Executive Brief:

IT Buyer's Guide

How to Calculate and Understand IT Support Costs For Your Business

AFFILIATED

Cybersecurity, Compliance, & Managed IT Support

The Executive's Guide
To IT Support Services And Fees

How to Calculate and Understand IT Support Costs for Your Business

How to Sort Through the Confusion and Complexity of IT Services Companies' Contracts, Services and Pricing to Avoid Hiring the Wrong One

Read this executive guide to discover:

- ✓ The 3 most common ways IT 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 IT services; learn what it is and why you need to avoid agreeing to it.
- ✓ Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to.
- ✓ 4 ways "cheaper" IT firms hide the TRUE cost of their services in their contracts.
- ✓ 5 critical questions to ask your IT support firm BEFORE signing an agreement.

Never Ask An IT Services Company, “What Do You Charge For Your Services?” Instead, Make Sure You Ask, **“What Will I *Get* For My *Money*?”** Know What To Look For And What To Avoid

From the Desk of: Michael Moran
President
Affiliated

Dear Colleague,

One of the most common questions we get from prospective client is “What do you charge for your services?” Since this is such a common and important question, I decided to create this resource. There are 3 reasons why choosing your IT 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. The 3 reasons are:

1. Unlike most industries, there is no such thing as standard pricing for IT services companies, *even though most of the services appear to be the same*. That’s why it’s impossible to compare IT providers on their fees alone. In this resource I’ll explain the most common ways IT services company's package and price their services, and the pros and cons of each, so you can make an informed choice.

2. Certain lesser-known aspects of IT service contracts and SLAs can be misleading, as some budget IT companies may present lower fees that could inadvertently increase your vulnerability to cyber threats. Many executives are not fully aware of the critical elements to scrutinize, the right inquiries to make, or the severe repercussions of economizing excessively on backups, cyber defense, and compliance support. Recognizing these factors is beneficial, and I am here to clarify them for you.

.

3. It's essential for executives to understand how to select an IT services provider that aligns with their unique circumstances, financial constraints, and requirements, focusing on the VALUE provided rather than solely on cost, whether it be high or low.

In the end, my purpose is to help you make the most informed decision possible, so you accomplish what you want in a timely manner, that is budget friendly to your organization.

Dedicated to serving you,

Michael Moran, President,
Affiliated

Comparing Apples To Apples:
The Predominant IT Services Models Explained

Before you can accurately compare the fees, services and deliverables of one IT 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 $125 to $250 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. Value Added Resellers (VARs) typically do IT projects for organizations that have internal IT departments. The term VAR 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 IT departments. A trend that has been gaining ground over the last decade is that fewer VARs exist, as many have moved to the managed IT services model.

Managed IT Services (MSP, or "Managed Services Provider").

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

- Troubleshooting IT problems.
- Setting up and supporting workstations for new and existing employees, both on-site and remote.

To Schedule Your <u>FREE</u> IT Risk Assessment,
please visit **aresgrp.com/assessment** or call our office at 614-495-9658**.**

- Installing and setting up applications such as Microsoft 365, 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 IT problems.
- Monitoring and maintaining the overall health, speed, performance and security of your computer network on a daily basis.
- Regular meetings to gauge progress, discuss the status of your IT environment, and ask for feedback.
- Providing opportunities for you and your staff to learn more about the technology opportunities and risks in the world today.

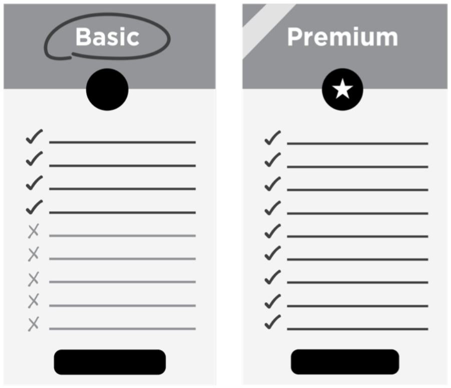
In addition to managing your IT, a good MSP will provide you with an IT Roadmap and budget for necessary projects to further secure your network and improve the stability and availability of critical applications, as well as ensure that your IT systems are compliant with various data protection laws (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 IT Services.

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

However, these are typically scaled-back services, limited to troubleshooting their specific 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 IT department." While it's often a good idea to buy some basic-level support package with a critical software application you use to run your business (often referred to as a "line-of-business" application), this is not sufficient to provide the full IT services, cybersecurity, backup and employee (end-user) support most businesses need.



As an executive looking to get IT support for your organization, 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 IT Services Vs. Break-Fix: Which Is The Better, More Cost-Effective Option?

The advantage of break-fix services is that you only pay for IT 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 IT needs where you don't experience a lot of user problems and don't host or handle sensitive data (medical records, credit cards, Social Security numbers, etc.), break-fix might appear to be the most cost-effective option for you.

However, the downsides of break-fix services are many if you' have more than 20 employees and are attempting to grow in revenue, staff and clients, or if you handle sensitive, protected data. The 6 big downsides are as follows:

1. **Break-fix can be very expensive** when you have multiple issues or a major problem (like a ransomware attack). Because you're not a managed client, the IT company resolving your problem will likely take longer to troubleshoot and fix the issue than if they were regularly maintaining your network and therefore familiar with your environment AND had systems in place to recover files or prevent problems from escalating.

2. **Paying hourly works entirely in your IT company's favor, not yours.** Under this model, the IT consultant can take the liberty of assigning a junior (lower-paid) technician to work on your problem who may take two to three times as long to resolve an issue that a more senior (and more expensive) technician may have resolved in a fraction of the time because there's no incentive to fix your problems fast. In fact, they're incentivized to drag it out as long as possible, given that they're being paid by the hour.

3. **You are more likely to have major issues.** One of the main reasons businesses choose a managed services provider is to PREVENT major issues from happening. As Benjamin Franklin famously said, "An ounce of prevention is worth a pound of cure." The smart way to avoid disasters and minimize the cost and damage is to prevent them from happening in the first place, not hope they won't happen.

4. **You can't budget for IT services** and, as already explained, could end up paying more in the long run if you have to constantly call for urgent "emergency" support.

To Schedule Your FREE IT Risk Assessment,
please visit **aresgrp.com/assessment** or call our office at 614-495-9658**.**

5. **You won't be a priority for the IT company.** All IT firms prioritize their contract managed clients over break-fix clients. That means you get called back last and fit in when they have availability, so you could be down for days or weeks before they can address your problem. Further, because you're not under a contract, the IT company has no incentive to keep you happy or even address the root causes of your problems, which can lead to MORE problems and MORE costs.

6. **If no one is actively maintaining the security of your network and data, your chances of getting hacked go up exponentially.** Believe me when I tell you most people grossly underestimate the costs and damage done by a ransomware attack. Your operations shut down and your client contracts, private e-mails, company financials, employee payroll and other sensitive data are in the hands of criminals who won't think twice about e-mailing your list of employees' and clients' confidential information.

   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 IT company monitor and maintain your company's IT 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 IT environment for an agreed-upon monthly budget can be, by far, the most cost-effective, smartest option for most businesses with 25 or more employees, or who handle critical operations and sensitive data and are risk-averse.

What Should IT Services Cost?

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

We are providing this information to give you a general idea of what most MSPs and IT 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 IT services companies selling break-fix services charge between $125 and $250 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 IT 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 IT consulting firm for a project, I suggest you expect to see 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 IT 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.

- **A detailed List of the equipment (hardware, software, etc.) to be included in the project.** A single line for a server of a single line for certain vendor software licenses may leave you "holding the bag" when you find out you need more – or can't meet business requirements because your vendor quoted you something that looks good – but won't work in your environment.

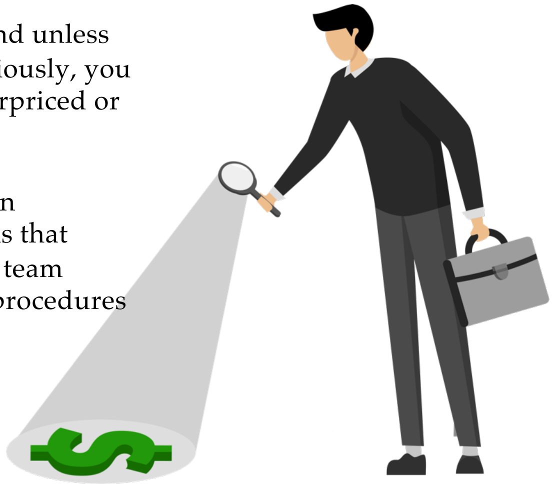
Managed IT Services: Most managed IT services firms will quote you a MONTHLY fee based on the number of devices, users and locations they need to maintain. According to Service Leadership, the average fee per user (employee) ranges from $146.08 per month to $249.73 per month – and those fees are expected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

4 Ways "Cheaper-Priced" IT Firms Hide The TRUE Cost Of Their Services In Their Contracts



As we said previously, no two IT 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 IT provider can end up costing you a lot more due to quoting inadequate solutions that you'll later need to pay to upgrade, poor response that costs your team productivity, or doing rework because they did not have proper procedures to manage your needs.

Here are the 4 most common things "cheaper" IT 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 IT 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 cyber-protections 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. Without these additional protections, you have a higher risk of a cyber-attack, and you also are at risk of being denied an important insurance claim (or denied coverage, period).

2 Inadequate Backup And Disaster Recovery Solutions.

Make sure your IT company includes **daily** backups of your servers as well as CLOUD APPLICATIONS such as Microsoft 365, and other line-of-business applications your control, 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 IT company if that's what they quoted you.

To Schedule Your FREE IT Risk Assessment,
please visit **aresgrp.com/assessment** or call our office at 614-495-9658**.**

3 Nonexistent Vendor Liaison And Support.

Some IT 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). You need to ask how much vendor support is included – and for what specific areas that are included in their services, without extra charges.

4 Cheap, Inexperienced Techs And No Dedicated Account Managers.

Many of the smaller MSPs will hire techs under a 1099 agreement or find cheaper, less experienced engineers to work on your network and systems. Obviously, the more experienced and knowledgeable a tech is on networking and, more specifically, cybersecurity, the more expensive they are. Make sure the company you are considering can explain how they will services your organization *(are they local resources – or from a remote location? Are they W-2 employees or 1099's or outsourced? What is the average years of experience of your helpdesk staff, your network admins, your project engineers? Are their roles segmented – or does the same resource do all 3 roles (helpdesk, network admin, projects?)*

Further, smaller MSPs can't afford dedicated account managers, which means you're depending on the owner of the company (who's EXTREMELY busy) to pay attention to your account and look for problems brewing and critical updates that need to happen, upgrades and budgeting you need. Good account management includes creating and managing an IT budget, a custom roadmap for your business and review of regulatory compliance and security on a routine basis to make sure nothing is being overlooked.

Buyer Beware! In order to truly compare the cost of one managed IT 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 IT 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.

19 Questions You Should Ask Your IT Services Firm Before Signing A Contract

The following are 19 questions to ask your IT 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.

Customer Service:

Q1 How do you request support?

detail: When you have an IT issue you need help with, how do you get support? Do you have to put in a service ticket via your PC? Can you call in to a dedicated help desk or do you have to send an e-mail? If they require you to enter a ticket, what do you do when the Internet is out or your laptop or PC isn't working? Do they have engineers that answer the phone and start helping you right away or do they use a 3rd party answering service or dispatcher – that will have "someone get back with you"? Make sure they explain exactly how they handle IT support requests.

Q2 How do you track response time for working on resolving service requests?

detail: The #1 frustration we hear from business owners about their current IT 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. Ask how they report their response times. Can you see a real time timer for your organization? Can they provide examples of reports they share in your IT Operations meetings? What are their "dropped call" numbers?

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?

detail: How do they provide updates on your requests? Can they share examples of tickets, alerts or major issues? Ask to see their procedure for client ticket entry and Priority 1 status updates?

Q4 Do they create an IT 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 IT with your business goals. Most MSPs don't offer these fractional CIO services, don't know how to put together an IT 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?

detail: Another complaint we hear from new clients is over billing. Either the IT 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. Ask to see an example invoice for your monthly agreement, an out of "agreement" extra charge, and a project invoice to see how they reflect their work efforts.

Q6 Do they have adequate insurance to protect YOU?

detail: Since your IT company is directly maintaining and supporting your critical data and IT 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. They should have at least $1,000,000 in both Cyber-liability AND Errors & Omissions (not just general liability insurance).

Q7 Do they have a dedicated account management team?

detail: 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?

detail: 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.

This is an example of a regulatory requirement that almost all organizations must deal with as a part of their operations. If your current IT company has not talked to you about this (or your regulatory requirements in general), they are putting you at significant risk. Not being aware or choosing not to deal with these requirements is one of the ways cheaper MSPs charge less is because they allow their clients to operate without these critical protections. It becomes not the "bargain" their clients think it is.

Q9 Do they provide you with a regular monthly 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?

detail: Ask for a copy of their IT Operations reports to see an example that shows a status for their network and the updates made to their network from period to period. Ask to see their real time dashboard that reflects status of your IT Operations. Ask to see their reporting to validate you are doing what you committed to do in your Cyber-Liability insurance policy?.

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"?

detail: All clients should receive this in written and electronic form at no additional cost.

If your current IT 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 IT company to have that much control over your company. If you get the sneaking suspicion that your current IT resource is keeping this under their control as a means of job security, evaluate your expectations and options as this is very dangerous to your dangerous to your organization, so don't tolerate it!

Q11 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?

detail: as a means of transferring their risk, approximately 65% of organizations 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 – or pay your claim. If your IT 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 IT 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:

Q12 Do they INSIST on immutable backups for your data?

detail: 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 IT firm, they should not only know about this type of backup, but insist you have it.

Q13 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?

detail: Regular test restores of your backups 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.

Q14 Do they insist on backing up your network BEFORE performing any type of project or upgrade?

detail: Ask your team to show you the "project plan" It's simply as a precaution in case a hardware failure or software glitch causes a major problem.

Q15 If you were to experience a major disaster, such as an office fire or ransomware attack, does your IT resource you have a written plan for how your network could be restored FAST and/or enable you to work from a remote location?

detail: Having an Incident Response Plan is a key part of your cyber risk management approach. "Call the IT team" is not an effective plan today. The plan has multiple parts that get you back up and running quickly WHILE ensuring you follow the expectations of your cyber liability insurance are met so your claim will get paid.

Technical Expertise And Service:

Q16 Is their help desk U.S.-based or outsourced to an overseas company or third party?

detail: If your support team is not a part of your provider's staff, you risk multiple challenges – from language and knowledge issues to commitment focus as your resources aren't local and understand the Ohio approach to work efforts. This is one of the most important aspects of customer service, plus we feel it's important to keeping your data secure.

Q17 Do their technicians maintain current vendor certifications and participate in ongoing training – or are they learning on your dime?

detail: Ask about your providers staff certifications and training programs. Our engineers are scheduled to attend over 80 hours of technical and customer service training each year. Certifications are tracked and expected to validate technical capabilities and performance. This provides reassurance that the resources working in your environment have the training and experience needed to successfully complete their tasks.

Q18 Do their technicians conduct themselves in a professional manner?

detail: Engineers/technicians should be professionals who are not only polite, but trained in customer service, communication and high standards. They should be able to minimize "geek-speak," and not talk down to you. If they have to be on-site at your office, you should be proud to have them there. We believe these are minimum requirements for delivering a professional service.

Q19 When something goes wrong with your Internet service, phone systems, printers or other IT services, do they own the problem or do they say, "That's not our problem to fix"?

detail: Your IT provider should own the problem for you so you can focus on your responsibilities – that's just plain old good service and, while it may not be fun, it is a part of the role of the IT team.

To Schedule Your FREE IT Risk Assessment,
please visit **aresgrp.com/assessment** or call our office at 614-495-9658**.**

Are You Done With Frustrating IT Support And Never-Ending IT Problems?

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

If you want to find an IT company you can trust to do the right thing, the next step is simple: call my office at 614-495-9658 and reference this report to schedule a brief 10- to 15-minute initial phone consultation.

On this call we can discuss your unique situation and any concerns you have and, of course, answer any questions you have about us. If you feel comfortable moving ahead, we'll schedule a convenient time to conduct our proprietary Cyber-Readiness Review.

This Assessment can be conducted with or without your current IT company or department knowing (we can give you the full details on our initial consultation call). **At the end of the Assessment, you'll know:**

- ✓ Your risks that are currently in your environment that can be exploited by criminals to stop your productivity and steal your data.
- ✓ If you are meeting the expectations of your Cyber Liability Insurance carrier regarding your responsibilities to protect your environment form cyber risks.
- ✓ The odds of your ability to recover quickly and effectively in the event of a cyber incident.
- ✓ The potential real costs you could incur to recover form a cyber incident or other downtime event in your IT environment.
- ✓ What to focus on to minimize your risks and exposures via an executive Action Plan

Fresh eyes see things that others cannot – so, at a minimum, our Cyber-Readiness Review is a completely risk-free way to get a credible third-party validation of the security, stability and efficiency of your IT 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 IT services and support you need.

To Schedule Your FREE IT Risk Assessment,
please visit **aresgrp.com/assessment.**
or call our office at 614-495-9658**.**

Dedicated to serving you,

Michael Moran,
President Affiliated
Phone: 614.495.9658
E-mail: michaelmoran@aresgrp.com

See What Other Executives Are Saying:

Affiliated Provides Experienced Strategic IT Planning For Expansion And Growth

From setting the strategy with our IT team to coordinating hardware and software purchases and infrastructure upgrades to collaboration on projects and troubleshooting issues, Affiliated brings a high level of experience to every facet of our IT ecosystem. And because the entire Affiliated team has taken the time to understand our business and needs, they have been critical to our success in aligning our IT department's goals with our overall company goals. It is a strong partnership and has been for 10 years.

– CFO
Power Equipment Distributer

Affiliated Took Immediate Ownership Of Our Challenges

As one of the largest office furniture companies in Columbus, with over 30 employees, we needed a more strategic and effective approach to our IT that would increase our productivity and build a more organized approach for long-term success. Affiliated brought a comprehensive expertise and support we could not handle independently. Their team took immediate ownership of our challenges and provided solutions, demonstrating their genuine interest in seeing our business succeed. Partnering with Affiliated has given our company the ability to grow with confidence.

– CFO
Office Design Company

Always Have Our Best Interest In Mind

There's no doubt about it: Affiliated has helped us create a smarter, more streamlined business. They are a trusted advisor we can count on to make recommendations with our best interests in mind. For example, Affiliated has helped our IT department maximize cost savings across the board (actual savings are 12% to 18% annually) while improving our security and business continuity. With Affiliated running our IT, we're better positioned to innovate, collaborate, and take advantage of new opportunities more quickly.

– President
Custom Heavy Vehicle Manufacturer

Affiliated Is A Great Partner To Our Business

Affiliated has been our Managed Services firm since 2019, handling all of our IT needs, including employee support, backups, multi-factor authentication, and Microsoft licensing needs. With their knowledge, experience, and quick response times, we never have to worry about our staff's IT needs being met. Not only is Affiliated trustworthy and dependable, but their team is also very easy to work with—a great partner to our business.

– Office Manager
Finance Fund

See What Other Executives Are Saying:

Affiliated's Value And Services Have Exceeded Our Expectations

The biggest benefit to our company has been the speed, professionalism and value of the services that the Affiliated team has provided. We need our systems up and available to keep us productive - we must deliver to our customers on time. Our employees have found Affiliated’s Helpdesk easier to work with and more responsive than our previous providers. Getting problems solved quickly is important and has dramatically reduced our downtime. Our management team now spends its IT time deciding on recommended turnkey options, not trying to validate solutions - and then managing to get them installed correctly.

– ***President***
Custom Manufacturer

Affiliated Solved Issues Our Past Vendor Couldn't

Working with Affiliated has been a night and day difference from our past IT vendors. Their ability to proactively resolve issues - issues our past IT Firm couldn't or wouldn't resolve - has had an immediate impact on our business and employees. Right from the start, they listened, quickly understood our primary business needs, and tailored their services to meet those needs The most significant benefit is how they quickly and efficiently respond to our employee requests by identifying and solving problems to keep us productive. They have also done a fantastic job training our teams to protect our organization and get the most out of our software solutions. And for me, Affiliated has given me back a lot of my personal and professional time so I can focus on our core business. We are very happy that we made the change to Affiliated.

– **Vice President**,
Real Estate Development Company

To Schedule Your <u>FREE</u> Assessment,
please visit **aresgrp.com/assessment** or call our office at 614-495-9658**.**

About The Author

Mike Moran is the co-founder and president of Affiliated, a cybersecurity, IT compliance, and IT managed services company based in Columbus, Ohio. With more than 30+ years of business technology consulting experience, Moran leads Affiliated's company-wide strategy, marketing, and corporate development activities.

Mike has a proven track record for successfully helping organizations align their business and technology goals then identify and implement technology-based solutions that increase operational efficiencies, improve customer experience, and drive more profitable revenue.

Founded in 1993, Affiliated has grown into a multi-million-dollar technology and business consulting company serving growing and mid-market businesses throughout Greater Columbus and Central Ohio.

Affiliated specializes in serving businesses and organizations in the distribution/logistics, manufacturing, healthcare, non-profit, government and professional services industries.

Affiliated's services and solutions helps our customers

- ✓ Align their IT systems and resources to achieve their business goals
- ✓ Mitigate their risks – with security intelligence to provide the ability to detect and respond before the disaster happens, preventing disruptions, and ensuring minimum downtime
- ✓ Better manage their true IT costs
- ✓ Enhance their staff and IT team's effectiveness with our tools and processes

For more information and assistance, contact Mike at 614-495-9658 or michaelmoran@aresgrp.com.