Buyer's Guide To Finding Great IT Support For Your Business

This Business Advisory Guide Will Arm You With 15 Critical Questions You Should Ask Any IT Consultant Or Company Before Trusting Them With Your IT Systems

Their answers will reveal whether they prioritize excellence, security, availability, customization and accountability.

Read this guide and you'll discover:

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

From the Desk of Bill Hogan

Owner and President of Partners Plus, Inc.

Hi, my name is Bill Hogan and I'm the President of Partners Plus Inc. We have specialized in solving problems for other entrepreneurs since 1991—more specifically, technical problems and cybersecurity risks.

This is, of course, only one small part of the day-to-day issues you deal with as a business owner, but I think you'll agree that IT problems can be some of the most aggravating and expensive issues you run into.

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

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

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

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

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

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

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

It's about time the right level of support was made available. Since 1991, we have committed ourselves to delivering fast, affordable computer support from a professional and reliable team to small- and medium-sized businesses in the Delaware Valley

I thought you would find this material useful. Inside, there's information to help you better understand who we are and how we can best help your business succeed. If you're interested in partnering with us, I look forward to meeting with you!

We make IT great; you make your business great.

About The Author

Back in the early 1990s, I realized how badly businesses needed a support company that knew what they were doing and looked at partnering with their clients to give them an exceptional value-added relationship.

This relationship wouldn't be based on being the mechanic who runs around fixing broken things but rather would focus on preventing the things from breaking in the first place. I did this because I appreciated how frustrating it is for companies to have outages that affect their relationships with their customers and employee morale – not to mention the costs associated with staff who can't work. To that end, our focus is on being proactive, education-focused (both for ourselves and our clients) and is both friendly and efficient in addressing issues to help you minimize downtime and improve productivity.

Our team approach starts with a real person answering the phone and moves into a friendly, professional environment focused on addressing the challenge and resolving it as quickly and painlessly as possible (while minimizing the impact of both the problem and the solution). As our company has grown and evolved with the times, we have been able to increase our offered services. You can now not only get managed IT services with Partners Plus but also a Business Phone System solution and a Security Package. All of our services aid both security and productivity! We are proud to currently serve over 500 users spanning 30+ businesses on the East Coast.

Comparing Apples to Apples: The Predominant IT Service Models Explained

Before you can accurately compare the fees, services, and deliverables of one IT services company with another, you need to understand the three predominant service models most of these companies fit within. Some companies offer a blend of all three, while others are strict about offering only one service plan. The three predominant service models are:

- **Time and Materials.** In the industry, we call these "break-fix" services. Essentially you pay an agreed-upon hourly rate for a technician to "fix" your problem when something "breaks." Under this model, you might be able to negotiate a discount based on buying a block of hours. The scope of work may be simply to resolve a specific problem, like fixing a problem with your e-mail, or it may encompass a large project, like a network upgrade or move that has a specific result and end date clarified. Some companies will offer staff augmentation and placement under this model as well.

- **Managed IT Services.** This is a model where the IT services company takes the role of your fully outsourced "IT department" and not only installs and supports all the devices and PCs that connect to your server(s), but also offers phone and on-site support, antivirus, cyber security, backup, and a host of other services to monitor and maintain the health, speed, performance, and security of your computer network.

- **Software Vendor-Supplied IT Services.** Many software companies will offer IT support for their customers in the form of a help desk or remote support for an additional fee. However, these are typically scaled-back services, limited to troubleshooting their specific application and NOT your entire computer network and all the applications and devices connected to it. If your problem resides outside of their specific software or the server it's hosted on, they can't help you and will often refer you to "your IT department." While it's often a good idea to buy some basic-level support package with a critical software application you use to run your business, this is not enough to provide the full IT services and support most businesses need to stay up and running.

When looking to outsource your IT support, the two service models you are most likely to end up having to choose between are the "managed IT services" and "break-fix" models. Therefore, let's dive into the pros and cons of these two options, and then the typical fee structure for both.

Managed IT Services Vs. Break-Fix: Which Is the Better, More Cost-Effective Option?

You've probably heard the famous Benjamin Franklin quote, "An ounce of prevention is worth a pound of cure." I couldn't agree more – and that's why it's my sincere belief that some form of managed IT is essential for every small business.

At Partners Plus, we offer a total of seven membership levels, all with customizable features, in order to fit the needs of our clients. In some cases, where the business is small, we might offer a very basic managed services plan to ensure the most essential maintenance is done, then bill the client hourly for any support used. But for some of our midsize organizations, we offer a fully managed approach where more comprehensive IT services are covered in a managed plan. By doing this, we can properly staff for their accounts and ensure they get the fast, responsive support and expertise they need.

The only time I would recommend a "time and materials" approach is when you already have a competent IT person or team proactively managing your computer network and simply have a specific IT project to complete that your current in-house IT team doesn't have the time nor expertise to implement (such as migrating to a cloud-based solution, implementing a cyber security plan, etc.). Outside of that specific scenario, I do not think the break-fix approach is a good idea for general IT support for one very important, fundamental reason: you'll ultimately end up paying for a pound of "cure" for problems that could have easily been avoided with an "ounce" of prevention. That said, we do have a small number of clients currently, where this fits their needs. We also have clients in higher-level memberships that have an IT guy on staff that we work with!

Why Regular Monitoring and Maintenance Is Critical For Today's Computer Networks

The fact of the matter is computer networks absolutely, positively need ongoing maintenance and monitoring to stay secure. The ever-increasing dependency we have on IT systems and the data they hold – not to mention the *type* of data we're now saving digitally – has given rise to very smart and sophisticated cybercrime organizations that work around the clock to do one thing: hack into your network to steal data or money or to hold you ransom.

As you may know, ransomware is at an all-time high because hackers make millions of tax-free dollars robbing one small business owner at a time. But that's not their only incentive.

Some will attempt to hack your network to gain access to bank accounts, credit cards or passwords to rob you (and your clients). Some use your computer network to send spam using YOUR domain and servers, host pirated software, and, of course, spread viruses. Some even do it just for the "fun" of it.

And don't think for a minute these cybercriminals are solo crooks working alone in a hoodie out of their basement. They are highly organized and well-run operations

employing *teams* of hackers who work together to scam as many people as they can. They use advanced software that scans millions of networks for vulnerabilities and use readily available data on the dark web of YOUR usernames, passwords, e-mail addresses, and other data to gain access.

Of course, this isn't the only IT danger you face. Other common "disasters" include rogue employees, lost devices, hardware failures (still a BIG reason for data loss), fire and natural disasters and a host of other issues that can interrupt or outright destroy your IT infrastructure and the data it holds. Then there's regulatory compliance for any business hosting or touching credit card or financial information, medical records, and even client contact information such as e-mail addresses.

Preventing these problems and keeping your systems up and running (which is what managed IT services is all about) is a LOT less expensive and damaging to your organization than waiting until one of these things happens and then paying for emergency IT services to restore your systems to working order (break-fix).

Should You Just Hire a Full-Time IT Manager?

In most cases, it is not cost-effective for companies with under 100 employees to hire a full-time IT person for a couple of reasons.

First of all, no one IT person can know everything there is to know about IT support and cyber security. If your company is big enough and growing fast enough to support a full-time IT lead, you probably need more than one guy. You need someone with help-desk expertise as well as a network engineer, a network administrator, a CIO (chief information officer), and a CISO (chief information security officer).

Therefore, even if you hire a full-time IT person, you may still need to supplement their position with co-managed IT support using an IT firm that can fill in the gaps and provide services and expertise they don't have. This is not a bad plan; what IS a bad plan is hiring one person and expecting them to know it all and do it all.

Second, finding and hiring good people is difficult; finding and hiring skilled IT people is incredibly difficult due to the skill shortage for IT. And if you're not technical, it's going to be very difficult for you to interview candidates and sift and sort through all the duds out there to find someone with good skills and experience. Because you're not technical, you might not know the right questions to ask during the interview process or the skills they need to do the job.

More often than not, the hard and soft costs of building an internal IT department for general IT support just don't provide the best return on investment for the average small to midsize business. An internal IT department typically doesn't make sense until you have closer to 100 employees OR you have unique circumstances and need specialized skills, a developer, etc., but not for day-to-day IT support and maintenance.

Why "Break-Fix" Works Entirely in the Consultant's Favor, Not Yours

Under a "break-fix" model, there is a fundamental conflict of interests between you and your IT firm. The IT services company has no incentive to prevent problems, stabilize your network or resolve problems quickly because they are getting paid by the hour when things stop working; therefore, the risk of unforeseen circumstances, scope creep, learning curve inefficiencies, and outright incompetence are all shifted to YOU, the customer. Essentially, the more problems you have, the more they profit, which is precisely what you DON'T want.

Under this model, the IT consultant can take the liberty of assigning a junior (lower-paid) technician to work on your problem – one who may take two to three times as long to resolve an issue that a more senior (and more expensive) technician might resolve in a fraction of the time. There is no incentive to properly manage the time of that technician or their efficiency, and there is every reason for them to prolong the project and find MORE problems than solutions. Of course, if they're ethical and want to keep you as a client, they *should* be doing everything possible to resolve your problems quickly and efficiently; however, that's akin to putting a German shepherd in charge of watching over the ham sandwiches. Not a good idea.

Second, it creates a management problem for you, the customer, who now has to keep track of the hours they've worked to make sure you aren't getting overbilled, and since you often have no way of really knowing if they've worked the hours they say they have, it creates a situation where you really, truly need to be able to trust they are being 100% ethical and honest AND tracking THEIR hours properly (not all do).

And finally, it makes budgeting for IT projects and expenses a nightmare since they may be zero one month and thousands the next.

The Questions:

1. What **guarantees** on your services do you offer?

We're proud to offer SEVEN! Here is the list:

- **Ticket Guarantee**: Depending on your ticket and membership level, if we do not respond within the guaranteed time frame, we will cover the issue for free.

Regular Tickets	Within one business day (Mon-Fri, 8am-5pm)
Priority Tickets for Silver & Gold Members	Within one hour, 7x24x365
Priority Tickets for Bronze Members	Within one business hour

- **Money Back Guarantee**: If you're not convinced our services are worth every penny within 90 days, we'll refund you in full.
- **Service Guarantee**: If you're ever dissatisfied with any service from us, let us know within 72 hours or before another ticket (whichever's first). We'll immediately correct the service at no additional charge to you. If this still doesn't resolve the issue, we'll refund 100% of the money you've paid us.
- **It Stays Fixed Guarantee**: If anything we fix, breaks again within 30 days, let us know and we'll fix it, free of charge
- **Ransomware Guarantee**: If you have our Security Package and received a high score on your last QBR, but still get hit with ransom, we will provide free support through the entire recovery process. *Read Q10 for more on our Security Package.*
- **Server Guarantee**: If, within the one-year anniversary of a server install, you decide you no longer want it for any reason, we'll refund every penny of hardware, software and labor expenses associated with the server that you incurred to date.
- **Data Guarantee**: If we can't recover your data after a server crash, we'll refund 100% of the money you've ever paid us for backup services. We'll also provide you up to $25,000 worth of our labor to restore your network.

2. What does the **IT support** process look like?

You can place a ticket for an IT issue a few different ways—email Support@PartnersPlus.com or call/text us at 302-529-3700. Our help desk is live and on-site, so you won't have to deal with an 800-number and lengthy hold times. From there, you can place your ticket as regular or priority. *Refer to our Ticket Guarantee in Q1.* Once resolved to the best of our knowledge, you'll get a "Ticket closed" email. There, you have the option of rating your experience via these three emoticons:

This system is the best way to either leave a kind review or let us know the issue is not resolved! If the latter, we'll get back in touch as soon as we see the review. *See our Service and It Stays Fixed Guarantees in Q1.*

3. How transparent and organized is the **billing process**?

We always offer detailed invoices to explain projects. Projects are finished on budget and at a flat rate cost, so long as the entire project is brought to us up front. Our billing manager is easily accessible if you have any discrepancies or concerns.

4. What is your **onboarding** process?

Our typical process goes as followed:

- We begin with a phone call to discuss your business' size, needs, previous/current IT set up and pain points. This phone call helps us see if we are a good fit for your company! Our clients are small- or medium-sized businesses with a typical emphasis on data security or crucial operations.
- From there, we will conduct an on-site visit. We tour the space and look over your current IT set up. Sometimes, multiple on-site visits are beneficial. At this point, we are generally beginning to work closely with the executive team, IT employees and/or office managers.
- Based on the two previous steps, we will then create a gameplan for your business and suggest the best membership for you. Each membership is customizable, dependent on multiple factors, so you won't overpay for services you don't need. At this point, we begin discussing what could use improving upon…
- We don't rush you as you discuss partnering with us internally. We understand it's an investment, that typically requires discussion to see the importance of our services.
- Then, through your first months of membership, we are heavily involved with execution, implementation and education. From then on out, it's our goal to explain things well to your entire team.

5. Speaking of, are you **good at answering our questions** in terms we can understand and not in confusing "geek speak?"

Yes! We take the time to not only explain things in ways you'll understand, but also stay in conversations until all questions are answered and understood. We often use analogies and real-life examples to help you understand the *why* or *how* at hand. Additionally, we find this to be empowering for our clients. For example, part of the Security Package (*see Q10)* is training and testing all our clients' employees on bad email links and giving them the ability to report phishing attacks!

6. Do you **meet with your clients regularly** as part of your managed services agreement?

Yes! We hold Quarterly Business Reviews (QBR) with our Gold and Silver clients and Biannual Business Reviews with our Bronze clients. These meetings are part of your membership, at no additional charge. We review the overall health and security of your network, your tickets over the last quarter, make suggestions for the upcoming quarter and answer any questions you may have.
We understand that if we're doing our job well, you're not having to contact us frequently. Therefore, what we do may be lost on our clients. At these meetings, we bring you up to speed on all the preventative measures we've been conducting behind the scenes to keep your business up and running.

7. How do you **secure our employees' computers** and devices to ensure they're not compromising our network?

Our top priorities are security and ongoing operations. Therefore, we've spent the last 30 years nailing down a series of Best Practices that ensure your company is safe and productive. Some of these practices are mandatory while others are highly suggested. Because of this, we are able to support hundreds of employees from over 30 companies, from a small team. To learn more, check out the infographic here:

8. Out of necessity or convenience, can you enable clients to work from a **remote location**?

For better or worse, we are now pros at supporting remote work! The majority of our clients worked remotely (including us!) for a time during COVID and still occasionally do so out of convenience or safety. We quickly picked up on common pain points and established an additional set of Best Practices, so remote work can still be secure and productive. Check out some of our advice here:

9. Do you have a **SOC** (security operations center)? Is it in-house or outsourced?

Yes, we outsource it to an incredible vendor in Baltimore. Their team is made up of many NSA alums. They offer AI-based 7x24x365 monitoring for our Security Package clients. *Expanded upon in Q10.*
As the liaison between the SOC and our clients, we attend virtual demos together and can bring up any of our client's concerns to our representative. Then, if they notice something fishy on your network,

we're notified immediately, and we tend to the issue together. You are updated throughout the entire process.

10. Do you offer **additional, enhanced security features** to protect against ransomware?

As mentioned in Q1 and Q9, we have a Security Package that is an optional add-on to your membership. We have taken years to craft an effective stack that protects you from prominent threats. For our budget-conscience clients, we have an EasyData version as well! To learn more, check out our Security Package page online here:

11. What does your **Incident Response Plan** entail and does it include previously tested restores of your **backups**?

Of course, our IRP is dependent on the situation. To put it broadly, it includes priority calls, backups and restorations of servers, and the ability to work virtually/remotely. Everything is backed up to the cloud at the end of every business day, allowing a seamless transition of work locations, if need be. If you use our premium backup service, they're tested nightly, with a report of their success each morning. Our other backup service confirms if the backup is good. Backups occur on a daily basis (hourly is optional), and always include off-site storage as well.

12. Who **audits** <u>your</u> company's cybersecurity protocols and when was the last time they conducted their audit?

This summer, we switched to a new insurance provider, Lloyd's of London, which specializes in MSPs. To onboard, and once a year after (we predict), we fill out an audit questionnaire for them. Based on those responses, they give us a pass/fail and we must fix whatever failed. They also provide us with recommendations.

13. What **cyber-liability** and errors and omissions **insurance** do you carry to protect me?

The same insurance provider *mentioned in Q12* also takes care of these items. We have $2M limits of cyber liability errors & omissions insurance. With our Security Package *mentioned in Q10*, you can utilize the same insurance as us! You'll get better coverage and pricing because we manage what's most important.

14. Do you offer **documentation of our network** as part of our membership?

Yes! Our documentation includes the total number of network devices, printers, servers and workstations. We also provide a breakdown of each workstation's issues and updates. If you ever need to switch IT providers, your replacement company will be able to take over quickly because the network has been documented properly.

15. What is the **contract length**? Additionally, if I need or want to cancel my service with you, how does this happen and how do you **offboard** us?

Our contract length is two years, followed by one-year renewals. *See our Money Back Guarantee in Q1.* Oftentimes, our clients outgrow us and are integrated with larger companies which have their own full-fledged IT department. As sad as we are to lose you as a client, we are also elated for your growth! Regardless of whether you've outgrown us or have decided to move in another direction, we understand! *Per Q13* about network documentation, we aim to make it as smooth a transition as possible. We will pass documentation and all keys off to the necessary personnel, whether that's a new employee or IT company.

The 4 Most Costly Misconceptions About IT Services

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

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

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

- Cyber security patches, updates and management
- 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

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

1. Either they don't know enough to make this recommendation, which is a sure sign they are grossly inexperienced and unprofessional, or…

2. They recognize that they are *profiting* from your IT problems and don't want to recommend steps toward prevention, which would reduce the number of issues they are paying you to resolve.

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

Misconception #2: My nephew/neighbor's kid/brother-in-law/office manager knows this IT stuff and can take care of our network.

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

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

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

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

1. They are a small shop just getting started, and you don't need to be their test subject.

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

- ✓ They improperly diagnose problems, which means you're paying them to fix the wrong thing and they still won't resolve your issue. Case in point: A few years ago a TV reporter went undercover to IT services companies in LA with a perfectly working PC, but simply disconnected a cable in the back (a fix that the average tech would have caught in minutes with a visual inspection). Several shops improperly diagnosed the problem and wanted to charge them up to $275 to fix it!

- ✓ They could take three to five times as long to do the same repair an experienced technician could fix quickly. Again, you're paying for those extra hours AND you're frustrated and unproductive while you wait for the SAME problem to be fixed!

- ✓ They could do things that put your security and data in jeopardy. True story: An inexperienced engineer of a competitor turned off all security notifications his client's network was producing because it was "too much work" to sift and sort through them. Because of this, the company got hacked and ended up having to pay a ransom to get their data back, not to mention suffered downtime for days while they scrambled to recover. Don't let a cheap, inexperienced tech do this to you!

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

We take the view that most people want value for their money and simply want the job done right. You will find that we are not the cheapest, but we don't apologize for that. As the owner, I decided a long time ago that I would rather explain our higher rates ONE TIME than make excuses for POOR SERVICE forever. That said, we're not the most expensive either. We simply feel that we should offer a good service at a fair price. That's why we have been able to stay in business for over 30 years.

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

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

3 More Recommendations To Find A Great IT Company You'll Love

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

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

2. **Look for a company that can show you're the monthly and quarterly reports they will provide to review your network health.** These reports are invaluable in understanding your network and having discussions about how your network can better serve your business.

3. **Choose an IT consultant who is very Best Practices oriented.** When your IT Company is Best Practices oriented – you get a number of benefits, including faster, more reliable systems that are setup, migrated and serviced in less time – all while being more secure. This is a foundation of the services we provide.

A Final Recommendation

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

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

This is completely free, and with no expectations for you to hire us unless you feel that is the right thing for you to do. Here's how this works…

We'll meet by phone (or Zoom) to have a brief conversation about your current situation; what you are frustrated by, looking for in an IT company and any concerns and questions you have. We'll ask you a few questions that you should easily be able to answer. Depending on what we discover, we can move to the next step, which is to conduct a quick, non-invasive, CONFIDENTIAL investigation of your computer network, backups and security protocols.

Your current IT company or team DOES NOT NEED TO KNOW we are conducting this assessment, or we can involve them. (The choice is yours, but we recommend NOT letting them

know this inspection is happening so we can get a truer read of how secure you are. After all, the cybercriminals won't tip you off that they're about to hack you.)

Your time investment is minimal: 30 minutes for the initial phone consultation and one hour in the second meeting to go over what we discover. When this Risk Assessment is complete, here's what you will know:

- If your IT systems and data are truly secured from hackers, cybercriminals, ransomware and even sabotage by rogue employees.
- If your current backup would allow you to be up and running again fast if ransomware locked all your files – 99% of the computer networks we've reviewed failed this test.
- If you and your employees' login credentials are being sold on the dark web right now and what to do about it. (I can practically guarantee they are, due to a recent 8.4 billion credentials being sold on the dark web. What we find will shock you.)
- Answers to any questions you have about a recurring problem, an upcoming project or change or about the service you are currently getting.

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

After doing this for over 30 years, I can practically guarantee I will find significant and preventable security loopholes in your network and problems with your backups. Like Sherlock Holmes, we never fail. If nothing else, our Risk Assessment is an easy and cheap (free) way to get a valid third party to verify your security and give you peace of mind.

How To Request This Free Assessment:

- Go online to: https://www.PartnersPlus.com/Free-Audit
- Call us at 302-529-3700 or 215-774-8980
- E-mail me direct with questions: BHogan@PartnersPlus.com

Dedicated to your peace of mind,

Bill Hogan, President
Partners Plus, Inc.