it's our word.

LoyalITy

A BUSINESS OWNER'S GUIDE TO IT SERVICES SELECTION

2025 EDITION

An Open Letter To All Business Owners and Leaders Who Outsource IT Support

Dear Fellow Business Owner or Executive,

Selecting the right IT company can be overwhelming. Making the wrong choice could lead to a frustrating contract where IT issues and poor service pile up. Picking the right one can bring relief as your IT problems vanish, and your data and company are secure. However, all IT companies claim to be proactive, responsive, and professional, making it difficult to identify the right one before signing a contract and handing over your company's network.

This executive guide was created to help business owners avoid the aggravation and losses that come with hiring the wrong IT firm by asking the right questions and knowing what to look for ahead of time. Unfortunately, there are countless tales of incompetent IT "experts" who bungle jobs and create additional problems due to their incompetence, lack of qualified staff, and weak cybersecurity skills. Many people have had similar negative experiences with IT companies and can attest to their horror stories.

One of the reasons for this is that the IT services sector is not regulated like most other professions, allowing anyone to claim they are an "IT specialist." Therefore, you, the customer, must exercise greater caution in selecting an IT support company and equip yourself with the knowledge presented in this report.

From false claims and unskilled technicians to poor management and terrible customer service, we have seen it all. We know these subpar providers are prevalent because we have had numerous clients approach us to help them untangle issues caused by other IT companies.

The information provided in this guide aims to promote higher standards in the IT support industry and to provide you with valuable information to help you defend against the unethical or incompetent behavior of some IT firms and technicians.

Dedicated to serving you,

Kari Renn
President/CEO
Email: krenn@loyality.com
Direct:920-437-9701
200 Packerland Dr – Green Bay, WI

21 Questions You Should Ask Your IT Services Company or Consultant Before Hiring Them for IT Support

CUSTOMER SERVICE:

Q1: When I have an IT problem, how do I get support?

Our Answer: In our IT management system, we open a ticket when a client reports a problem. This helps us to assign, track, prioritize, document, and resolve issues efficiently. However, some IT firms only allow ticket submissions through a login portal, which can be inconvenient for clients. It's important to note that this practice is for the IT firms' convenience and not the clients. While having a portal is a good option, it should never be the only option for requesting support.

It's crucial to ensure that the IT firm you work with has a reliable system in place to keep track of client requests and tickets. Otherwise, there's a high chance that some requests will be overlooked, skipped, or forgotten. To make it easy for clients to request support, the IT firm should have multiple avenues for submitting problems. At our firm, we make it easy by allowing clients to call, email, or submit a ticket via our portal, which puts their IT issues on the fast track to resolution.

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 and respond from 8:00 a.m. to 5:00 p.m. every weekday. But many CEOs and executives work outside normal “9 to 5” hours and emergencies can happen at all hours of the day. Not only can you reach out after hours for support any time any day, but we also strive to maintain a response time of 30 minutes or less for standard issues, and within 15 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 client problems?

Our Answer: Be 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. LoyalITy's guaranteed response times are outlined by scenario in our agreement. We would be happy to share this with any potential client. A great IT 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 the initial call to the final resolution, you will work with a dedicated vCIO (Virtual Chief Information Officer) who will know you, your business, and your goals if you work with LoyalITy.

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 an IT company does not have a feedback system in place, they may be concealing poor customer service results. On the other hand, if they do have a feedback system, it's essential to ask for the actual scores and reporting to gauge the quality of their service. At our company, we maintain a feedback system and are pleased to share our client feedback scores with you as a testament to the quality of our service.

IT Maintenance (Managed Services):

Q6: Do you offer true managed IT services and support?

Our Answer: It's important to look for an IT company that provides proactive monitoring of your IT systems and performs routine maintenance. If an IT company cannot provide these services, seeking another provider is advisable. At LoyalITy, we take pride in our advanced remote network monitoring system, which diligently keeps a watchful eye on your network, identifying potential problems, security threats, and other concerns. We have dedicated resources solely focused on managing this powerful tool, enabling us to address any issues promptly and preventing them from escalating into major complications.

Q7: What is NOT included in your managed services agreement?

Our Answer: IT companies often fail to explain the limitations of their monthly managed services agreement which can result in unexpected invoices. It's crucial to know what is not included in the agreement before signing up for services.

Commonly excluded items include projects such as server upgrades, office relocation, onboarding new employees, and purchasing hardware and software. It's important to ask additional questions, such as:

- Is there a limit on help desk service?
- Does the service agreement cover cloud services such as Microsoft 365?
- Is there an extra charge for resolving problems with third party vendors like leased printers?
- Is on site support included in the agreement?
- Does the company offer support for remote employees?
- If employees need support for home PCs during a shutdown, natural disaster, or other situations, will it be covered in the agreement?
- If the network is affected by ransomware, fire, flood, theft, or other disasters, is network rebuilding included in the agreement or is an extra project chargeable to the customer?
- Where do I find information regarding what is not covered in my agreement?
- Are Technical writing requests included? Examples: Disaster Recovery Plans, Incident Response Plans, Business Continuity Plans, or specific, individual policies

It's essential to have these details flushed out to prevent unexpected charges or limitations. At LoyalITy, we believe in transparency and clear communication with our clients. We have a full list of exclusions in our agreements and will happily share these with any potential client.

Q8: Is your help desk local or outsourced?

Our Answer: When selecting an IT firm, be cautious of smaller companies that outsource critical functions such as tech support. This could result in help desk support from a technician who lacks familiarity with your network, previous issues, and personal preferences, or even one who is not qualified. This can cause frustration and prolong issue resolution time. Fortunately, LoyalITy provides a dedicated technical alignment manager (TAM) to your business who will get to know you and your company, as well as your preferences and history. Your dedicated TAM will collect and provide ample documentation to our internal help desk team to help them provide personal support when you need it most.

Q9: How many engineers do you have on staff?

Our Answer: When considering an IT firm to hire, exercise caution with smaller companies that only have one or two technicians, or that outsource critical roles a. It's important to remember that everyone can get sick, have emergencies, go on vacation, or take time off occasionally. To avoid potential disruptions to your IT services, it's advisable to select a firm with a team of full time technicians who can provide coverage in the event of staff absences. At LoyalITy, we have a robust team of technicians to ensure that our clients' needs are always met, even in unforeseen circumstances.

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

Our Answer: The term "network documentation" refers to the process of maintaining comprehensive technical records regarding your owned assets such as computers, devices, software, directory structure, user profiles, passwords, and so on, as well as how your network is configured, backed up, and secured. It is expected that every reputable IT company, including LoyalITy, should offer this service to you at no additional cost, providing copies when requested and updating this documentation regularly.

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

Our Answer: At LoyalITy, we prioritize meeting with each of our clients routinely to conduct a "technology business review." During these meetings, we provide updates on the status of ongoing projects, as well as the health and security of your network. We also offer recommendations for new equipment and upcoming upgrades that may be necessary in the near future. Our meetings are an opportunity for C-level discussions where we openly discuss your business goals, IT budget, critical projects, known problems, and best practices for cybersecurity. Additionally, this is your chance to give us the feedback we need to strive to build long lasting relationships with our clients, based on mutual trust and respect.

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

Our Answer: It is crucial to carefully examine the cancellation clause within your agreement when engaging with an IT firm. Certain companies may impose substantial penalties and exhibit unprofessional behavior during the offboarding process. At LoyalITy, we prioritize your satisfaction and strive to provide a seamless experience, even when parting ways. We have implemented an effortless cancellation policy that requires a 60 day notice given at the end of the contract. In the event that you decide to conclude your services with LoyalITy, we ensure a collaborative, helpful, and professional approach throughout the process.

Cybersecurity:

Q13: What cybersecurity solutions do you offer?

Our Answer: Cyber threats such as malware, phishing attacks, and data breaches are becoming increasingly sophisticated and prevalent, making it more important than ever to take proactive measures to protect sensitive information. A single security breach can result in devastating consequences including financial losses, reputational damage, and legal repercussions. Below is a list of just a few of the services we offer:

- Multi-Factor Authentication
- SIEM (Security Information Event Management)
- Email Security (Spam Filtering AND Offsite Filtering)
- Employee Security Training & Dark Web Monitoring
- Managed Endpoint Detection and Response

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

Our Answer: Similar to the previous question, while the technical details may be complex, the IT company should have a clear and confident response to this question. Some key points that should be included in their answer are:

- Their approach to implementing and enforcing strong passwords and password policies.
- Their use of two-factor authentication (2FA) to add an extra layer of security beyond passwords.
- Their implementation of advanced endpoint protection measures that go beyond traditional antivirus software.
- Their use of firewalls and intrusion detection/prevention systems to protect against external threats.
- Their approach to network segmentation to limit the potential impact of a security breach.
- Their policy for keeping software and systems up to date with the latest security patches and updates.

As a client, it's important to feel confident that your IT provider is taking all necessary steps to protect your business from cyber threats, and a clear and thorough response to this question is a good indication that they take this responsibility seriously.

Q15: What cyber liability errors and omissions insurance do you carry to protect my company?

Our Answer: It's important to ask about responsibility and insurance coverage when working with an IT firm. If the firm causes an issue with your network that results in downtime or data loss, or if one of their technicians is hurt on your property, who's responsible? Additionally, if your business is impacted by a cybersecurity breach caused by the IT firm's negligence, who will cover the costs associated with lost sales, recovery, and any legal fees?

To protect our clients, we carry all necessary insurance, including errors and omissions, workers' compensation, and cyber liability insurance. We understand that accidents can happen, and we take responsibility for our actions. If you have any questions about our insurance policies, we are happy to provide you with a copy for your review.

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

Our Answer: Nobody should proofread their own work, and every professional IT consulting firm should have an independent third party reviewing and evaluating their company for airtight cybersecurity practices.

You can be confident in the effectiveness of our cybersecurity because we are audited by Vonahi and Trace Security, and we will continue testing every year.

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 Security Operations Center, also known as SOC, is a centralized department that specializes in monitoring and addressing security issues related to a company's network.

At LoyalITy, we take the security of our clients' networks seriously. In order to guarantee the highest level of protection against network intrusions and data breaches, we partner with Barracuda to provide dedicated proactive security monitoring. Through the integration of our SIEM (Security Incident Event Monitoring) software, we can swiftly detect and address any potential threats, significantly reducing the risk of a security breach. This comprehensive approach ensures that your systems are continuously monitored, enabling us to promptly mitigate any security vulnerabilities that may arise.

Backups & 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: Backing up your data involves two important aspects that many business owners overlook: failover and failback. Failover is like using a spare tire when you have a flat, and failback is getting a new or repaired tire at a service station.

If your data and network are wiped out by a ransomware attack or a natural disaster, you need a failover solution in place to allow your employees to continue working with minimal interruption. This solution must be separate and secure, to prevent ransomware from infecting the backups, servers, and workstations.

Regardless of the disaster, your business must resume operations within eight hours and critical functions should be transferred without delay. We recognize the significance of your data and your team's prompt recovery in the prosperity of your enterprise. If a disaster occurs, we have full confidence we can restore your network in eight hours or less in conjunction with yearly DR tests and our suggested backup solution.

Q19: If I were to experience a location disaster, pandemic shutdown, or any 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: The pandemic has shown us that unforeseen events can happen at any time, disrupting work and forcing businesses to adapt quickly. Natural disasters such as fires, floods, hurricanes, and tornadoes can also cause significant disruptions to a company's operations. As a result, it's crucial to ask your potential IT consultant about their ability to quickly transition their clients to remote work, securely, during a pandemic or disaster.

LoyalITy holds the belief that the pandemic has taught us a valuable lesson: companies should prioritize forward-thinking planning for unexpected events, including pandemics and disasters. By creating Business Continuity Plans (BCPs), organizations can clarify their course of action. Additionally, taking a proactive stance toward end user mobility is preferable to waiting until the eleventh hour.

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: An exceptional IT consultant will ensure that your backup systems are being checked daily to guarantee that backups are taking place without any issues. Additionally, your IT company should conduct a monthly randomized test to restore some of your files from backups to verify that your data can be recovered in case of an emergency. It's crucial to test backups regularly to ensure their reliability because the worst time to realize a backup isn't working is when you need it the most.

Ensuring daily backup verification and regular testing are vital components of an effective IT strategy. As part of LoyalITy's commitment to our clients, we test restores for all servers currently done on a quarterly basis.

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

Our Answer: The purpose of asking this question is to assess whether the IT consultant has a defined plan or process in place for taking over the IT operations. It is essential that they can provide a clear and detailed explanation of their process.

It is particularly important to discuss how they plan to transition from the current IT company, especially if there are potential conflicts or hostilities. A reputable IT services provider should have a comprehensive process for handling such situations.
If you choose LoyalITy as your IT services provider, we will be happy to share our client onboarding process and documentation with you. We have a well-defined and documented process that ensures a smooth transition and sets the stage for a successful partnership.

The 4 Most Costly Misconceptions About IT Services

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

Many business owners hold a costly misconception that their IT systems are immune to failure and therefore don't require regular updates and maintenance. However, this is akin to not wearing a seatbelt just because one hasn't been in an accident before.

IT networks are complex and constantly evolving, requiring regular maintenance to ensure they remain secure, fast, and problem-free. With the increasing prevalence and sophistication of ransomware and hacker attacks, regular updates have become even more critical. Here are just a few examples of the updates that should be performed regularly:

- Patches, updates, and management
- Antivirus updates and monitoring
- Firewall updates and monitoring
- Backup monitoring and test restores
- Operating system updates and management
- Monitoring hardware for signs of failure

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

Hiring a part-time IT "guru" may seem like a cost-effective solution, but it can lead to serious consequences. We've received countless calls from business owners who have suffered data loss or damage caused by inexperienced individuals who were simply trying to help. It's important to understand that IT networks are complex and require regular updates and maintenance to stay secure, fast, and problem free. If your IT support is not provided by a professional who specializes in this field, there is a high chance that they lack the necessary knowledge and expertise to provide effective solutions. Choosing a part-time, inexperienced person to handle your data and IT network can be a risky move. While it's not necessary to break the bank to find a reliable IT firm, it's crucial to avoid making decisions based solely on price. Remember, you get what you pay for in life.

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

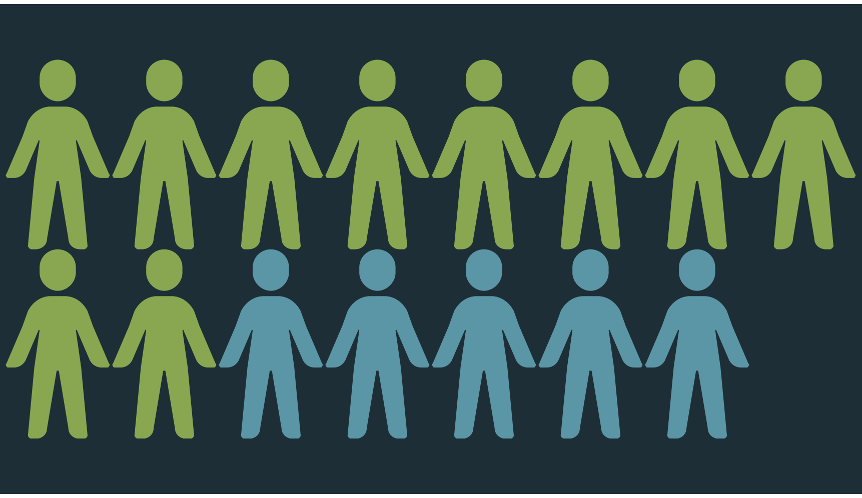
It is a well known fact that you get what you pay for. A cheap hourly rate often indicates subpar work. As with any other profession, skilled IT engineers and technicians do NOT come cheap because their services are in high demand. When you come across low IT service fees, it's usually because of one of the following reasons:

1. They are a small company that's just starting. They usually have only one or two technicians working for them (or they are a one person shop). Such a company might be suitable for a small business that is not regulated, doesn't have complex IT needs, and/or has only 10 or fewer computers to support. However, it would not be a good option for a larger organization that requires professional IT services for its expanding business.

2. The average years of experience within the technical team are low. Many businesses make the mistake of hiring cheap, inexperienced technicians to save a few dollars. They may hire college students or interns who work for next to nothing, but this can end up costing them more in the long run. Inexperienced technicians may misdiagnose problems, take longer to fix them, or even put your security and data at risk. For example, a technician may turn off important security notifications to avoid the work of sifting through them, which can leave your company vulnerable to hackers and cause downtime.

Your client data, accounting records, and other critical pieces of information are too important to trust in the lowest priced shop. Instead, you want value for your money and the job done right. While we may not be the cheapest, we offer a good price for a good service. We believe that it's better to explain our higher rates upfront than to make excuses for poor service in the future. That's why we've been in business for over 19 years, with a team of rock star technicians with an average of 15 years of experience in the IT industry.

Looking for information on how our costs compare to hiring in-house technicians? We have that information too!



75% OF OUR TEAM HAS OVER

15 YEARS

OF TECHNICAL EXPIRENCE

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

I would like to believe this is the case, but unfortunately, it is not. Similar to a reputable doctor, an ethical and experienced technician must assess your network before providing a quote over the phone.

A FINAL RECOMMENDATION

I hope this guide has provided some helpful insights into what to consider when outsourcing IT services for your company. My intention in sharing this information was to assist you in making an informed decision and steer clear of untrustworthy service providers.

If you are seeking a reliable partner to manage your digital infrastructure, we would appreciate the opportunity to earn your business. To demonstrate our commitment, we are pleased to offer you a complimentary network assessment.

This assessment is entirely free, and you are under no obligation to engage our services unless you believe it is the right choice for your organization.

Here's how it works:
We will arrange a brief call via phone or Teams to discuss your current situation, including your frustrations, requirements, concerns, and queries. We will ask a few straightforward questions, and depending on your answers, we may proceed to the next stage, which involves a quick, confidential investigation of your network, backups, and security protocols.

Your time investment is minimal: less than 30 minutes for the initial phone consultation and one hour for the second meeting to go over our findings and recommendations. When this network assessment is complete, here's what you will know:

✓ If your IT systems and data are truly secured from hackers, cybercriminals, ransomware, and even by rogue employees.

✓ If your current backup would allow you to be up and running again quickly if ransomware locked all your files.

✓ If you and your employees' login credentials meet industry standards to keep your company secure.

✓ Answers to any questions you have about a recurring problem, an upcoming project or change, or the service you are currently getting.

✓ When done, we'll provide you with a score that will show you how vulnerable you are 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.

How To Request This Free Assessment:

- Call me direct at 920-437-9701
- E-mail me directly with questions: krenn@loyality.com
- Scan the QR code and schedule a call with me

Dedicated to your peace of mind,

Kari Renn
President/CEO
Email: krenn@loyality.com
Direct: 920-437-9701
200 Packerland Dr – Green Bay, WI
Loyality it's our word.

it's our word.

LoyalITY