Centrend

21 CRITICAL CYBERSECURITY QUESTIONS

2026 Edition

A Free Education Guide By: Centrend, Inc. | www.centrend.com | 774-241-8600

Start

What Every Business Owner **Must** Know About Choosing an Honest, Competent, Responsive, and Security-First **IT Partner**

This Business Advisory Guide Will Equip You With
21 Critical Questions
you should ask any
IT provider
Before giving them access to your systems, users, and data.

Read this guide and you'll discover:

- The Support Standards you should expect response times, ownership and reporting
- The Questions that Expose Weak IT fast
- What Managed IT should include in 2025
- How Modern Attacks happen and how to reduce risk
- How to Judge Backups and recovery with proof, not promises

From the desk of: **Paul LaFlamme**
CEO & Founder
Centrend, Inc.

Dear Fellow Business Owner or Executive,

Choosing an IT provider should not feel like a gamble. But for many businesses, it does.

The problem is simple: the wrong IT partner creates chaos. Slow responses. Constant “urgent” issues. Surprise invoices. Weak security. And no clear plan.

It gets worse in 2025. Attacks do not wait for a convenient time. Phishing, account takeover, and ransomware hit fast. One missed update or one compromised login can shut down operations, disrupt your team, and cost far more than the monthly IT fee.

Most business owners only learn the truth after the damage is done. When support disappears. When backups do not restore. When no one can clearly explain what happened or what to do next.

T**hat is why we created this guide.**

These 21 questions help you quickly spot the difference between a real managed IT partner and a “break-fix” provider with good marketing.

You will learn what to ask, what proof to request, and what red flags to take seriously before you hand over access to your systems and data.

IT is not a regulated profession. Anyone can call themselves an expert. This guide helps you protect your business by raising the standard, demanding accountability, and choosing support that is competent, responsive, and security-first.

Dedicated to serving you,

Paul LaFlamme

The Vision of Centrend

> **It's not just about the tech itself, it's about finding the right tools and keeping your systems secure, because the best tech in the world is useless if it's unsafe.**

Paul LaFlamme is the President and Founder of Centrend, Inc.

In 2025, most IT pain is not “random.” It is predictable. Slow support. Surprise costs. Weak security. Backups that fail when you need them most.

One missed update or one stolen login can turn into downtime, lost revenue, and a stressful recovery. Many businesses only find out their IT provider is not ready after something goes wrong.

Centrend delivers proactive managed IT services, consulting, and cybersecurity support so businesses stay stable, secure, and productive. Based in Central Massachusetts, Centrend supports customers across New England and also works with companies in other regions, including the Midwest and Florida.

Paul and the Centrend team focus on one outcome: IT that supports real business goals, with clear standards, plain language, and consistent follow-through.

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

Customer Service:

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

Our Answer: When something breaks, the worst outcome is confusion. No clear path, no ticket, no ownership, and your issue gets lost in someone's inbox.

That is why every request should create a tracked ticket. A ticket is how we assign the right person, set priority, document the work, and close the loop with you. It also gives you a history you can reference later.

A portal is helpful, but it should not be your only option. In 2025, support needs to be easy and fast. We provide multiple ways to reach us (phone, email, and portal), and every request is logged so nothing gets missed.

What this protects you from: "I never saw your email," slow follow-ups, and repeat problems that never get properly documented.

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

Our Answer: Problems and attacks do not wait for business hours. Nights and weekends can turn small issues into downtime.

We provide after-hours emergency support with clear response targets. If you are down, locked out, or facing a security incident, you will reach a live person fast.

We define what counts as an emergency, how to contact us, and response times in writing.

What this protects you from: being stuck until Monday or losing critical time.

To Request Your FREE Assessment, please visit www.centrend.com or call our office at 774-241-8600.

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

Our Answer: If response time is not in writing, it is not real. When problems hit, vague promises turn into delays.

We provide written response targets based on priority, and we track them. You should be able to see ticket history, response times, and resolution trends, not just hear "we're on it."

What this protects you from: being stuck behind other clients, slow follow-ups, and problems that drag on with no accountability.

Q4 Will I be given a dedicated account manager?

Our Answer: Without an owner, IT gets messy. You repeat yourself and issues drag on.

You get a dedicated contact who owns follow-through. Support handles tickets; your account manager sets priorities.

What this protects you from: confusion and "no owner" problems.

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 a provider will not show feedback, they may be hiding it. In 2025, service quality should be measured.

We collect quick post-ticket feedback and share trends, because we expect to be held accountable. What this protects you from: bad service that never gets fixed.

I.T. Maintenance (Managed Services):

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

Our Answer: Break-fix reacts. Managed IT prevents. Managed services cover monitoring, patching, security hardening, and reviews. If a provider only reacts, you pay in downtime. What this protects you from: fire drills, outages, and security gaps. somewhere else.

To Request Your FREE Assessment,
please visit www.centrend.com or call our office at 774-241-8600.

Our 24/7 monitoring watches your network and key systems for early warning signs, security threats, and performance issues so we fix them fast BEFORE they become major outages, breaches, or big downtime.

Q7 What is NOT included in your managed services agreement?

Many I.T. firms surprise you with what is NOT included and what triggers extra invoices. In 2025, "all you can eat" is rarely unlimited, so get the limits in plain writing before you sign.

Projects are often excluded (new users, office moves, server/firewall upgrades, and new hardware or licenses). You should know this upfront, before go-live.

Here's the question that matters most: If If you face ransomware, account takeover, or a serious breach, is incident response and recovery **INCLUDED** or **EXTRA**? Containment, cleanup, and restores can take **HOURS** of senior-level I.T. work. Who pays for that time? Get this in writing before you sign. Surprise crisis bills are unacceptable. Confirm what is covered, billable, and capped upfront..

Other things to inquire about are:

- Scope and "extra fees": Is support for business apps, internet/VoIP, printers, vendors, Microsoft 365, and Google Workspace included, or billable? In 2025, your IT partner should own the issue and coordinate with vendors, not point fingers.
- Help desk and coverage: Is help desk truly unlimited, or capped by users/calls? Are on-site visits, remote sites, and remote-work support (home vs company devices) included? Get it in writing.
- Crisis costs: If you face ransomware or a serious breach, is incident response and recovery **INCLUDED** or **EXTRA**? Who pays for hours of cleanup and restores, and are rates/caps defined upfront?

Q8 Is your help desk local or outsourced?

Our Answer: If your help desk is outsourced, you may get someone who does not know your environment, your users, or your standards. That can mean slower fixes, more handoffs, and more risk. Ask who answers your calls, where they are, how they are trained, and how tickets escalate to your dedicated team.

To Request Your FREE Assessment,
please visit www.centrend.com or call our office at 774-241-8600.

Whenever possible, we assign a dedicated technician to your account. They learn your environment, your users, and your priorities, so issues get resolved faster and more consistently.

Fortunately, we assign a dedicated technician to your account who learns your business, your preferences, and your history. With a consistent local help desk contact, issues get resolved faster, handled the way you want, and you are not starting from scratch every time.

Q9 How many engineers do you have on staff?

Our Answer: Be careful with one-person I.T. shops or tiny firms that outsource core support. People get sick, go on vacation, or get pulled into emergencies. If there is no bench, you are stuck waiting.

ALSO: We maintain coverage so support continues even when a primary tech is out. That means more than one trained engineer can step in, follow standards, and keep work moving.

Also: We document changes, fixes, access, and history. So if someone steps in, they are not guessing, and they do not "learn your network" by trial and error.

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

Our Answer: Network documentation is the blueprint of your environment. It should include devices, key settings, user/admin access, network layout, vendors, licenses, and how core systems are set up and secured. We keep documentation in a secure system and update it regularly. You should receive it in a usable format, without extra fees, because it is your environment.

Why is this important? There are several reasons:

First, it shows professionalism and accountability in **protecting YOU**. No I.T. provider should be the only holder of the keys. Because we document your assets and access, you have a clear blueprint you can hand to another trusted team if needed.

Second, good documentation helps engineers resolve issues faster and safer. They are not guessing, hunting for settings, or uncovering accounts, hardware, and licenses the hard way.

Third, if you ever need to restore after a disaster, strong documentation gives you the blueprint to rebuild fast and correctly.

All clients receive documentation in written and electronic form at no extra cost. We also review and update it quarterly, and we make sure the right people on your team know where it is and how to use it, so you stay in control of your network.

Side note: You should never allow an I.T. provider to have total control over your company. If your current provider is holding passwords or access hostage, that is a serious risk. We can help you regain control safely, so you are not left with hidden "side effects." Do not tolerate it.

Q11 Do you meet with your clients quarterly as part of your managed services agreement?

Our Answer: If you only talk to your I.T. provider when something breaks, you are already behind. Quarterly reviews prevent surprises and keep your tech aligned with your business.

We meet at least quarterly (often more) to review current projects, network health, and security status. We also bring recommendations for upcoming upgrades and risk reduction.

These are business-focused meetings. We discuss goals, budget, priority projects, compliance needs, known issues, and practical cybersecurity steps.

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

Our Answer: Long lock-ins and cancellation penalties are a red flag. If a provider has to trap you, service quality is not the reason you stay.

We make cancellation straightforward. If you ever choose to leave, we provide a clean offboarding process: documentation handoff, credential transfer, and an orderly transition with no drama.

Our goal is simple: earn your business every month by being responsive, consistent, and worth keeping.

Cyber Security:

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

Our Answer: Anyone can claim they do cybersecurity. Certifications are not everything, but they show commitment to standards, training, and staying current.

Ask what certifications they maintain, how often training is renewed, and who handles incident response, cloud security, and compliance. A solid provider will answer clearly and show proof. If they cannot, ask: “Who is protecting us, and are they keeping up?”

Q14 How do you lock down our employees’ PCs and devices to ensure they’re not compromising our network?

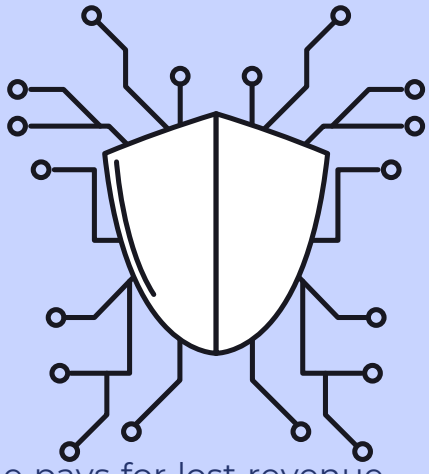
Our Answer: Most breaches start at the endpoint. If devices are not hardened, patched, and monitored, you are exposed.

- Phishing-resistant MFA for key systems and admin access
- EDR (modern threat detection and response), not just basic antivirus
- Automated patching for OS and common apps
- Device encryption and safe configuration baselines

A provider should be able to explain their standard build, how they monitor risk, and what happens when a device shows signs of compromise.

Q15 What cyber liability and errors and omissions insurance do you carry to protect me?

Our Answer: If your IT provider makes a mistake or mishandles a security event, you should not be left holding the bill.



Ask what insurance they carry (cyber liability and errors & omissions), what it covers, and request a current certificate of insurance. Also ask about coverage limits, key exclusions, and whether business interruption and incident response costs are included. If they manage sensitive systems or data, this matters even more.

If ransomware hits due to their negligence, someone pays for lost revenue, recovery, and downtime. If they do not carry coverage that can pay for business interruption and related losses, they may not be able to make you whole. Then you are left chasing costs when you should be restoring operations, especially if sensitive data is involved.

To Request Your FREE Assessment,
please visit www.centrend.com or call our office at 774-241-8600.

If client data is compromised, who pays the fines, notification costs, legal fees, and damages? No one is perfect. That is why your I.T. provider must carry proper insurance.

True story: A few years ago, a company (name withheld) was hit with multiple lawsuits after customers' data was exposed due to technician mistakes. In some cases, technicians accessed customer PCs and laptops for repairs, then lost a device or mishandled data, causing an exposure. The lesson is simple: make sure your I.T. firm carries the right coverage to **protect YOU.**

Rest assured, we carry the insurance needed to protect our clients, and we are happy to provide proof of coverage.

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

Our Answer: Nobody should "grade their own work." A professional I.T. firm should have independent third-party review of their cybersecurity practices.

Ask who audits them, how often, and when the last audit occurred. If they cannot answer clearly, refuse to share proof, or have not been reviewed in a long time, do not hire them. That is a sign they are not taking security seriously.

Q17 Do you have a SOC and do you run it in-house or outsource it? If outsourced, what company do you use?

Our Answer: A SOC (Security Operations Center) monitors systems for threats, investigates suspicious activity, and helps respond quickly when incidents occur.

Here is the key: not every I.T. firm can run a SOC in-house. Some outsource, and that can be fine if the provider is credible and response is clear. What matters is what you actually get: 24/7 monitoring, escalation, and real response support, not just alerts.

Basic monitoring is not security. Ask who watches, what tools they use, what happens after hours, and what the response process looks like in writing.

To Request Your FREE Assessment, please visit www.centrend.com or call our office at 774-241-8600.

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.

Q18 *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.

To Request Your FREE Assessment, please visit www.centrend.com or call our office at 774-241-8600.

important if you host sensitive data (financial information, medical records, credit cards, etc.) and fall under regulatory compliance for data protection.

Rest assured, we do everything to provide proactive security monitoring for our clients to better prevent a network violation or data breach.

Backups And Disaster Recovery:

Q19 *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.

Q20 *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

That's why you want to ask your prospective I.T. consultant how quickly they were able to get their clients working remotely (and securely) when Covid shut everything down. Ask to talk to a few of their clients about how the process went.

Q21 *Show me your process and documentation for onboarding me as a new client.*

Our Answer: The reason for asking this question is to see if they HAVE SOMETHING in place. A plan, a procedure, a process. Don't take their word for it. Ask to SEE it in writing. What's important here is that they can produce some type of process. Further, they should be able to explain how their process works.

One thing you will need to discuss in detail is how they are going to take over from the current I.T. company – particularly if the current company is hostile. It's disturbing to me how many I.T. companies or people will become bitter and resentful over being fired and will do things to screw up your security and create problems for the new company as a childish way of getting revenge. (Sadly, it's more common than you think.) A good I.T. company will have a process in place for handling this.

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

Other Things To Notice And Look Out For:

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.

Paul and his team are true professionals. They respond quickly to any and all questions. When they say they'll be there, you can count on them being there. I highly recommend them.

– Marco Schiavo, Attorney, Simmons & Schiavo, LLP

To Request Your FREE Assessment, please visit www.centrend.com or call our office at 774-241-8600.

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.

Do they have expertise in helping clients similar to you?

Do they understand how your business operates the line-of-business applications you depend on? Are they familiar with how you communicate, get paid, service your clients or patients and run your business? We have several clients.

The 4 Most Costly Misconceptions About I.T. Services

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

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

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

- Cyber security patches, updates and management
- Antivirus updates and monitoring
- Firewall updates and monitoring

To Request Your FREE Assessment, please visit www.centrend.com or call our office at 774-241-8600.

- Backup monitoring and test restores
- Spam-filter updates
- Operating system updates, management
- Monitoring hardware for signs of failure

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

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

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

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

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

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

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

1. They are a small shop just getting started. Usually they will have only one to two techs working for them (or they are a solo shop). That size of company may be perfectly fine for a small business that is not regulated, doesn't have sophisticated I.T. requirements and/or has only 10 or fewer PCs to support. This would not be a good choice for a larger organization that needs professional I.T. services for their growing company.

2. They are hiring inexperienced (cheap) college kids or newbie technicians because they will work for next to nothing, OR they allow interns to support your network because they don't have to pay them at all – but what you don't realize is that an inexperienced technician like this can end up costing more because:

- They improperly diagnose problems, which means you're paying them to fix the wrong thing and they still won't resolve your issue. Case in point: A few years ago a TV reporter went undercover to I.T. services companies in LA with a perfectly working PC, but simply disconnected a cable in the back (a fix that the average tech would have caught in minutes with a visual inspection). Several shops improperly diagnosed the problem and wanted to charge them up to $275 to fix it!
- They could take three to five times as long to do the same repair an experienced technician could fix quickly. Again, you're paying for those extra hours AND you're frustrated and unproductive while you wait for the SAME problem to be fixed!
- They could do things that put your security and data in jeopardy. True story: An inexperienced engineer of a competitor turned off all security notifications his client's network was producing because it was "too much work" to sift and sort through them. Because of this, the company got hacked and ended up having to pay a ransom to get their data back, not to mention suffered downtime for days while they scrambled to recover. Don't let a cheap, inexperienced tech do this to you!

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

We take the view that most people want value for their money and simply want the job done right. You will find that we are not the cheapest, but we don't apologize for that. As the owner, I decided a long time ago that I would rather explain our higher rates ONE TIME than make excuses for POOR SERVICE forever. That said, we're not the most expensive either. We simply feel that we should offer a good service at a fair price. That's why we have been able to stay in business for over 17 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.

To Request Your FREE Assessment, please visit www.centrend.com or call our office at 774-241-8600.

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

1 Ask to speak to several of their current clients.

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.

2 Look for a company that Responsive & Reliable

When you experience problems with technology, you want the most reliable service, however, you also want things to get fixed as soon as possible because time is money! So how do you make sure that the company you choose will be providing fast reliable and effective services? Ask questions! How fast do you typically respond to issues? How quickly are issues resolved? How long will it take if you need onsite support?

3 Choose an I.T. consultant who experience is knowledge

The technology that your business uses will vary depending on the industry. It is wise to choose a provider that knows about your particular industry technologies and has worked with them before. The best way to determine this is to find out if they service any other company in your industry, or if they are certified for particular industry technologies. This will ensure that they will be comfortable handling any problem that you might have.

To Request Your FREE Assessment, please visit www.centrend.com or call our office at 774-241-8600.

A Final Recommendation

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

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

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

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

Here's how this works...

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

To Request Your FREE Assessment, please visit www.centrend.com or call our office at 774-241-8600.

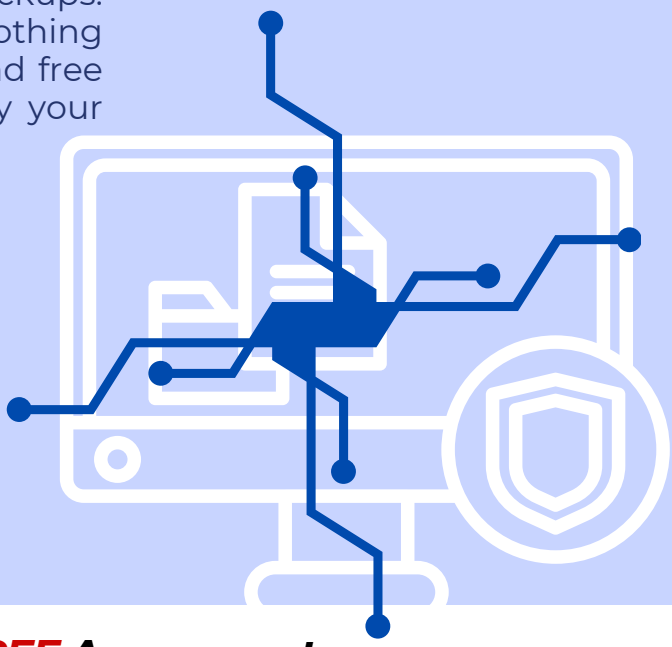
Your current I.T. company or team **DOES NOT NEED TO KNOW** we are conducting this assessment, or we can involve them. (The choice is yours, but we recommend NOT letting them know this inspection is happening so we can get a truer read of how secure you are. After all, the cybercriminals won't tip you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

Your time investment is minimal: 15 mins 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 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.

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.)

After doing this for more than 17 years, I can practically guarantee I will find significant and preventable security loopholes in your network and problems with your backups. Like Sherlock Holmes, we never fail. If nothing else, our Risk Assessment is an easy and free way to get a valid third party to verify your security and give you peace of mind.



Dedicated to your peace of mind.

Paul LaFlamme, CEO/President
Centrend, Inc.

To Request Your FREE Assessment, please visit www.centrend.com or call our office at 774-241-8600.