CAPTAIN I.T.

21 CRITICAL I.T. SECURITY QUESTIONS

BY: ANTHONY HERNANDEZ
PRESIDENT & CEO

BELL ROOF COMPANY, INC.

★★★★★ **"CAPTAIN IT STEPPED IN TO HELP"**

"Before we met Captain IT, there were a few holes in our system. We had outdated systems and software that needed an upgrade, but we didn't know what to do. We needed someone who could patch up those holes. ***Captain IT stepped in to help.*** *After giving us recommendations concerning our budget and company needs, we hired them. They even provide monthly reports on what they've been protecting us from!"*

David Lenaker
CFO

GERI'S, LLC

★★★★★ **"ABLE TO SOLVE THE PROBLEM QUICKLY"**

"I strongly recommend Captain IT. I have been working with them for several years now. They helped us on several occasions to fix software and networking problems. When we were installing a new network printer, it had lost connection. Captain It was ***able to solve the problem quickly*** *and get us back on track with our install. Although we never look forward to having computer problems it is always assuring that we can call Captain IT and know that our issues will be taken care of! Tremendous service!"*

Russ Hilbig
General Manager

What Every Business Owner Must Know About Hiring An Honest, Competent, Responsive And Fairly Priced I.T. Services Firm.

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

READ THIS GUIDE AND YOU'LL DISCOVER:

- The "dirty little secret" many I.T. support companies don't want you to know and will never tell you (this will surprise you).
- 21 revealing questions that will help you instantly spot an unethical or grossly incompetent I.T. support technician in minutes.
- 4 costly misconceptions most business owners have about I.T. services and what you need to consider when selecting an I.T. firm.
- Hackers, ransomware and data theft: what you REALLY need to know to protect yourself from a costly, devastating ransomware attack.

Anthony Hernandez

CEO

Dear Fellow Business Owner or Executive,

Choosing the right I.T. 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 I.T. problems and horrible service.

Pick the right one and you'll breathe a sigh of relief as your I.T. 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 I.T. 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 I.T. "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 I.T. services industry is not regulated like most other professions, which means ANYONE can claim they are an "I.T. expert." This means you, the consumer, must be far more diligent about who you choose to provide I.T. 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 I.T. support industry and to give YOU useful information to help you guard against the lack of ethics or incompetence of some I.T. companies and technicians.

Dedicated to serving you,

Anthony Hernandez

MEET THE AUTHOR

CAPTAIN I.T.

Anthony Hernandez is a Senior Technology Consultant. He grew up in Los Angeles, CA and is a proud graduate of Cal Poly Pomona, where he earned a Computer Science degree. He's always had a passion for technology and helping people, evidenced by his commitment to technology employment throughout college and beyond. He's worked as a computer repair technician, website designer, database programmer, senior level field engineer, technology manager, and technology director.

Prior to establishing Captain IT, he worked for Green Dot Public Schools, a charter school management group that encompassed 20 school sites. From scratch, he helped the entire organization design and implement an effective computer network infrastructure that served each one of these sites. At the conclusion of his seven years of service, the school system had a reliable, robust technology infrastructure that continues to operate today.

Customer satisfaction has always been his top priority; it serves as his motivation to acquire new skills and learn new technologies. At Green Dot, the infrastructure consisted of clustered Microsoft exchange servers, Cisco firewalls, backup strategies, designing data centers, replicating servers (across all 20 locations), and asset management systems; he developed policies and procedures for effective technology management, budget management, and procurement where each of these were concerned. Needless to say, he learned everything from scratch; and as a result, the knowledge and expertise that was gained while managing the technology of an entire school district gave him the skills, motivation, and courage to start his own business.

Anthony Hernandez
President & CEO
Captain IT

CAPTAIN I.T.

21 QUESTIONS YOU SHOULD ASK YOUR I.T. SERVICES COMPANY OR CONSULTANT BEFORE HIRING THEM FOR I.T. SUPPORT

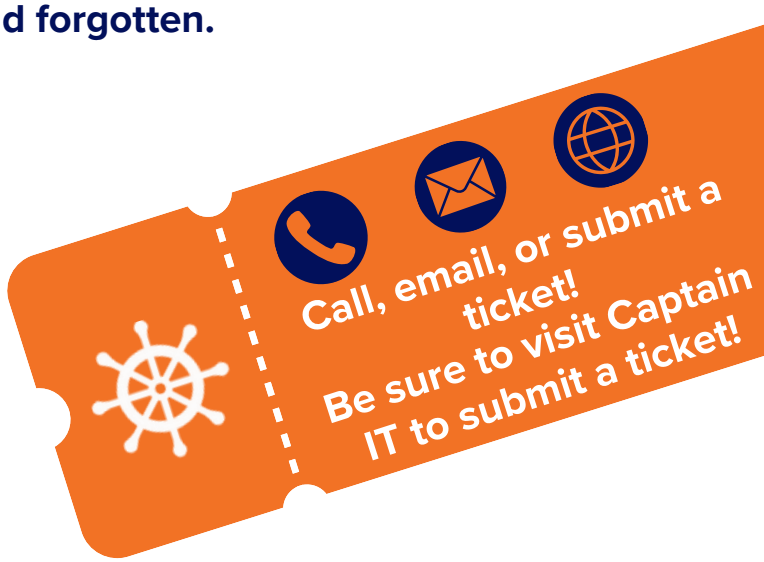
CUSTOMER SERVICE:

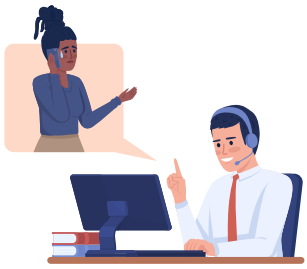
1 WHEN I HAVE AN I.T. PROBLEM, HOW DO I GET SUPPORT?

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.





2 DO THEY ANSWER THEIR PHONES LIVE OR DO YOU ALWAYS HAVE TO LEAVE A VOICEMAIL AND WAIT FOR SOMEONE TO CALL YOU BACK?

Our Answer: We answer our phones live from 6:00 a.m. to 7:00 p.m. and give all clients a direct phone number they may call if a problem arises, including weekends. Why? Because many of the CEOs and executives we support work outside normal hours and find it to be 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.

3 DO YOU HAVE A WRITTEN, GUARANTEED RESPONSE TIME FOR WORKING ON 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.

We guarantee a 5 minute response time to critical issues. This is written into every service agreement we give to our clients because it's standard procedure. 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.

4 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 and semi-annual 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 is to help our clients be more profitable, efficient and competitive with these meetings.

5 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.

I.T. MAINTENANCE (MANAGED SERVICES):

6 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.

7 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.

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 I.T. 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 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?

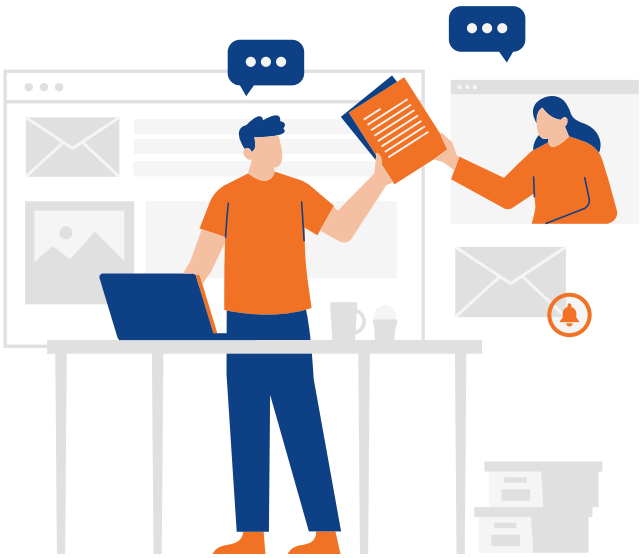
- If our employees had to work remote (due to a shutdown, natural disaster, etc.), would you provide support on their home PCs or would that trigger a bill?
- If we were to get ransomed or experience some other disaster (fire, flood, theft, tornado, hurricane, etc.), would rebuilding the network be included 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 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 infrastructure proactive maintenance, server support, and cyber security services.

8 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 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 I.T. issues and handling things the way you want.



9 ARE YOU A ONE-MAN SHOW OR DO YOU HAVE OTHER TECHS?

Our Answer: Be careful about hiring one-person I.T. consultants. Everyone gets sick, has emergencies, goes on vacation or takes a few days off from time to time. We have multiple 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.

10 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 a quarterly 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!

11 DO YOU MEET WITH YOUR CLIENTS REGULARLY 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 or bi-annually 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 I.T. 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.

12 IF I NEED OR WANT TO CANCEL MY SERVICE WITH YOU, HOW DOES THIS HAPPEN AND HOW DO YOU OFFBOARD US?

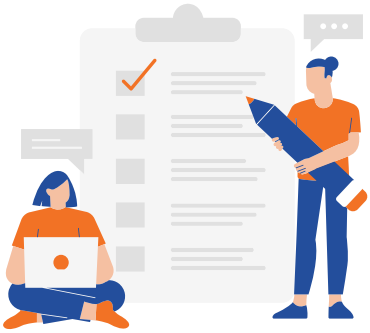
Our Answer: Make sure you carefully review the cancellation clause in your agreement. Many I.T. firms hold their clients hostage with long-term contracts that contain hefty cancellation penalties and will even sue you if you refuse to pay.

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.

TECHNICAL EXPERTISE:

13 WHAT TECHNICAL CERTIFICATIONS DOES 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 cybersecurity 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 training and certifications available, including A+ which is the foundation of IT support, Network+ which is knowing how to configure networks, and lastly, Security+ which is understanding system security.

14 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
- Email Phishing Detection
- Cybersecurity Training

Because a combination of these lockdown strategies is essential to protecting your network and data, we employ ALL of these for our clients. Effective cybersecurity should never compromise between choosing this OR that. It should feature every weapon in your arsenal.

15 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. Simply ask, and we will be happy to show you a copy of our policy.

16 WHO AUDITS YOUR COMPANY'S CYBERSECURITY 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 cybersecurity 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 cybersecurity seriously.

17 WHAT ARE YOUR MINIMAL SECURITY STANDARDS?

Our Answer: : We understand how important it is to secure your network from internal and external cyber threats. Minimal security standards include at least the following:

1. **A good firewall with top grade security services**
2. **Good spam filtering and DNS systems**
3. **Frequent Security Assessments**
4. **Security Awareness Training**
5. **Multi-layer approach to data backups and disaster recovery**
6. **Ongoing computer updates and security patching**
7. **Ongoing Dark Web Monitoring**
8. **Multi-Factor Authentication**
9. **Encryption on all critical systems**
10. **Advanced Endpoint Security (not just Antivirus)**

BACKUPS AND DISASTER RECOVERY:

18 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 2 hours or less.

19 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 “3-2-2” rule of backups, which has evolved from the “3-2-1” rule. The 3-2-1 rule is that you should have three copies of your data: your working copy, plus two additional copies on different media (tape and cloud), with at least one being off-site for recovery. That rule was developed when tape backups were necessary because cloud backups hadn’t evolved to where they are today. Today, there are more sophisticated cloud backups and BDR (backup and disaster recovery) devices.

20 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. You should ask to talk to a few of their clients about how the process went.

21 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.

OTHER THINGS TO NOTICE AND LOOK OUT FOR:

1 ARE THEY GOOD AT ANSWERING YOUR QUESTIONS IN TERMS YOU CAN UNDERSTAND AND NOT IN ARROGANT, 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. Just look at what this one client had to say:

2 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.

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:

- **Security patches applied – with NEW viruses and hacker attacks cropping up DAILY, this is a CRITICAL part of maintaining your network.**
- **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**

MISCONCEPTION #2: I.T. SERVICES ARE ONLY FOR BIG COMPANIES

Many small businesses or startups believe that I.T. services are only necessary for large organizations. However, I.T. support is crucial for businesses of all sizes. Even small companies rely on technology for communication, data storage, security, and operations. Outsourcing I.T. services can help businesses of any size streamline their processes, protect sensitive data, and reduce operational risks.

Small businesses are increasingly targeted by cybercriminals. I.T services can help protect sensitive business data and customer information through firewalls, encryption, anti-virus software, and regular security audits. I.T services enable small businesses to take advantage of cloud computing, offering access to powerful software, storage, and collaboration tools without the upfront cost of physical infrastructure.

I.T issues can arise at any time, and small businesses often lack the resources to hire full-time I.T staff. I.T services provide on-demand support to resolve technical issues, minimizing downtime and keeping business operations running smoothly.

MISCONCEPTION #3: ALL I.T PROVIDERS ARE THE SAME

People tend to think that all IT service providers are identical in terms of the services and quality they offer. However, there are significant differences in expertise, customer service, and the technologies used. It's important to evaluate an IT provider based on their specialization, reputation, and ability to meet the specific needs of your business. A good IT partner can make a major difference in optimizing your infrastructure, security, and overall technology performance.

Some IT service providers offer a broad range of services for all types of businesses, while others may specialize in particular industries (e.g., healthcare, finance, or retail). Choosing a provider with expertise in your specific industry can be valuable as they understand the unique challenges you face.

The depth of expertise in various IT fields—such as cybersecurity, cloud services, or infrastructure management—can vary. Some providers may have specialized certifications or extensive experience in specific technologies or platforms.

Managed service providers (MSPs) offer proactive, ongoing support, monitoring, and maintenance, while break-fix providers only address issues as they arise. Managed services tend to be more reliable because they focus on preventing issues before they occur.

MISCONCEPTION #4: IT SERVICES ARE JUST ABOUT FIXING PROBLEMS

While it's true that I.T services help fix technical issues, they also focus on proactive solutions. This includes things like monitoring network performance, updating software, implementing security protocols, and strategizing technology to support the business's goals. IT services are meant to keep systems running smoothly, avoid issues before they arise, and ensure that technology aligns with a business's long-term objectives.