



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



Choosing A Consultant

This Business Advisory Guide Will Arm You With 20 Critical Questions You Should Ask Any I.T. Consultant or Company Before Giving Them Access To Your I.T. Systems.

Choosing the wrong I.T. consultant to support your network can be incredibly frustrating and expensive and could end up costing you downtime, data loss, and expensive repair bills, not to mention the headaches and frustration!

Read this guide, and you'll discover:

- ❑ The “dirty little secret” of the I.T. support industry that most people don't know and will never be told by their I.T. guy (this will surprise you).
- ❑ 20 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.



From The Desk of: Leah Freiman
CEO, ItCon, Inc.



Dear Colleague,

Choosing a computer support company isn't easy. There is no shortage of horror stories about incompetent computer repair “gurus” bungling jobs and causing MORE problems as a result of their loose morals or gross incompetence. I'm sure if you talk to your own friends and colleagues you will get an earful of the unfortunate experiences they have encountered in this area.

Why is this? Because the computer repair and consulting industry, along with a lot of other industries, has its own share of incompetent or unethical businesses that will try to take advantage of trusting business owners who simply do not have the ability to determine whether or not the technician knows what they are doing. Sometimes this is out of greed for your money, but more often it's simply because they don't have the skills and competency to do the job right, but won't tell you that up front. 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.

Buyer Beware: The Computer Repair And Consulting Industry Is NOT Regulated

Here's an embarrassing (and little-known) fact about my industry: it is not regulated like many other professional service industries, which means ANYONE can claim they are a “computer repair expert.” **In fact, a lot of the businesses in this industry started because the owner was FIRED or laid off from their job and couldn't find work anywhere else. That means many of the so-called experts are useless and make sleazy auto repair shops look like the pinnacle of virtue and competence.**

Automotive repair shops, electricians, plumbers, lawyers, realtors, dentists, doctors, accountants, etc., are heavily regulated to protect the consumer from receiving substandard work or getting ripped off. However, the computer industry is still highly unregulated, and there



A Letter From The Author

aren't any laws in existence to protect the consumer – **which is why it's so important for you to arm yourself with the information contained in this report.**

Anyone who can hang out a shingle can promote themselves as a computer expert. Even if they are honestly *trying* to do a good job for you, their inexperience can cost you dearly in your network's speed and performance or in lost or corrupt data files. That is why we decided to offer this report. The information in this guide is provided to help raise standards within the computer repair and support industry and to give YOU useful information to help you guard against the lack of ethics or incompetence of some companies and technicians.

Dedicated to serving you,

Leah Green



About The Author

ItCon's success as a leading IT and Cybersecurity company is driven by Leah Freiman's passion for helping people. Before Leah founded ItCon, she worked as a mortgage broker and taught music on the side. Her love of helping others played itself out in both jobs. As a mortgage broker, Leah took clients with bad credit and debt and helped them get loans with low taxes and closing costs. As a music teacher, she used her skills to help 'special' children expand their capabilities and find joy in music.

On a professional level, her passion is to help companies thrive by overcoming issues that could undermine all their best efforts to succeed. In working closely with the clients of the computer repair company she formed with her husband, the destructive power of cybercrime became dramatically and drastically evident. More and more companies around the globe were falling prey to aggressive cyber attacks. The financial damage and loss of business were insufferable. Leah Freiman applied her energy, drive, and focus on creating a company that would provide clients with all-encompassing tools and tactics needed to secure the future for numerous clients successfully.

Leah Freiman is a recognized expert in the cybersecurity industry. She provides cybersecurity training for many large organizations, has been called upon to deliver a presentation to the NYSii in Albany, has lectured at Touro College, and is the founder of ITCON2019, the Premier Cybersecurity Conference for Business Owners. ItCon was ranked #17 on the MSP501 list and #723 on the Inc5000 list in 2021. ItCon is also on the MSSPAAlert Top 250 MSSPs and CRN MSP500 list. Leah starred in the movie Cyber Crime, a documentary film that explores the world of cybercrime and how you can avoid becoming a victim. She is also the author of "Double Your Revenue with the Right Technology," an Amazon bestseller that teaches business owners how technology can help them grow rather than add business expense.

ItCon represents her passion for creating awareness and providing solutions for companies looking to grow their business with the right technology and fighting cybercrime activities.



20 Questions You Should Ask Your I.T Services Company or Consultant Before Hiring Them To Support Your Network

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: 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 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. Not only can you reach our after-hours support any time and any day, we GUARANTEE to have a technician working on a problem within 60 minutes or less of your call. This is written into every service agreement we give to our clients because it’s standard procedure.

Q3: 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. Our written, guaranteed response time is 60 minutes 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?

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 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.

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.

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.)

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.



20 Questions

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.

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 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.



20 Questions

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 more often) to provide a "technology review."

In these meetings, we provide you with the status updates of projects you're working on and of the health and security of your network. We also make recommendations for new equipment and upgrades you'll be needing soon or sometime in the near future. Our quarterly meetings with you are C-level discussions (not geek-fests) where we openly discuss your business goals, including your 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.

Q12: If I need or want to cancel my service with your, 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.

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?”

Q14: How do you lock down your 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

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: 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.

Backups and Disaster Recovery:

Q16: 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-premises 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.



4 Costly Misconceptions

Q17: 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.

18: 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.

All clients receive a simple disaster recovery plan for their data and network. We encourage them to do a full disaster recovery plan for their office, but at a minimum, their network will be covered should something happen.



Q19: Do they INSIST on monitoring an offsite as well as an onsite backup, or are they letting you rely on outdated tape backups?

Our Answer: We do not allow our clients to use tape backups because they are incredibly unreliable. We make sure all of our clients have a reliable and secure backup – onsite and offsite.

Q20: Do they insist on backing up your network BEFORE performing any type of project or upgrade?

Our Answer: We do, and that's simply as a precaution in case a hardware failure or software glitch causes a major problem.

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 disaster; but that's similar to 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, running fast, and problem-free. In fact, it's surprising how fast a brand-new PC will slow down after a few weeks of use without proper updates and maintenance. 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
- ❑ Antivirus updates and monitoring
- ❑ Firewall updates and monitoring
- ❑ Backup monitoring and test restores
- ❑ Spam-filter installation and updates
- ❑ Spyware detection and removal
- ❑ Monitoring disk space on workstations and servers



5 Mistakes To Avoid

- ❑ Monitoring hardware for signs of failure
- ❑ Optimizing systems for maximum speed

Your computer network is just like a car: if you don't change the oil, replace the filter, rotate the tires, flush the transmission and perform other regular maintenance on your car, it will eventually break down and cost you FAR MORE to repair than the cost of the basic maintenance – and a car is far simpler than a computer network!

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

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

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 neighbor, friend, or relative who was just trying to help.

If the person you have working on your machine does not do computer repair and 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 computer 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 technician, 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.

As we stated a moment ago, you get what you pay for. A cheap price usually means a cheap job. Really good technicians do



5 Mistakes To Avoid

NOT work cheap because they are in high demand, just like every other professional service category. The only technicians that will work cheap are those who are just starting, and they are grossly inexperienced.

And some shops will hire college kids or newbie technicians because they will work for next to nothing to gain experience, OR they allow interns to support your network because they don't have to pay them at all – ***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:
3. 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!
4. 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!
5. 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



Five mistakes to avoid

do this to you!

With your client data, accounting records, email, 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 15 years and have customers 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.



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, not too big, and not too small.

#3: Choosing a computer consultant without speaking to several of their current clients.

A Final Recommendation...

I hope you have found this guide to be helpful in shedding some light on what to look for when outsourcing the support of your company's network. 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 have any additional comments or questions, we welcome them! Have an idea to make this guide even more helpful? Let us know! And, of course, 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.

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...



FREE Network Health Check

We will 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.)

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 15 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.



Looking forward to your call!

Dedicated to your peace of mind,

Leah Freiman

Leah Freiman

Phone: 845.738.1661

Web: www.itconinc.com

Why Should You Care About This?

Because there are literally dozens of ways hackers and viruses can – undetected – gain access to and remotely control your network, corrupt your data and use your network as a conduit for spreading spam, viruses, and even illegal software.

There are numerous system checks and updates that should be done on a regular basis to ensure maximum speed, performance, and security. Ignore them, and your system will get progressively slower, more unstable, and susceptible to viruses, spyware, and hackers.

Tape backups have a failure rate of 100% – that means all tape drives will fail at some point, often without warning. You don't want to find out that your backup was not working the day after your hard drive fried.

To claim this offer, just call me at 845.738.1661, or shoot me an email at lfreiman@itconinc.com.

I am looking forward to hearing from you!





14 N. Madison Avenue, #201, Spring Valley, NY 10977
845.738.1661 | fax: 845.738.1662

www.itconinc.com

We win together or we win together, there is no other way!