you refuse to pay. Our contract is only for 1-year, which ensures flexibility and demonstrates our commitment to client satisfaction. We would never "force" a client to stay with us if they are unhappy.

Cyber Security

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

Our Answer: It's important that your IT firm have some type of recent training and certifications, and they should be able to answer this question, which demonstrates a dedication to learning and keeping up with the latest cyber security protections. 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 in 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+

CompTIA CYSA+

CompTIA CASP+

ISACA CISA

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:

- Only company owned and managed PC/Laptops can access company data
- Devices are managed in Microsoft's Cloud Azure Entra ID
- 2FA (two-factor authentication)
- Provide Employees with Security Awareness Training on Phishing scams
- Advanced end-point detection and response (EDR) protection, NOT just antivirus
- Use an internet filter, even when remote.
- Use disk encryption on all computers
- Restrict access to data from within the U.S. (unless travel time is requested)

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: Does your IT company supply Secure Awareness Training to help educate your employees to identify email phishing scams?

Our Answer: Using a Phishing training solution can offer better content and tests than passing on detected phishing emails. Security Awareness Training & Phishing Simulation. Training programs try to lower the chance of employees being tricked by phishing attacks. As employees become more mindful of the risks, they are less likely to click on harmful links, give away sensitive information, or do things that could jeopardize security.

- Training videos: A library of short videos is assigned to spot actual phishing scams. You can use these for new hires and yearly training.
- Phishing simulation: Email training is a proactive approach to cybersecurity education that involves simulating real-world phishing attacks to train employees on how to recognize and respond to threats.

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 IT consulting firm will have an independent third party reviewing and evaluating their company for airtight cyber security practices.

There are many companies that offer this service, so 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 cybersecurity measures, as we have undergone and passed a Service Organization Control Type 1 audit with a focus on cybersecurity by MSP Alliance.

Q17: Do you have a Security Operation Center 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.

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 as quickly as possible.

Q19: Is all your data backed up? Do you know what your data backup recovery retention schedule is? Your data may be in multiple places.

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.

If you don't feel comfortable asking your current IT company to test your backup OR if you have concerns and want to see proof yourself, just conduct this little test: Copy three unimportant files onto a thumb drive (so you don't lose them) and delete them from your server. Make sure one was newly created that same day, one was created a week earlier and the last a month earlier. Then call your IT company and let them know you've lost three important documents and need them restored from backups as soon as possible. They should be able to do this easily and quickly. If not, you have a problem that needs to be addressed immediately!

Our Answer: At CNS It is a requirement for the client to provide written acknowledgment in the form of a signed Backup Data Source Report, confirming the inclusion of all data sources. This list should encompass any new source drives that may arise subsequent to CNS's commencement of data protection services. CNS's data protection services encompass various platforms, namely Microsoft 365 data, on-premises servers, and Azure cloud machines.

Q20: Do you restrict sending sensitive data in an email?

Our Answer: It is not safe to send sensitive data in an email without encryption by mistake. Data Loss Prevention (DLP) is a collection of tools and features that help organizations avoid the unwanted or deliberate exposure of sensitive information.

DLP can help protect sensitive data by identifying and preventing the unauthorized sharing or exposure of confidential information such as financial records, customer data, intellectual property, and more.

Policy Enforcement helps organizations define and enforce policies that specify how sensitive information should be handled. This includes preventing the sharing of certain data outside the organization or encrypting emails containing sensitive content.

DLP helps meet Compliance with Regulations by assisting organizations in complying with industry regulations and data protection laws by providing tools to control the flow of sensitive information. This is crucial for industries with strict regulatory requirements, such as healthcare (HIPAA), finance (PCI DSS), and others.

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.

Is Your IT Provider Secure?

To further protect your business against today's threats, CNS developed security solutions and best practices that follow the Cyber Security Framework developed by the National Institute of Standards and Technology (NIST).

Maintain Your Small Business Compliance Perfectly With CNS IT Security Services

Our team at CNS can help you to maintain your compliance perfectly. You will save money when you are not missing regulatory changes and requirements as CNS stays abreast of industry requirements and adjustments. This is one of the key services that CNS offers, and keeping your business compliant is critical for most industries.

Being spared regulatory mistakes is not only going to save you money, but it will save your company from unnecessary downtimes and struggles with security risks that could have been prevented. There are many reasons to remain compliant, and CNS can take care of this business essential for you every single day.

We have made sure that we meet Soc 2 standards because we know that you deserve the best security protection for your business operations.

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. Just look at what our clients had to say:

Douglas Woods

★★★★★

"We have been using CNS for our IT needs for about 6 months. They are friendly, knowledgeable, responsive, innovative and consistently proactive in making sure that if one individual has an issue that no one else at the branch experiences that problem. CNS works well servicing large and small organizations."

Douglas Woods - Branch Production Manager - American Pacific Mortgage

Cooper Hosley

★★★★★

"More than five years ago, Grow West handed over our IT infrastructure to CNS. They've been a crucial business partner ever since, consistently delivering dependable service and stellar support. Through challenges like wildfires, winter storms, and the pandemic, our team maintained full access to our systems, even with our offices closed. With CNS, we can focus on our core functions, secure in the knowledge that our IT infrastructure and support are in excellent hands."

Heather Headley

★★★★★

"I work for APMC mortgage as a LO/Loan. Since CNS-Service/Capital Network Solutions, Inc. has become our in-house help desk, it's been AWESOME. They're corrected tech items that just couldn't be handled before. I've spoken with 4 different people and every single one has been knowledgeable, courteous, works and gets things done at warp speed and have always completed correctly. They're really nice too. I can't recommend this company highly enough. Heather Headley, NMLS #247345"

The 4 Most Costly Misconceptions About IT Services

Misconception #1: My IT 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.

IT 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
- Remediate alerts from EDR (End Point Detection and Response)
- Firewall updates and monitoring
- Backup monitoring
- Spam-filter updates
- Operating system updates, management
- Monitoring hardware for signs of failure

If your IT 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 IT problems and don't want to recommend steps toward prevention, which would reduce the number of issues they are paying you to resolve.

Either reason is a good one to get as far away from that person as possible!

Misconception #2: My nephew/neighbor's kid/brother-in-law/office manager knows this IT 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 IT systems does not do IT 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 IT 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 IT firm, but you shouldn't be choosing someone based on price alone.

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

We all know you get what you pay for. A cheap hourly rate usually means a cheap job. Like every other profession, good IT engineers and techs do NOT work cheap because they are in high demand. When you see low IT 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 IT 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 IT 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 IT 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 35 years and have more than 100 customers.

Misconception #4: An honest IT 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.

3 More Recommendations To Find A Great IT 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 has been in business for more than 10 years with an internal staff. Not a one-man shop who "partners" with cheap overseas support.

3. Choose an IT consultant who regularly collaborates with you to develop a budget and a roadmap for larger projects. Ensure they present both on-premise and cloud-based solutions, providing a clear understanding of the risks and costs associated with each option.

A Final Recommendation

I hope you have found this guide to be helpful in shedding some light on what to look for when outsourcing IT 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 IT 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 IT 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 IT 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: <<30 minutes>> for the initial phone consultation and 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 IT 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 25 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 cheap (free) way to get a valid third party to verify your security and give you peace of mind.