CloudMinders®
IT as it's meant to be

I.T. BUYER'S GUIDE

- 503.210.5203
- www.CloudMinders.com
- 7128 SW Gonzaga St., Suite 200, Tigard, OR 97223

What You Should Expect To Pay For I.T. Support For Your Small Business

How To Sort Through The Confusion And Complexity Of I.T. Services Companies' Contracts, Services And Pricing To Avoid Hiring The Wrong One

Read This Guide And You'll Discover:

- ✓ The 3 most common ways I.T. services companies charge for their services, and the pros and cons of each approach.
- ✓ A common billing model that puts ALL THE RISK on you when buying I.T. services; learn what it is and why you need to avoid agreeing to it.
- ✓ Exclusions, hidden fees and other "gotcha" clauses I.T. companies put in their contracts that you DON'T want to agree to.
- ✓ 5 ways "cheaper" I.T. firms hide the TRUE cost of their services in their contracts.
- ✓ 21 critical questions to ask your I.T. support firm BEFORE signing an agreement.

From the Desk of:
Jeremy Davis
Founder and President | CloudMinders

Dear Colleague,

One of the most commons questions we get from new prospective clients calling our office is "What do you guys charge for your services?" Since this is such a common and important question, I decided to write this report. Furthermore, there are 3 reasons why choosing your I.T. company on their fees alone – or even using that as one of the top criteria – can lead to overpaying, even if their pricing appears cheaper initially, and to extreme frustration and unappreciated risk to your organization. They are:

1 Unlike most industries, there is no such thing as "standard" pricing for I.T. services companies, even though most of the services appear to be the same. That's why it's impossible to compare I.T. providers on their fees alone. In this report I'll explain the most common ways I.T. services companies package and price their services, and the pros and cons of each, so you can make an informed choice.

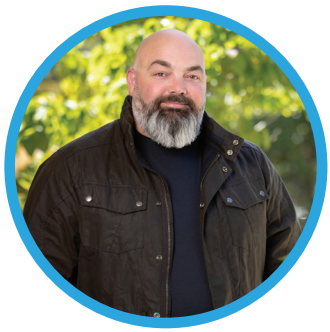
2 There are a few "dirty little secrets" about I.T. service contracts and SLAs (service level agreements) that "cheaper" I.T. firms use to make their fees appear less expensive, but actually end up putting you at high risk for cyber-attacks. Almost no business owner knows what to look for, what questions to ask or the true consequences to them being too cheap with backups, cyberprotections and disaster recovery, which is how the "cheaper" firms can get away with it. You NEED to understand this, and I'll explain it to you.

3 I wanted to educate business owners on how to pick the ***right*** I.T. services company for their specific situation, budget and needs based on the ***VALUE*** the company can deliver, not just the price, high OR low.

In the end, my purpose is to help you make the most informed decision possible so you end up working with someone who helps you solve your problems and accomplish what you want in a time frame, manner and budget that is right for you.

Dedicated to serving you,

Jeremy Davis
Founder and President | CloudMinders



About The Founder

Jeremy, the founder of **CloudMinders**, launched the company in 2015 with a vision to provide **innovative IT solutions that elevate businesses**. With a deep passion for technology and a commitment to **empowering businesses through reliable IT infrastructure**, Jeremy built CloudMinders from the ground up, establishing it as a trusted **Managed Service Provider (MSP)** in the Portland metro area.

Our Philosophy

At CloudMinders, we believe that **technology should be an enabler, not an obstacle**. Our philosophy is rooted in **proactive service, transparency, and building strong relationships**. We don't just fix problems—we anticipate them, ensuring our clients stay ahead of IT challenges. By offering **strategic IT support, cloud solutions, cybersecurity, and infrastructure management**, we help businesses focus on what they do best while we handle their IT needs.

Customer service is at the heart of everything we do. We prioritize **responsiveness, reliability, and trust**, ensuring that every business we support gets the personalized service it deserves. Our goal is to **act as an extension of our clients' teams**, offering expert guidance and support tailored to their unique needs.

Why CloudMinders?

- **Experience & Expertise:** With nearly a decade of experience in IT services, CloudMinders has become a **go-to partner** for businesses looking to scale securely and efficiently.
- **Proven Track Record:** Our clients range from **startups to established enterprises**, all benefiting from our hands-on approach and commitment to excellence.
- **Innovation-Driven:** We stay ahead of industry trends to **deliver cutting-edge solutions**, ensuring that our clients maintain a competitive edge.
- **Community-Focused:** Jeremy believes in **giving back and fostering a thriving business community**, ensuring that success is shared.

At CloudMinders, we don't just manage IT—we **empower businesses** to grow, adapt, and succeed in a fast-paced digital world.

Comparing Apples To Apples: The Predominant I.T. Services Models Explained

Before you can accurately compare the fees, services and deliverables of one I.T. services company to another, you need to understand the 3 predominant pricing and service models most of these companies offer. Some companies offer a blend of all 3, while others are strict about offering only one service plan.

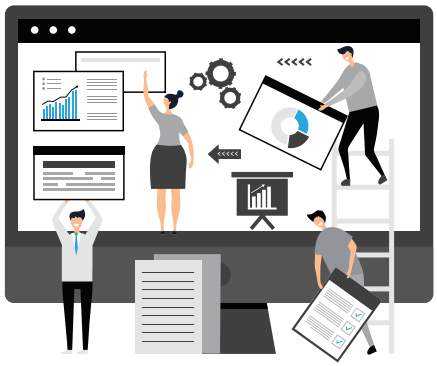
The 3 Predominant Service Models Are:

Time and Materials (Hourly). In the industry, we call this "break-fix" services. Essentially, you pay an agreed-upon hourly rate for a technician to "fix" your problem when something "breaks." The price you pay will vary depending on the provider you choose and the complexity of the problem, but most will be in the $200 to $300 range.

Under this model, you might be able to negotiate a discount based on buying a block of hours. The scope of work ranges from simply resolving a specific problem (like fixing slow WiFi or resolving an e-mail problem) to encompassing a large project like a software upgrade, implementing cyber protections or even an office move. Some companies will offer staff augmentation and placement under this model as well.

Similar to this are value added reseller services. VARs typically do I.T. projects for organizations that have internal I.T. departments. The term "value added" reseller is based on the fact that they resell hardware (PCs, firewalls, servers, etc.) and software, along with the "value added" services of installation, setup and configuration. VARs typically service larger organizations with internal I.T. departments. A trend that has been gaining ground over the last decade is that fewer VARs exist, as many have moved to the managed I.T. services model.

Managed I.T. Services (MSP, or "Managed Services Provider"). This is a model where the I.T. services company, called an MSP, takes on the role of your fully outsourced I.T. "infrastructure." That includes things such as:

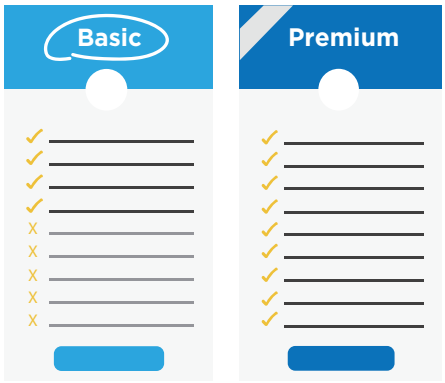


- Troubleshooting I.T. problems.
- Setting up and supporting PCs, tablets, Macs and workstations for new and existing employees, both on-site and remote.
- Installing and setting up applications such as Microsoft 365, Google Workspace, SharePoint, etc.
- Setting up and managing the security of your network, devices and data to protect against hackers, ransomware and viruses.

- Backing up your data and assisting in recovering it in the event of a disaster.
- Providing a help desk and support team to assist employees with I.T. problems.
- Setting up and supporting your phone system.
- Monitoring and maintaining the overall health, speed, performance and security of your computer network on a daily basis.

In addition to managing your I.T., a good MSP will provide you with an I.T. Roadmap and budget for necessary projects to further secure your network and improve the stability and availability of critical applications, as well as ensure that your I.T. systems are compliant with various data protection laws (HIPAA, FTC Safeguards, PCI, etc.) and that your cyber protections meet the standards on any cyber insurance plan that you have.

These projects are not included in the routine, day-to-day maintenance and are typically planned out in advance, based on the growth of your organization, your risk tolerance, operations, unique business model, etc.



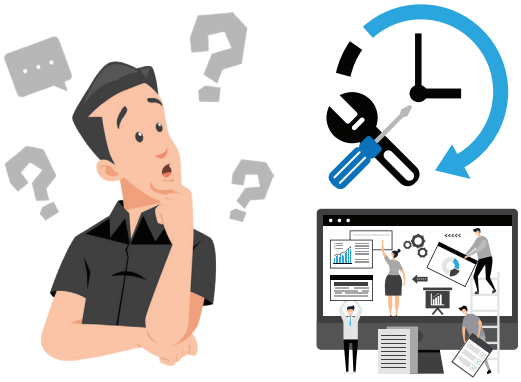
Vendor-Supplied I.T. Services. Many software companies and vendors will offer pared-down I.T. support for their customers in the form of a help desk or remote support for an additional fee.

However, these are typically scaled-back services, limited to troubleshooting their specific software 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 and won't help you and will often refer you to "your I.T. 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 (often referred to as a "line-of-business" application), this is not sufficient to provide the full I.T. services, cybersecurity, backup and employee (end-user) support most businesses need.

As a small or midsize business looking to outsource your I.T. support, you are most likely to end up having to choose between two service models: the managed 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 I.T. Services Vs. Break-Fix: Which Is The Better, More Cost-Effective Option?

The advantage of break-fix services is that you only pay for I.T. support when you need it, without being locked into a monthly or multi-year contract. If you're not happy with the service you're getting, you can change providers easily. If you're a micro-business with only a few employees, very simple I.T. needs where you don't experience a lot of problems and don't host or handle sensitive data (medical records, credit cards, Social Security numbers, etc.), break-fix might be the most cost-effective option for you.



However, the downsides of break-fix services are many if you're NOT a micro-business and are attempting to grow in revenue, staff and clients, or if you handle sensitive, "protected" data. **The 6 big downsides are as follows:**

X **High Costs During Crises:** Break-fix services might seem cost-effective at first. But when something goes wrong, like a ransomware attack, hardware failure, or network outage, the bills can climb quickly. Since there's no proactive care, problems are often more severe and costly. You're not just paying for time—you're also paying for lost productivity, downtime, and potential data recovery.

X **Slower Response and Resolution Times:** As a non-managed client, you're a lower priority. The provider has no historical insight into your systems, no monitoring in place, and often needs extra time to get up to speed before they can even begin fixing the issue. That delay means longer downtime and frustration, especially during emergencies.

X **Incentives Work Against You:** In a break-fix model, the longer a problem takes to fix, the more money the provider makes. They may assign a junior technician who takes longer to resolve an issue simply because they cost less. There's no built-in incentive to resolve problems quickly or permanently.

X **You're at Higher Risk for Major Problems:** Without proactive monitoring, patching, or strategic planning, you're more likely to experience serious issues. Break-fix providers step in only after something breaks. Managed services are designed to prevent problems from happening in the first place.

- **No Budget Predictability:** Break-fix costs vary wildly. You might pay nothing in a good month, then face thousands of dollars in charges the next. This inconsistency makes it hard to plan, control spending, or scale your business with confidence.

- **Zero Preventative Care:** Break-fix support is reactive by nature. There's no routine maintenance,system checks, or forward-looking advice. This leaves your business vulnerable to avoidable issues.A proactive approach like managed services provides peace of mind and long-term savings throughprevention.

  Thinking you're fine because "nobody wants to hack us" or "we're 100% in the cloud" is gross ignorance. If you don't have a professional I.T. company monitor and maintain your company's I.T. security, you WILL get hacked, incurring significant financial losses, not to mention reputational damage and client losses.

For all these reasons, hiring an MSP to manage your I.T. environment for an agreed-upon monthly budget is, by far, the most cost-effective, smartest option for most businesses with 10 or more employees, or who handle critical operations and sensitive data and are risk-averse.

What Should I.T. Services Cost?

This is one of the most common questions we get. The truth is, the right I.T. partner isn't always the cheapest, but they should deliver the best value for your investment.

At CloudMinders, we are not the lowest-cost provider, and we're proud of that. Our pricing reflects the quality, responsiveness, and strategic value we deliver to our clients every day. That includes proactive support to prevent problems, not just react to them. We offer high-touch service and fast response times from experienced technicians. Our clients receive clear communication and accountability so they always know what's happening and why. We also provide ongoing strategic guidance to align I.T. decisions with business goals.

We've designed our service model to maximize value. By leveraging offshore resources, we deliver enterprise-level support efficiently. Our flat-rate pricing offers budget certainty with no surprise fees.

If another provider comes in significantly cheaper, it's important to ask where they may be cutting corners. Are they delivering the same experience, accountability, and outcomes? In I.T., the cheapest option can often become the most expensive in the long run.

Important! Please note that the following price quotes are industry averages based on a recent I.T. industry survey conducted by a well-known and trusted independent consulting firm, Service Leadership, that collects, analyzes and reports on the financial metrics of I.T. services firms from around the country.

We are providing this information to give you a general idea of what most MSPs and I.T. services charge and to help you understand the VAST DIFFERENCES in service contracts that you must be aware of before signing on the dotted line. Please understand that this does NOT reflect our pricing model or approach for your unique situation. We are simply providing this as an educational resource to help you understand the vast differences in price and value.

Hourly Break-Fix Fees: Most I.T. services companies selling break-fix services charge between $200 and $300 per hour with a one-hour minimum. In some cases, they will give you a discount on their hourly rates if you purchase and pay for a block of hours in advance.

Project Fees: If you are getting an I.T. firm to quote you for a onetime project, the fees range widely based on the scope of work outlined and the complexity of the project. If you are hiring an I.T. consulting firm for a project, I suggest you demand the following:

- **A detailed scope of work that specifies what "success" is.** Make sure you document what your expectations are in performance, workflow, costs, security, access, etc. The more detailed you can be, the better. Clarifying your expectations up front will go a long way toward avoiding miscommunications and additional fees later on to give you what you REALLY wanted.
- **A fixed budget and time frame for completion.** Agreeing to this up front aligns both your agenda and the consultant's. Be very wary of hourly estimates that allow the consulting firm to bill you for "unforeseen" circumstances. The bottom line is this: it is your I.T. consulting firm's responsibility to be able to accurately assess your situation and quote a project based on their experience. You should not have to pick up the tab for a consultant underestimating a job or for their inefficiencies. A true professional knows how to take into consideration those contingencies and bill accordingly.
- **Clear Post-Project Support Plan.** Make sure the proposal outlines what happens after the project is complete. Will support be provided if something needs to be adjusted? Is that support included or billed separately? You should never assume post-project help is part of the deal unless it's spelled out.
- **Stated Assumptions and Limitations.** A professional I.T. firm should document any assumptions they made in creating your quote—like system requirements or user availability. This helps clarify expectations, reduce surprises, and protect both sides from scope creep.

Managed I.T. Services: Most managed I.T. services firms will quote you a MONTHLY fee based on the number of devices, users and locations they need to maintain. According to Service Leadership, the average fee per user (employee) ranges from $146.08 per month to $249.73 per month – and those fees are expected to rise due to constant inflation and a tight I.T. talent labor market.

Obviously, as with all services, you get what you pay for. "Operationally mature" MSPs typically charge more because they are far more disciplined and capable of delivering cybersecurity and compliance services than smaller, cheaper-priced MSPs.

They also include CIO (chief information officer) services and dedicated account management, have better financial controls (so they aren't running so lean that they are in danger of closing their doors) and can afford to hire and keep knowledgeable, qualified techs vs. junior engineers or cheap, outsourced labor.

To be clear, I'm not suggesting you have to pay top dollar to get competent I.T. services, nor does paying "a lot of money" guarantee you'll get accurate advice and responsive, customer-centric services. But if an MSP is charging on the low end of $146.08 per employee or less, you have to question what they are NOT providing or NOT including to make their services so cheap. Often they are simply not providing the quality of service you would expect.

5 Ways "Cheaper-Priced" I.T. Firms Hide The TRUE Cost Of Their Services In Their Contracts

As we said previously, no two I.T. services agreements are alike, and unless you are technically savvy (and most C-level executives aren't, obviously), you won't really know if what you're being quoted is insufficient, overpriced or even underquoted.

If you're not careful, the "cheapest" or less expensive I.T. provider can end up costing you a lot more due to carve-outs and hidden fees in their contracts that they will later nickel-and-dime you over, or quoting inadequate solutions that you'll later need to pay to upgrade.

Here are the 5 most common things "cheaper" I.T. companies leave out of their proposal to make themselves appear cheaper – but those companies are NOT the bargain you might think they are.

1 Grossly Inadequate Compliance And Cybersecurity Protections.

A ransomware attack is a significant and devastating event for any business; therefore, you must make sure the I.T. company you're talking to isn't just putting a basic (cheap) antivirus software on your network and calling it done. This is by far the one critical area most "cheaper" MSPs leave out.

Antivirus is good but woefully insufficient to protect you. In fact, insurance companies are now requiring advanced cyberprotections such as employee cyber awareness training, 2FA (2-factor authentication) and what's called "advanced endpoint protection" just to get insurance coverage for cyber liability and crime insurance. We provide those standard in our offering, so not only do you greatly reduce your chances of a cyber-attack, but you also avoid being denied an important insurance claim (or denied coverage, period).

2 Inadequate Backup And Disaster Recovery Solutions.

Make sure your I.T. company includes **daily** backups of your servers and workstations, as well as CLOUD APPLICATIONS such as Microsoft 365, Google Workspace and other line-of-business applications, such as your CRM data, client data, etc. That's because online applications do NOT guarantee to back up your data (read the small print in your contract and you'll be shocked). Further, your backups must be immutable, which means they cannot be corrupted by a hacker. Many insurance companies now *require* immutable backups to be in place before they insure against a ransomware or similar cyber event that erases data. Be sure to ask your I.T. company if that's what they quoted you.

3 Carve-Outs For On-Site And After-Hours Support.

This is another area that takes many business owners by surprise: all after-hours and on-site visits might involve an extra fee. We include ALL of this in our agreements so you aren't nickel-and-dimed for every request, but you need to make sure you understand what is and isn't included in the service agreement you're signing.

4 Nonexistent Vendor Liaison And Support.

Some I.T. firms will charge you hourly to resolve issues with your phone system, ISP, security cameras, printers and other devices they didn't sell you but that still reside on the network (and give you technical problems). As a client of ours, you get all of that INCLUDED, without extra charges.

5 Cheap, Inexperienced Techs And No Dedicated Account Managers.

Some lower-priced I.T. providers keep costs down by relying heavily on junior technicians or by assembling a loose network of part-time or contract staff. While this may reduce overhead, it often results in inconsistent service, slower resolution times, and limited expertise, especially in complex areas like networking and cybersecurity. The concern is not whether a technician is full-time or contract, but whether they are experienced, well-managed, and accountable for outcomes.

Make sure the firm you hire has a structured approach to service delivery and can show that their team, regardless of employment model, is trained, certified, and supported by internal quality control. Many low-cost providers also lack dedicated account management. Without this, no one is actively monitoring your I.T. strategy, anticipating upgrades, or helping you plan for growth. Good account management includes building an I.T. roadmap tailored to your business, regularly reviewing security and compliance, and ensuring that key priorities do not get overlooked.

Buyer Beware! In order to truly compare the "cost" of one managed I.T. services contract to another, you need to make sure you fully understand what IS and ISN'T included in the SLA you are signing up for. It's VERY easy for one I.T. services provider to appear far less expensive than another UNTIL you look closely at what you are getting.

The SLA should define the following:

- What services the MSP is providing in clear terms.
- Guaranteed response time to a problem (both minor and major outages).
- What fees are extra (like on-site fees, after-hours support, etc.).
- Contract terms and renewals.
- Cancellation terms: specifically, how do you get out of the contract if they are not delivering the services promised?
- Liability protection, both for them and you.
- Payment terms.

But the BEST way to avoid having a problem is to pick the right MSP to begin with.

The following are 21 questions to ask your I.T. services provider that will clarify exactly what you're getting for your money. Some of these items may not be that important to you, while others (like response time, adequate insurance and cybersecurity and compliance services) may be critical. Make sure you fully understand each of these items before making a decision about who the right provider is for you; then make sure you get this IN WRITING.

21 Questions You Should Ask Your I.T. Services Firm Before Signing A Contract

Customer Service:

Q1. How do you request support?

Our Answer: Make sure you clearly understand how to request help when an I.T. issue arises. Can you call a live person directly, or do you have to submit a ticket online or send an email? What happens if your internet is down or your device is unresponsive? It is important to know what options are available and how quickly you can expect a response.

At CloudMinders, we provide multiple support channels to make it easy to get help quickly. You can call our dedicated support line, email our help desk. Most importantly, we have real people ready to respond promptly and professionally, so you are never left waiting during a critical issue.

Q2. Do you have a written, guaranteed response time for working on resolving your problems?

Our Answer: The #1 frustration we hear from business owners about their current I.T. company is "They never return our calls" or "I have to wait forever to get someone to respond to a problem." Obviously, if you're paying for support, that's unacceptable. At CloudMinders, we guarantee our response times with a clearly defined Service Level Agreement (SLA) and back it up with real-time performance tracking. Our clients have full transparency into response times, so you never have to wonder when help is coming—we prove it.

With our proactive monitoring, dedicated support team, and commitment to innovation, we resolve most issues before they impact your business and ensure you get the IT support you need, when you need it.

Q3. Do they take the time to explain what they are doing and answer your questions in terms that you can understand (not geek-speak) or do they come across as arrogant and make you feel stupid for asking simple questions?

Our Answer: Our technicians are trained to have the "heart of a teacher" and will take time to answer your questions and explain everything in simple terms. Just look in the client comments section of this report to see how our clients rave about our team of techs dedicated to supporting you.

Q4. Do they create an I.T. Roadmap and budget and meet with you quarterly to review it?

Our Answer: We conduct quarterly strategy meetings with our clients to look for areas of high risk (such as cybersecurity, compliance, unstable systems, old equipment, etc.) as well as new ways to help improve employee productivity, lower costs, increase efficiencies and align I.T. with your business goals. Most MSPs don't offer these fractional CIO services, don't know how to put together an I.T. budget and Roadmap, and simply offer basic help desk support and some maintenance, NOT strategy.

Q5. Do they bill you properly and provide invoices that clearly explain what you are paying for?

Our Answer: Our Answer: Another complaint we hear from new clients is over billing. Either the I.T. company forgets to invoice you for something, then hits you with a giant bill to make up for months of incorrect billing, or they invoice you so randomly with confusing bills that you don't really know what you're paying for. We provide detailed invoices that At CloudMinders, we believe trust starts with transparency. That's why our invoices are detailed, easy to understand, and 100% accurate. Every invoice clearly outlines:

- **What work was done**
- **Why it was necessary**
- **When it was completed**

Plus, before we send a single bill, our team double-checks everything for accuracy—so you'll never be caught off guard by hidden fees or vague charges. With CloudMinders, you'll always know exactly what you're paying for—and why.

Q6. Do they have adequate insurance to protect YOU?

Our Answer: Since your I.T. company is directly maintaining and supporting your critical data and I.T. infrastructure, it's extremely important that they carry cyber liability and errors and omissions insurance to cover any damages (and costs) they might inadvertently cause to you. If they fail to carry insurance, it's YOUR liability. Don't be afraid to ask to see their coverage.

Q7. Do they have a dedicated account management team?

Our Answer: If they are too small to offer dedicated account management, you'll end up frustrated trying to find someone to help you. If it's the owner, ask how they are going to be able to dedicate time to you while running the company (the answer: they won't). Make sure you know what team is going to be dedicated to supporting YOU when you need help.

Cybersecurity And Compliance:

Q8. Do they insist on providing security that meets the FTC Safeguards Rule?

Our Answer: The FTC Safeguards Rule has been around for years, but recently has been updated to be far more aggressive in its requirements for all businesses. Penalties are serious – $100,000 per violation and over $43,000 per day. If you fail to meet the security standards outlined (and most businesses ARE required to meet these standards) you could be fined by the FTC and sued, creating significant financial costs, tying you up in litigation and lawsuits, not to mention reputational damages.

If your current I.T. company has not talked to you about this, they are putting you at significant risk. We won't allow a client to NOT have adequate security measures in place to meet these standards; and one of the ways cheaper MSPs charge less is because they allow their clients to operate without these critical protections. It is not the "bargain" their clients think it is. We ensure that **every client** meets or exceeds **FTC Safeguards Rule requirements** by implementing **industry-leading cybersecurity protections, compliance monitoring, and proactive risk management.**

Cheap MSPs cut corners—CloudMinders doesn't. The cost of inadequate security is far greater than the price of doing things right the first time. Let's make sure your business is protected.

Q9. Do they provide you with a quarterly report that shows all the updates, security patches and the status of every machine on your network so you know for SURE your systems have been secured and updated?

Our Answer: Every quarter, our clients get a detailed report that shows an overall health score for their network and the updates we've made to their network. We reassess their security, stability and compliance every quarter to ensure we are doing OUR job in watching over critical operations and data to drastically reduce the chances of a disaster or cyber-attack.

Q10. Is it standard procedure for them to provide you with written network documentation detailing what software licenses you own, user information, hardware inventory, etc., or are they the only person with the "keys to the kingdom"?

Our Answer: All 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.

If your current I.T. company doesn't provide you with any documentation and they keep you in the dark about what "inventory" you have of equipment, software licenses, system passwords, etc., you are being "held hostage" and should NEVER allow an I.T. person to have that much control over 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 they, and their leadership team, understand regulatory compliance such as the HIPAA, PCI compliance, FTC Safeguards Rule?

Our Answer: If your business is subject to regulatory requirements, it is critical that your I.T. provider understands those obligations and builds systems that support compliance. Many providers focus only on technology and overlook key compliance standards, putting your organization at risk.

At CloudMinders, we have experience supporting clients in regulated industries, including those governed by HIPAA, PCI DSS, and the FTC Safeguards Rule. Our team stays current with evolving compliance requirements and integrates those standards into our security strategies, documentation practices, and reporting. We do not just keep your systems running. We help keep your business aligned with the compliance standards that apply to your industry.

Q12. Have they asked to review your cyber liability, ransomware or crime insurance application to ensure they are doing what is required in your policy for coverage?

Our Answer: Many businesses now carry insurance to help cover the costs of a ransomware attack or other cyber fraud case where money is stolen from your organization. HOWEVER, all insurance carriers are now requiring strict cybersecurity protections be implemented BEFORE they will cover you. If your I.T. company has not talked to you about this, you might be at risk to have your claim denied for coverage due to your failure to meet the cyber standards YOU agreed to in the policy.

If a ransomware attack happens, your insurance company won't simply pay out. They will investigate the matter first to determine what happened and who caused it. If they discover you didn't have adequate preventative measures in place (as outlined on the application you completed to get coverage) they are within their right to deny coverage.

You might think your I.T. company is actually doing what is outlined on the policy, but there's a very good chance they aren't. We see this all the time when reviewing potential new clients' networks. One of the things we can do for you in a complimentary Risk Assessment is review this important area of protection and see whether or not you're meeting basic cybersecurity requirements that are in most insurance policies.

Backups And Data Recovery:

Q13. Do they INSIST on immutable backups for your data?

Our Answer: The only kind of backup you should have is an "immutable" backup, which means your backup data cannot be changed or corrupted. This is important because ransomware attacks are designed to infect your backups so you are forced to pay the ransom to get your data back. This is why cyber insurance policies now require the companies they are insuring to have immutable backups in place. If you're working with an I.T. firm, they should not only know about this type of backup, but insist you have it.

Q14. Do they INSIST on doing periodic test restores of your backups to make sure the data is not corrupt and could be restored in the event of a disaster?

Our Answer: We perform a monthly "fire drill" and perform a test restore from backup for our clients to make sure their 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.

Q15. Do they insist on backing up your network BEFORE performing any type of project or upgrade?

Our Answer: Any time a project or upgrade is performed, there is a risk something could go wrong. A hardware failure, software conflict, or unexpected issue could disrupt your systems or cause data loss.

At CloudMinders, we always back up your environment before starting any major work. It is a simple but essential precaution that protects your data and ensures we can quickly recover if something does not go as planned. Skipping this step is a risk no responsible provider should take.

Q16. If you were to experience a major disaster, such as an office fire or ransomware attack, do they have a written plan for how your network could be restored FAST and/or enable you to work from a remote location?

Our Answer: Whether it is a ransomware attack, office fire, or natural disaster, your I.T. provider should have a clear, written plan for how to restore your systems quickly and minimize downtime. Without one, you are left guessing during a crisis.

At CloudMinders, every client receives a tailored disaster recovery plan that outlines how their network and data will be restored in the event of an emergency. While we encourage clients to develop a full office-wide business continuity plan, we ensure their I.T. systems are covered with fast recovery options and remote access capabilities. You should never be caught off guard when disaster strikes.

Technical Expertise And Service:

Q17. Who handles your support requests, and how are they managed for quality and responsiveness?

Our Answer: It is important to know who will be handling your day-to-day support requests and how those technicians are managed. Are they part of a structured support team with clear standards and accountability? Will they be familiar with your systems and business environment, or are they a rotating pool of unknown agents?

At CloudMinders, we use a carefully selected, well-managed support team that is trained to deliver consistent, high-quality service. Every ticket is tracked, documented, and reviewed to ensure responsiveness and resolution quality. Our clients always know who is responsible for their experience, and we maintain full accountability for every interaction.

Q18. Do their technicians maintain current vendor certifications and participate in ongoing training – or are they learning on your dime?

Our Answer: Technology changes fast, and your I.T. provider should be committed to keeping their team trained and certified on the tools and platforms they support. You do not want technicians experimenting on your systems because they lack proper experience or training.

At CloudMinders, our technicians are required to maintain up-to-date vendor certifications for all the major technologies we support. We also invest in ongoing training to keep our team sharp, efficient, and aligned with best practices in cybersecurity and support. Our hiring process is highly selective, and we screen thoroughly for both technical skill and customer service ability. In fact, fewer than one percent of applicants make it through our hiring pipeline.

This ensures you get qualified experts from day one, not someone learning as they go.

Q19. Do their technicians conduct themselves in a professional manner?

Our Answer: Our technicians are true professionals who are not only polite, but trained in customer service, communication and high standards. They won't confuse you with "geek-speak," make you feel stupid or talk down to you. If they have to be on-site at your office, you would be proud to have them there. We believe these are minimum requirements for delivering a professional service.

Q20. Are they familiar with (and can they support) your unique line-of-business applications?

Our Answer: We own the problems with all line-of-business applications for our clients. That doesn't mean we can fix faulty software – but we WILL be the liaison between you and your vendor to resolve problems you are having and make sure these applications work smoothly for you.

Q21. When something goes wrong with your Internet service, phone systems, printers or other I.T. services, do they own the problem or do they say, "That's not our problem to fix"?

Our Answer: Many I.T. providers take a narrow view of their responsibilities and will tell you, "That's not our problem," when the issue involves your internet provider, phone system, or printer vendor. This leaves you stuck in the middle, trying to coordinate technical support for systems you did not set up and do not manage.

At CloudMinders, we believe it is our job to take ownership of the problem and drive it to resolution. Whether the issue is with your ISP, phone vendor, or another third party, we act as your single point of contact so you do not have to waste time chasing multiple support teams. That is what real service looks like, and it is what you should expect from a true I.T. partner.

Are You Done With Frustrating I.T. Support And Never-Ending I.T. Problems?

Give Us A Call To Get The Competent I.T. Support You Need And The Responsive, Honest Service You Want

Get the Competent I.T. Support You Need and the Responsive, Honest Service You Deserve
If you are looking for an I.T. company you can trust to do the right thing, the next step is simple. Call our office at **503-210-5203** and reference this guide to schedule a brief 10- to 15-minute consultation.

You can also visit **www.CloudMinders.com/call** to schedule your consultation online. On this call, we will discuss your current situation, any concerns you have, and answer any questions about how we work. If you are comfortable moving forward, we will schedule a time to complete our proprietary **18-Point I.T. Systems and Risk Assessment**.

This assessment can be done with or without your current I.T. provider knowing. We will explain how that works during our initial call.

By the end of this free assessment, you will know:

- Whether your systems and data are truly secure from cyber threats and where you may be exposed.
- If your backups are properly configured to allow a fast and full recovery in a real emergency.
- Where you may unknowingly be out of compliance with HIPAA, PCI, the FTC Safeguards Rule, or other industry regulations.
- How to reduce overall I.T. costs while improving security, communication, and employee productivity.

There is no cost, no obligation, and nothing to lose. At a minimum, you will gain a valuable third-party perspective. At best, you will discover a trusted partner who can deliver the support and results you have been looking for.

Fresh eyes see things that others cannot – so, at a minimum, our free Assessment is a completely risk-free way to get a credible third-party validation of the security, stability and efficiency of your I.T. systems. There is no cost and no obligation. We are here to earn your trust and demonstrate a far better way to get you the I.T. services and support you need.

To Schedule Your FREE Assessment, please visit
www.CloudMinders.com or call our office at **503-210-5203**

Dedicated to serving you,

Jeremy Davis
Founder and President | CloudMinders