21

Critical

I.T. Security

Questions

06/06/24
From the Desk of: Zac Abdulkadir
CEO / CISO Netready

Dear Fellow Business Owner or Executive,

Finding the perfect IT partner can make a world of difference for your company's success. They can become a trusted advisor, ensuring your technology runs smoothly and supporting your growth. However, choosing the wrong provider can lead to frustration and lost productivity. With so many IT companies out there, how do you know which one is right for you?

This guide will equip you with the knowledge to make an informed decision. We'll discuss key questions to ask, red flags to watch out for, and the benefits of partnering with a reliable IT firm.

The Value of a Strong IT Partnership:

- Peace of mind: Knowing your data and systems are secure allows you to focus on running your business.
- Increased productivity: Reduced downtime and a proactive approach to IT issues keeps your team working efficiently.
- Strategic IT planning: The right partner can help you leverage technology to achieve your business goals.

Choosing the Right Partner:

This guide will equip you with the knowledge to confidently select an IT partner who aligns with your needs. We'll cover topics such as:

- Understanding your IT requirements.
- Evaluating a provider's experience and expertise.
- Ensuring clear communication and responsiveness.

By taking the time to choose wisely, you can gain a valuable partner who empowers your business to thrive.

Sincerely,

Zac Abdulkadir

About The Author

Meet Zac Abdulkadir, Your Cybersecurity and IT Expert

Zac Abdulkadir, president of Netready, is a cybersecurity leader with over 20 years of experience. He's a trusted advisor for businesses in finance, construction, hospitality, and non-profits, as documented in his bestselling book "Exposed to Secure." Zac even offered his insights into real-world cybercrime investigations for the movie "Cyber Crime Investigations."

Netready is your one-stop shop for all your IT and cybersecurity needs. We offer a comprehensive range of services, including:

- Fortress-like Defenses: We design secure networks, identify vulnerabilities, and implement robust intrusion detection systems.
- Advanced Threat Protection: We stay ahead of the curve, safeguarding your business from the latest cyber threats.
- Insider Threat Management: We help you mitigate the risk of internal security breaches.
- CISO Support and Security Coaching: We empower your security team and leadership.

What Makes Netready Different?

- Business-Centric Approach: We align our cybersecurity solutions with your specific business goals and objectives.
- Holistic Security Expertise: We go beyond just protection. We optimize your IT systems, improve efficiency, and empower your employees.

In today's ever-changing threat landscape, Netready and Zac Abdulkadir provide a comprehensive solution to safeguard your business. We offer peace of mind by protecting your data, optimizing your systems, and empowering your people.

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

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. 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, 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 7:00 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, but we also GUARANTEE a response time of 2 hours or less for normal problems, and within 30 minutes for problems marked "emergency," such as a network being down or a critical problem that is significantly impacting your ability to work.

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

Our Answer: Most I.T. firms offer an 8-hour or 6-hour 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 4 hours 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 a feedback system in place for your clients to provide "thumbs up" or "thumbs down" ratings on your service? If so, can I see those reports?

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

I.T. Maintenance (Managed Services):

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 or DAYS 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.)

To Request Your FREE Assessment,
please visit **www.NetreadyIT.com**
or call our office at 213.463.2100**.**

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 creeping up over and over, longer resolution time and you having to spend time educating the tech on your account.

Fortunately, we provide a dedicated technician to your account who will get to know you and your company, as well as your preferences and history. When you work with our local help desk technician, they'll be more capable of successfully resolving your I.T. issues and handling things the way you want.

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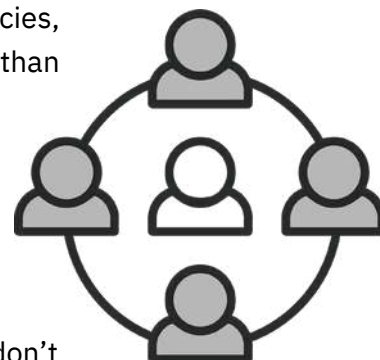
Q10 Do you offer documentation of our network as part of the plan, and how does that work?

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.

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 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 where we openly discuss your business goals, including your I.T. budget, critical projects, compliance issues, known problems and cybersecurity best practices.

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

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

Our Answer: Make sure you carefully review the cancellation clause in your agreement. Many I.T. firms hold their client's 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.

To Request Your __FREE__ Assessment,
please visit **www.NetreadyIT.com**
or call our office at 213.463.2100**.**

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?"

You can feel confident that our in-house technicians have among the most advanced cyber security training and certifications available, including:

Certified Information Systems Security Professional –CISSP CertifiedInformationSystemsSecurityManager–CISM Certified Information Systems Auditor –CISA CertifiedinRisk&InformationSystemsControls– CRISC SophosCertifiedEngineer -SCE

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

Our Answer: As above, the question may get a bit technical. The key is that they HAVE an answer and don't hesitate to provide it. Some of the things they should mention are:

- 2FA (two-factor authentication)
- Advanced end-point protection, not just anti-virus
- Security Awareness Training

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

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

Our Answer: Here's something to ask about: if THEY cause a problem with your network that causes you to be down for hours or days, to lose data or get hacked, who's responsible? What if one of their technicians gets hurt at your office? Or damages your property while there? In this litigious society we live in, you better make darn sure whomever you hire is adequately insured with both errors and omissions insurance, workers' compensation and cyber liability –and don't be shy about asking them to send you the policy to review!

If you get hit with ransomware due to their negligence, someone has to pay for your lost sales, the recovery costs and the interruption to your business operations. If they don't have insurance to cover YOUR losses of business interruption, they might not be able to pay, and you'll have to end up suing them to cover your costs. If sensitive client data is compromised, who's responsible for paying the fines that you might incur and the lawsuits that could happen? No one is perfect, which is why you need them to carry adequate insurance. True story: A few years ago, a company that shall not be named was slapped with several multimillion-dollar lawsuits from customers for bad behavior by their technicians. In some cases, their techs were accessing, copying and distributing personal information they gained access to on customers' PCs and laptops brought in for repairs. In other cases, they lost a client's laptop (and subsequently all the data on it) and tried to cover it up. Bottom line, make sure the I.T. firm you're hiring has proper insurance to protect YOU.

Rest assured, we make it a priority to carry all the necessary insurance to protect you, including Cyber errors and omission. Simply ask, and we will be happy to show you a copy of our policy.

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

Our Answer: Nobody should proofread their own work, and every professional I.T. consulting firm will have an independent third party reviewing and evaluating their company for airtight cyber security practices. There are many companies that offer this service, so who they use can vary (there's a number of good ones out there.) If they don't have a professional cyber security auditing firm doing this for them on at least a quarterly basis, or if they tell you they get their peers to audit them, DO NOT hire them. That shows they are not taking cyber security seriously. You can be confident in the effectiveness of our cyber security because we are audited by Galactic Advisors, and we have just recently been audited in May of 2024.

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 (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.

Rest assured; we do have an outsourced SOC to provide proactive security monitoring for our clients to better prevent a network violation or data breach.

Backups And Disaster Recovery:

Q18 Can you provide a timeline of how long it will take to get my network back up and running in the event of a disaster?

Our Answer: There are two aspects to backing up your data that most business owners aren't aware of. The first is "fail over" and the other is "fail back." For example, if you get a flat tire, you will 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 24 hours or less.

Q19 Do you Insist on doing periodic test restores of my backups to make sure the data is not corrupt and could be restores in the event of a disaster?

Our Answer: A great I.T. consultant will place eyes on your backup systems every single day to ensure that backups are actually occurring, and without failures. However, in addition to this, your I.T. company should perform a monthly randomized "fire drill" test restore of some of your files from backups to make sure your data CAN be recovered in the event of an emergency. After all, the WORST time to "test" a backup is when you desperately need it.

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

Verifying your backups daily and testing them on a regular basis is a cornerstone of a successful overall I.T. strategy. These are the lengths we go to for all our clients, including multiple random "fire drill" test restores to ensure ALL your files are safe because they are always backed up.

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

Q20 If I were to experience a location disaster, pandemic shutdown or other disaster that prevented me from being in the office, how would you enable me and my employees to work from a remote location?

Our Answer: If Covid taught us anything, it's that work-interrupting disasters CAN and DO happen when you least expect them. Fires, floods, hurricanes and tornadoes can wipe out an entire building or location. Covid forced everyone into lockdown, and it could happen again.

We could experience a terrorist attack, civil unrest or riots that could shut down entire cities and streets, making it physically impossible to get into a building. Who knows what could be coming down the pike? Hopefully, NONE of this will happen, but sadly it could.

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

One of our standard security tools is a Virtual Private Network (VPN). This tool allows you to work remotely from anywhere securely. We also offer our clients a way to connect to their office computers from home, so you really can work from anywhere.

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 confusing "geek-speak"?

Good I.T. companies won't confuse you with techno-mumbo-jumbo, and they certainly shouldn't make you feel stupid for asking questions. All great consultants have the "heart of a teacher" and will take time to answer your questions and explain everything in simple terms. As you interact with them in the evaluation process, watch for this.

Our technicians are trained to take time to answer your questions and explain everything in simple terms. Just look at what one of our long-term clients had to say:

> " Thank you for not making me feel ridiculous when I need you to help me do something. Your team always takes the time to ask questions and explain issues in detail **–Construction Manager**"

Do they and their technicians present themselves as true professionals when they are in your office? Do they dress professionally and show up on time?

If you'd be embarrassed if YOUR clients saw your I.T. consultant behind your desk, that should be a big red flag. How you do anything is how you do everything, so if they cannot show up on time for appointments, are sloppy with paperwork, show up unprepared, forget your requests and seem disorganized in the meeting, how can you expect them to be 100% on point with your I.T.? You can't. Look for someone else.

Our technicians are true professionals who you would be proud to have in your office. They dress professionally and show up on time, and if they cannot be there on time (for some odd, unforeseen reason), we always notify the client immediately. We believe these are minimum requirements for delivering a professional service.

The 4 Most Costly
Misconceptions
About I.T. Services

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

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

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

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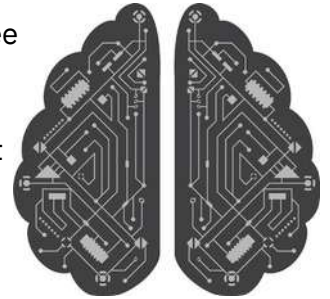
Misconception #3: You shouldn't have to pay "that much" for I.T. services.

We all know you get what you pay for. A cheap hourly rate under $150 per hour, which is the average fee for professional IT firms in Southern California 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 25years.

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.

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.

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: 30minutesfor 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.

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 25years, 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.
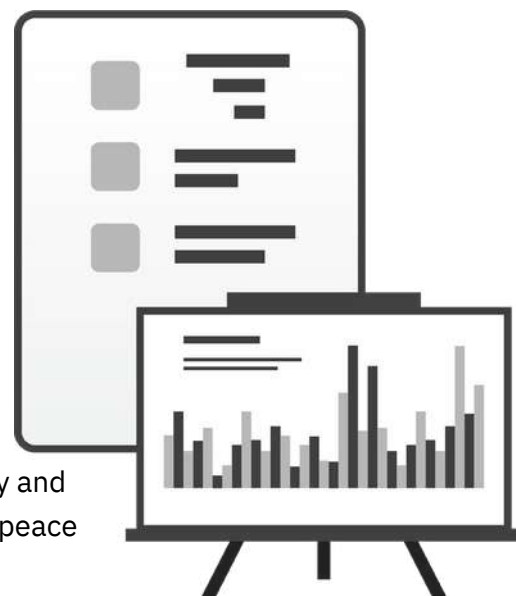
Dedicated to your security,

Zac Abdulkadir CEO / CISO
Netready

Read On To Hear What
Our Clients Have To Say:

"Our medical office got hit with Ransomware and we lost access to all our data for almost a week. Our IT guy at the time tried everything he could but was not experienced in dealing with Ransomware. We contacted Zac at Netready, he and his team took the time to walk us through their process and was able to identify how we were compromised. Within 24 hours they had our data back and our office was up and running again." **–Jazmin Castello, Office Manager**

"Working with the Netready team is like having our own IT department, intimate with our needs, but without the overhead that comes with keeping IT in-house. Netready cares about our satisfaction. In the rare instance we experience an issue, they listen to our concerns, and address them quickly and completely. Their proactive monitoring assures that we address potential IT issues before they become bigger problems. Netready allows us to focus on our work and leave IT concerns in their capable hands." **-David Weiner, CEO**

"Even as a small business, Netready treats our IT issues as importantly as if we were a large business. They respond quickly and are always up to date on the latest options for security and improving our system. We have used other IT companies in the past that were not as knowledgeable and progressive in the IT world as Netready. They make us feel like we are their most important client."
–Debbie Unruh, Executive Director