I.T.

Buyers Guide

TECHSPERT
data services LLC

Northeast Ohio's Small Business Guide to I.T. Support

What A Small Business Should Expect To Pay for IT Services Support

(And How to Get *Exactly* What You Need Without Unnecessary Extras, Hidden Fees and Bloated Contracts)

Read this guide and you'll discover:

- ✓ The two 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, the customer, when buying I.T. services; you'll 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.
- ✓ How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate.
- ✓ 21 revealing questions to ask your I.T. support firm BEFORE giving them access to your computer network, e-mail and data.

From The Desk Of: Adam Siemienski
CEO, Techspert Data Services, LLC

Dear Colleague,

If you are the owner/CEO/President of a business in Northeast Ohio, that is currently looking to outsource some or all of the IT support for your business, this report contains important information that will be extremely valuable to you as you search for a competent firm you can **trust**.

My name is Adam Siemienski, President of Techspert Data Services, LLC . We've been providing technology services to businesses in the Cleveland/Akron/Canton area for over 20 years. You may not have heard of us before, but I'm sure you're familiar with one or more of the many businesses who are clients of ours.

One of the most commons questions asked in our industry is "What do you guys charge for your services?" Since this is such a common question — and a very important one to address — I decided to write this report for 3 reasons:

1. I wanted an appropriate way to answer this question and educate all prospective clients who come to us regarding the most common ways Technology Services companies package and price their services, and the pros and cons of each approach.

2. I wanted to bring to light a few ***industry secrets*** about technology service contracts and SLAs (service level agreements) that few business leaders think about, understand or know to ask when evaluating IT service providers, that can end up burning you with hidden fees and locking you into a long-term contract when they are unwilling or unable to deliver the quality of service you expected.

3. I wanted to educate business leaders on how to pick the best Technology Servives company for their specific infrastructure, budget and unique needs based on the ***VALUE*** the company can deliver—***for the right price***.

In the end, my purpose is to help you make the most informed decision, resulting in working with the right company 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 your cybersecurity, productivity, and minimal downtime,

Techspert Data Services, LLC
Adam Siemienski, President
Phone: 330.441.4426 x104
E-mail: ajsiemienski@techspert-data.com
www.techspert-data.com

About The Author

Techspert Data Services grew out of a long-time passion for computers and networking by its founder Adam Siemienski since he was in grade-school and the start of the personal computer craze in the mid-80's. After high school, a search for degrees for computer networking didn't exist so Adam opted for engineering. Working as many jobs as necessary to pay for college, a Mechanical Engineering degree (BSME) was earned from the University of Akron with which Adam began his professional career as a junior Mechanical Engineer at a steam generating plant in Cleveland Ohio, focusing more on any chance to help support the corporate data network. An opportunity to teach as a Microsoft Certified Trainer was Adam's break into the I.T. world. Next a partnership with a local construction accounting software developer, to a network engineer for the largest technology consulting company in NE Ohio at the time.

Adam continued building client relationships and supporting small business networks during evenings and weekends all the while running the helpdesk for a local 450-user health insurance company in Akron.

For over 23 years, Techspert has provided technology expertise to Northeast Ohio customers with 10 to 100's of users, ***specializing in the Manufacturing, Construction, and Professional Services Industries.***

We strive for long relationships with our customers. Our philosophy has always been to minimize downtime to keep businesses productive, for the right price. Our network engineers and technicians are highly trained and skilled for the most challenging infrastructures. We look to employ only those individuals who can support our clients technically, but also interact with business owners to explain inherent technology risks and how to mitigate them. Ransomware, for example, is a true threat for every business and we provide tested solutions to minimize both the possibility or effects.

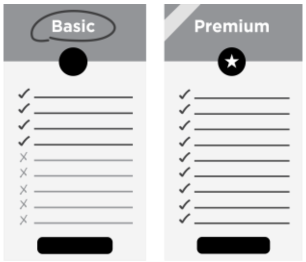
Technology Experts. It's in our name!

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

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

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

- **Managed I.T. Services.** This is a model where the IT services company takes the role of your ***fully outsourced IT department*** and not only installs and supports all the devices and PCs that interconnect, but also offers remote and on-site helpdesk support, device and network cybersecurity, backup and disaster recovery options, and a host of other services to monitor and maintain the health, speed, performance and security of your data infrastructure to minimize downtime.



- **Software Vendor-Supplied I.T. Services.** Many software companies will offer 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 application and NOT your entire computer network and all the applications and devices connected to it. If your problem resides outside of their specific software or the server it's hosted on, they can't help you and will often refer you to "your 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, this is not enough to provide the full I.T. services and support most businesses need to stay up and running.

When looking to outsource your I.T. support, the two service models you are most likely to end up having to choose between are the "managed I.T. 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.

To Schedule Your FREE Assessment,
please visit **https://techspert-data.com/initial-consultation-success/** or call our office at **216.800.7800**

Managed I.T. Services Vs. Break-Fix: Which Is The Better, More Cost-Effective Option?

Under the break-fix model, there could be a conflict of interest between you and your technology support company. The technology services company can't prevent problems, stabilize your network or resolve problems quickly and since they are paid by the hour, the risk of unforeseen circumstances, growing project scope, learning curve inefficiencies and outright incompetence are all shifted to YOU, the customer. Essentially, the more problems you have, the more they profit, which is precisely what you DON'T want.

Under this model, the technology 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. There is no incentive to properly manage the time of that technician or their efficiency, and there is every reason for them to prolong the project and to find MORE problems than solutions. Of course, if they're ethical and want to keep you as a client, they should be doing everything possible to resolve your problems quickly and efficiently; however, that's akin to putting a German shepherd in charge of watching over the ham sandwiches. The temptation may be too great!

It also creates a management problem for you, the customer, who now has to keep track of the hours they've worked to make sure you aren't getting overbilled; and since you often have no way of really knowing if they've worked the hours they say they have, it creates a situation where you really, truly need to be able to trust they are being 100% ethical and honest AND tracking THEIR hours properly (not all do). And finally, it makes budgeting for technology projects and expenses a nightmare since they may be $0 one month and $1000's the next.

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

The ever-increasing dependency we have on technology systems and the data they contain — not to mention the type of data we're now saving digitally — has given rise to highly sophisticated cybercrime organizations who work around the clock for one outcome: to steal your data and hard-earned money.

As you may be aware, ransomware (the infectious and malicious software that encrypts all your data for monetary ransom) is at an all-time high because these criminals combined now make $BILLIONS robbing businesses.

To Schedule Your FREE Assessment,
please visit **https://techspert-data.com/initial-consultation-success/**or call our office at **216.800.7800**

Other risks involve criminal hackers gaining access to bank accounts, credit card or passwords to rob you and potentially even worse—your clients too! Some may use your company's technology infrastructure to perform their malicious intent by sending malicious spam email under the guise of YOUR domain, host pirated software for illegal distribution, or other malicious software to help infect other businesses.

These criminals aren't the envisioned lowly solo hackers in their dark hoodies in their basements. Cyber criminals are now at the Nation State level and highly funded by enemy governments such as China, Russia, North Korea, and Iran. They are highly organized and efficient BUSINESSES with thousands of employees just like their legitimate counterparts with the sole intent of disruption, mayhem, stealing Intellectual Property, and your money. Targets are not picked by their size or amount of revenue. Targets are ANYONE with a computer because the processes are automated to find a crack and THEN the attacker takes a personal interest to inflict the maximum damage.

Of course, this isn't the only technology risk you face. Other common disasters such as rogue employees, lost devices, hardware failures, fire, natural disasters, and a host of other issues can interrupt or outright destroy your digital assets (data). Not to mention all the current and upcoming regulatory compliance for specific industries.

Should You Just Hire A Full-Time I.T. Manager?

In many cases small businesses under 100 employees find it difficult to financially justify a full-time employee to maintain their technology infrastructure for the following reasons:

1. **Cost of expertise.** Highly-skilled individuals come at a price and that price (salary and overhead) is in a range far higher than the cost of employing a Managed Service Provider (MSP). The most basic networks require a skillset now commanding $50K+ salaries.
2. **Level of expertise.** No single person has the expertise to handle EVERY technology challenge, especially in the critical area of cybersecurity. Once a situation goes beyond that person's level, outside consultation is needed and is costly. And if your business is substantial enough to justify full-time technology staff, the roles necessary to sustain will probably require multiple individuals: helpdesk, network engineer, network administrator, a CIO (chief information officer) and a CISO (chief information security officer).
3. **PTO/Vacation/FMLA/Bereavement.** What happens when an event occurs that require the expertise of a staff member who isn't available? You may have to hire outside consultation to get by.
4. **Hiring the right person.** Does HR understand technology enough to hire the right person for the job? Without the intrinsic knowledge of the positions for which they are hiring, this can lead to a huge waste of time and money.

As demonstrated, hiring internal may not be the best, most cost-effective solution. This is where MSP's shine and can literally save a company $1000's.

Important! Please note that the following price quotes on the following pages are industry averages based on a recent I.T. industry survey conducted of over 750 different I.T. services firms. We are providing this information to give you a general idea of what most I.T. services firms 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, which is simply to understand exactly what you want to accomplish FIRST and then customize a solution based on your specific needs, budget and situation.

What Should You Expect To Pay?

Hourly Break-Fix Fees:

Most I.T. services companies selling break-fix services charge between $175 to $250 per hour (depending on the complexity—ex. Desktop PC vs. Server) with a one-hour minimum. In most cases, they will give you a discount of 5% to as much as 20% on their hourly rates if you purchase and pay for a block of hours in advance.

If they are quoting a **project**, the fees range widely based on the scope of work outlined. If you are hiring an I.T. consulting firm for a project, I suggest you demand the following:

- **A very detailed scope of work that specifies what "success" is.** Make sure you detail what your expectations are in performance, workflow, costs, security, access, etc. The more detailed you can be, the better. Detailing 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 loose 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.

Managed I.T. Services:

Most managed I.T. services firms will quote you a MONTHLY fee based on the number of devices/users/mailboxes/etc. they need to maintain, back up and support. In Northeast Ohio, that fee is somewhere in the range of $150-$300 per supported user per month.

If you hire an I.T. consultant and sign up for a managed I.T. services contract, here are some things that SHOULD be included (make sure you read your contract to validate this):

- ✓ Anti-phishing email filter
- ✓ Operating systems (Windows/Mac/Linux) security patches applied weekly, and immediately for urgent and emerging threats
- ✓ Third-party software patching
- ✓ EndPoint Firewall management and monitoring
- ✓ Application control/zero-trust whitelisting
- ✓ 24x7x365 computer and server proactive monitoring and alerting

The following services may **NOT be included** and will often be billed separately. This is not necessarily a "scam" or unethical UNLESS the managed I.T. services company tries to hide these fees when selling you a service agreement. Make sure you review your contract carefully to know what is and is NOT included!

- ✓ Hardware (ex. new servers), PCs, laptops, etc.
- ✓ Software licenses
- ✓ Special projects

Warning! Beware the gray areas of "all-inclusive" service contracts. In order to truly compare the cost of one managed technology services contract to another, you need to make sure you fully understand what IS and ISN'T included AND the SLA *or service level agreement* for which you are signing. It's VERY easy for one technology services provider to appear far less expensive than another UNTIL a detailed comparison reveals the important difference. .

The following are 21 questions to ask your I.T. services provider that will clarify exactly what you're getting for the money. Some of these items may not be that important to you, while others (like response time, adequate insurance and uptime guarantees) 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 An I.T. Services Company Before Hiring Them For I.T. Support

Customer Service:

Q1 How difficult is it to transition from the old I.T. services company?

Our Answer: Our Standard Operating Procedures were designed to make this transition as painless as possible. We simply install a device on the network that immediately begins inventorying devices. Once our system is finished, we can then deploy our Endpoint Protection and other tools —all the while end-users aren't even aware. We distribute instructions on how to contact us for support and it's that easy!

Q2 Do you offer after-hours support, and if so, what is the guaranteed response time?

Our Answer: Any reputable technology services company should answer their phones LIVE (not voice mail or phone trees) and respond during normal business hours and customize it for special circumstances (fees may apply!) since many clients work outside normal hours. We offer 24x7 support and respond LIVE within 60 or less. Resolution times will vary depending on the complexity of the incident. Emergency incidents will always take precedent and may affect resolution times for non-emergency incidents.

Q3 Do you have a written, guaranteed response time for problem resolution?

Our Answer: Most technology services companies offer a 60 or 30-minute response time to your call during normal business hours. Be very wary of companies without documented response times which may be a sign of disorganization, over utilization, and/or inexperience. Our response time goals start at just 15 minutes.

Q4 How do we contact you for support?

Our Answer: Once a go-live date is established, we distribute to whomever is authorized, a complete welcome document that explains all methods for contacting our support technicians. You can email, call, or create your own incident through your access to our Professional Services Automation (PSA) system which creates incident tickets that will keep track of every request and all the pertinent details through resolution.

Q5 Do we get a dedicated person to service our requests

Our Answer: Each client is assigned a primary technician and 2 other backups in order to spread the availability for quicker incident resolution. Our systems allow for the sharing of all your company details, including previous resolutions so that anyone on the team has access to the same exact information to assist you as quickly as possible.

Q6 What does your managed technology services and support consist of?

Our Answer: Managed Service Providers (MSPs) must be able to proactively monitor for problems and perform routine maintenance on your systems. They must have some form of ticketing AND Remote Monitoring and Management (RMM) system to be effective at supporting your infrastructure. Without these and many other tools (we call our technology stack), they are not a true MSP and you will want to look elsewhere. Our systems continuously monitor your technology infrastructure observing for developing problems, security and other issues, so they can be alerted and addressed BEFORE they turn into bigger problems.

Q7 What is NOT included in your managed services agreements?

Our Answer: Another gotcha many technology services companies fail to explain is what is NOT included in their monthly managed services agreement that will trigger an invoice. If they offer an all-you-can-eat, you should be wary of many gray areas that will exist. Reputable MSP's reveal the limitations to their inclusive agreements and are up-front about these types of projects. It's very common for projects not to be included, like a server upgrade, moving offices, adding offices, adding new employees and, of course, the software and hardware you need to purchase to run your business. Be certain to obtain an accurate list of areas of support outside the agreement and typical examples of projects.

Our TotalCare managed services agreement is completely transparent and covers all listed maintenance items under management. Our scope of uncovered services is well documented and examples include:

- Parts, equipment or software not covered by vendor/manufacturer warranty or support.
- The cost of any parts, equipment or shipping charges of any kind.
- The cost of any software, licensing, or software renewal or upgrade fees of any kind.
- The costs of any 3rd party vendor or manufacturer support or incident fees of any kind.
- Failures due to acts of God, building modifications, power failures or other adverse environmental conditions or factors.

Q8 Is your help desk local or outsourced?

Our Answer: Be careful because smaller IT companies may outsource this critical function. As a result, you may get a tech who is not familiar with you, your network, previous problems and personal preferences. Or worse, they may not be qualified. This can be frustrating and lead to the same problems cropping up over and over, longer resolution time and you having to spend time educating the tech on your account.

Our local, dedicated resolution team of technicians will get to know you, your company, as well as your preferences and history so they'll be more capable of successfully resolving your IT issues and handling things the way you want.

Q9 How many engineers do you have on staff?

Our Answer: The real question is probably; Do you have enough technicians to handle our company size? What we have found is that the majority of customers (up to hundreds of computers) can be successfully managed by a support team of 3 technicians: one main contact who handles the majority of incidents, and another two for proper incident resolution times per the goals in the agreement. We make certain we maintain the number of employees necessary to manage all our partners.

ALSO: Ask how they will document fixes, changes, and credentials for you organization so if one tech is out or unavailable, another one can step in and know your network settings, history, previous issues, etc. and how those issues were resolved. This is important or you'll be constantly frustrated with techs who may need to start from scratch to resolve an issue which may mean more downtime and thus, less productivity.

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

Our Answer: Network documentation is exactly what it sounds like: the practice of maintaining detailed technical records about the assets you own (computers, devices, software, directory structure, user profiles, passwords, etc.) and how your network is set up, backed up and secured. Every technology support company should offer this to you in both written (paper) and electronic form at no additional cost and update it as necessary.

Why is this important? There are several reasons:

First, it shows professionalism and integrity in protecting YOU. No technology support person or company should be the only holder to the keys of the kingdom. Because we document your network assets and passwords, you have a blueprint you can give to another technology support person or company to take over if desired.

Second, good documentation allows the engineers working on your account to resolve problems faster because they don't waste time rediscovering and troubleshooting your network trying to find things and uncover accounts, hardware, software licenses, etc.

Third, if you had to restore your network after a disaster, you'd have the blueprint to quickly put things back in place as they were.

Finally, and most important, if you ever need to switch technology support providers, your replacement company will be able to take over quickly because the network has been documented properly.

All of our clients can receive this in electronic form at no additional cost. We also perform updates as necessary for all documentation that belongs to you and is available by request at any time.

Q11 How often do you meet with us to discuss our Strategic Business Reviews?

Our Answer: Our SBR's are provided annually or more often as necessary as in the case of new threats that were previously unknown.

In these meetings, we provide you with the status updates of projects we're working on and the health and security of your network. We also make recommendations for new equipment and upgrades you'll be needing soon or sometime in the near future. Our vCIO meetings with you are decision maker discussions that cover current risks and their mitigations, business goals, improvements in our service delivery, technology services budget, critical projects, compliance issues where applicable, known problems and cyber security best practices.

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

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

Our Answer: Make sure you carefully review the cancellation clause in your agreement. Many technology support companies hold their clients hostage with long-term contracts that contain hefty cancellation penalties and will even sue you if you refuse to pay.

We will never force a client to stay with us if they are unhappy for any reason. We request the opportunity to resolve any stated grievances, but beyond that our clients are only obligated to pay the remainder for specific assets for which we've invested for the term of the original agreement. An example may be the cost of the managed firewall we've included in the agreement.

To Schedule Your FREE Assessment,
please visit **https://techspert-data.com/initial-consultation-success/**or call our office at **216.800.7800**

Q13 What are the most common breach points for all networks?

Our Answer: This answer is a bit subjective, but a prospective technology services company should be able to rattle off at least a few areas.

Techspert has identified the 6 most common breach points in every network, and we've tailored our solutions to defend those breach areas, so our clients don't have to worry about ransomware. And should a breach occur (no solution is 100%!) our incident response (what is done AFTER a breach to get you up and running again) is built on industry best practice with highly effective recovery procedures which minimize downtime and loss of data. To date our customers have never been afflicted but we know the possibility exists, so we aren't resting on our laurels, and constantly monitor the threat horizon to improve our cyber defenses.

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

Our Answer: The key is that they HAVE an answer and don't hesitate to provide it. Some of the things they should mention are:

- 2FA (two-factor authentication) or MFA for Multi-factor Authentication
- Advanced end-point protection, NOT just antivirus
- Security Information an Event Management (SIEM)
- Zero-trust application control
- Secure WiFi
- Network Segmentation or VLAN's

Because a combination of these lockdown strategies are essential to protecting your network and data, we employ all relevant strategies we deem necessary for the cyber defenses for our high-level of cyber defenses.

Q15 What cyber insurance do you carry to protect me?

Our Answer: Here's another way to approach this topic. You can ask "if YOU cause a problem with our network that causes downtime and thus loss of productivity and/or other assets, who's responsible? What if one of your technicians gets hurt at our office or damages our property while there?"

In our overly litigious society, it's better to be certain that your chosen technology services company is adequately insured with both errors and omissions insurance, workers' compensation and cyber liability. It is advisable to request their policy for review.

If you get hit with ransomware due to their negligence, someone has to pay for your lost sales, the recovery costs and the interruption to your business operations. If they don't have insurance to cover YOUR losses of business interruption, they might not be able to pay, and you'll have to end up suing them to cover your costs. If sensitive client data is compromised, who's responsible for paying the fines that you might incur and the lawsuits that could happen? No one is perfect, which is why you need them to carry adequate insurance.

We do keep our $1MM+ EPLI, E and O, and Cyber Insurance policies active and renewed annually.

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 reputable technology services company will have an independent third party reviewing and evaluating their company cybersecurity for best-practices.

We've partnered with multiple third-party companies that assist in our development of our best-practice and cybersecurity standards and standard operating procedures. Our operations are under continual review, and we discuss in detail as often as necessary with these partners. In doing so, we too practice what we preach and have many eyes peering at our operations to ensure both our and our clients' assets are safe under our management.

To Schedule Your FREE Assessment,
please visit **https://techspert-data.com/initial-consultation-success/** or call our office at **216.800.7800**

Q17 Do you have a SOC?

Our Answer: A SOC (pronounced sock), or security operations center, is a centralized department or entire company solely utilized for cybersecurity and defense with the capabilities for all aspects of reporting including regulatory and compliance.

This functionality is CRUCIAL to the success of your cyber defenses and is certainly a deal-beaker should the prospective technology services company not have one or is not partnered with one to provide these necessary services.

Our dedicated SOC partner provides the necessary and relevant services to help ensure all layers of cyber security and defense are in place and operating correctly both at our Network Operations Center (NOC) and your company.

Backups And Disaster Recovery:

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

Our Answer: There are two aspects to backing up your data that most business owners don't realize. The first is fail over and the other is fail back. As a comparison, if you get a flat tire, you would fail over by putting on the spare tire to get to a service station where you can then fail back to a new or repaired tire.

Depending on the type of disaster, you'll need to fail back internally or via the cloud in the case of natural disasters such as fire, flood, tornados, etc. Without offsite backups, your business would cease in a natural disaster scenario

Our standard Recovery Time Objective (RTO)—how long it will take to get you operational after a hardware failure– is one day or less. This is a common standard. We can provide shorter RTO's but costs can exponentially increase as you shorten this timeframe. Critical operations should be considered when discussing your RTO requirements. Our standard is only a default, and we can't answer the question "How long can you afford to be down?" for you.

Q19 Do you INSIST on performing periodic test restores of our backups to make sure the data is not corrupt and could be restored in the event of a disaster?

Our Answer: A reputable technology services company will require a DAILY test to ensure entire backup images are available and bootable! In addition to this, they should periodically perform test restores of files from backups to make sure your data CAN be recovered in the event of an emergency.

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

Verifying your backups daily and literally testing them on a regular basis, is a cornerstone of a successful overall Business Continuity and Disaster Recovery plan.

TIP: Ask your I.T. provider about the 3-2-1 or 3-2-1-1 rule of backups. The 3-2-1 rule is that you should have three copies of your data: 2 local copies of your data (working and backed up) plus an additional 1 copy offsite (cloud). The 3-2-1-1 or 3-2-2 rule adds an additional immutable or air-gapped copy that is read-only and cannot be degraded by ransomware or any other malware.

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

Our Answer: If COVID-19 taught us anything, it's that work-interrupting disasters CAN and WILL happen when you least expect them. Fires, floods, hurricanes and tornadoes can wipe out an entire building or location. C-19 forced everyone into lockdown, and it will happen again.

Your prospective MSP should have secure methods and solutions for a remote workforce and should be able to explain in detail how that would work for you.

Our secure multi-factor authentication VPN's and site-to-site VPN's have enabled our clients to work from anywhere, regardless of the situation. Our customized remote solutions will allow the necessary and authorized access to your data any time from anywhere.

Q21 Show me your process and documentation for disaster recovery.

Our Answer: The reason for asking this question is to see if they HAVE SOMETHING in place. A plan, a procedure, a process. Don't take their word for it. Ask to SEE it in writing. What's important here is that they can produce some type of process. Further, they should be able to explain how their process works.

One thing you will need to discuss in detail is how they would take over your current I.T. company (see Q1).

To Schedule Your FREE Assessment,
please visit **https://techspert-data.com/initial-consultation-success/**or call our office at **216.800.7800**

Other Things To Consider:

Are they good at answering your questions in terms you can understand and not in arrogant, confusing *geek-speak*?

Being able to effectively communicate to a customer at THEIR level is highly important. We train our technicians to handle all levels of experience.

Our technicians are trained to take time to answer your questions and explain everything in simple terms.

> *I felt fairly confident regarding Cybersecurity with the previous firm I was with, however after learning from you and talking through our current set up, I am nervous we are at risk without further intervention. Techspert's overall knowledge with current threats and how they change daily made me realize I was missing this important component with my previous vendor. In addition, setting up older proprietary shop related machines was missing.*
>
> *Also, Techspert's risk assessment demonstrated how we may be currently and unknowingly exposed. Business is hard enough when everything goes right. To be down an extended period of time in today's world because of computer issues is too much of a hardship.* ***– Tim Gorbach, Treasurer, A&C Welding, Inc.***

Do they have expertise in helping clients like you?

Our decades of experience specializing in the construction and manufacturing industries has enabled us to quickly evaluate and understand these types of business processes and offer tried and tested solutions. We've many customers outside of these industries too!

To Schedule Your FREE Assessment,
please visit **https://techspert-data.com/initial-consultation-success/**or call our office at **216.800.7800**

A Final Word and Free Offer To Engage With Us

I hope you have found this guide helpful and enlightening. We've spent decades on perfecting or systems and have detailed our experiences herein for your benefit. As I stated in the opening of this report, my purpose in providing this information was to help you make an informed decision and avoid getting burned by incompetent or unethical companies luring you in with cheap prices.

The next step is simple: call our office at 216-800-7888 and reference this letter to schedule a brief 15-minute initial consultation.

On this call we can discuss your unique situation, any concerns you have, and of course, answer any questions you may have about us. If you feel comfortable moving forward, we'll schedule a convenient time to conduct our proprietary 27-Category Technology Review.

FREE Cybersecurity Risk Assessment

*This is **completely free**, and without obligation or expectation for you to hire us. We hope once you experience our professionalism, expertise, and transparency, that you'll want to engage in a long-lasting mutually beneficial business relationship.*

To Schedule Your FREE Assessment,
please visit **https://techspert-data.com/initial-consultation-success/**or call our office at **216.800.7800**

This Assessment can be conducted with or without your current technology service company or department knowing (we can give you the full details on our initial consultation call).

Your time investment is minimal: 15 minutes for the initial phone consultation and about one hour for the second meeting to go over what we discover). **At the end of our process, you'll know:**

- Where you are overpaying (or getting underserved) for the services and support you are currently getting from your current I.T. company or team.
- Are your I.T. systems truly secured from hackers, viruses and rogue employees?
- Are your backups configured properly to ensure that you could be quickly back up and running again after a disaster?
- Are you unknowingly exposing your company to expensive fines and litigation under new Ohio data breach laws (where applicable)?
- Could you utilize cheaper and more efficient cloud computing technologies to lower IT costs and make it easier to work remotely?
- Are your systems optimized for maximum speed and performance?

Ultimately, we'll provide you with an *EASY-TO-UNDERSTAND* assessment of our findings with green, yellow, and red indicators of risk. Your overall score is based on the 27 categories and will demonstrate any areas of cyber defense vulnerabilities, potentially troublesome devices, business continuity and disaster recovery risks, etc. We'll also provide you with an Action Plan on how to remediate any less than favorable situation or problem we discover – and if you choose, we can assist you in its implementation.

With my personal 30+ years of experience, I can practically guarantee I will find specific vulnerabilities and breach areas in your network. And if nothing else, our Risk Assessment is an easy and no-cost or obligation method for a valid third-party assessment to verify your security and give you peace of mind.

Dedicated to your cybersecurity, productivity, and minimal downtime,

Adam Siemienski, CEO
Techspert Data Services, LLC

To Schedule Your <u>FREE</u> Assessment,
please visit **https://techspert-data.com/initial-consultation-success/** or call our office at **216.800.7800**

What Our Clients Have To Say

"I am very secure in knowing that I have the right company working on my network to keep our environment safe and secure. I can't compare other IT companies with Techspert because we've been doing business for over 20 years! I would highly recommend Techspert Data Services to any business."
– Sharon Lunato, CEO, Relmec Mechanical LLC

"When it comes to Techspert's cybersecurity expertise, we feel like we are in a very safe place with the measures that have been implemented. The steps we have taken are a big deterrent to anyone with malicious intentions. Also, Techspert is exceptionally responsive and tentative to any questions or issues that come up. Previous IT companies I've dealt with have been challenging to get a hold of, especially when you need them the most. The outsourcing technology services requires trust and I completely confide in the Techspert team to manage and protect all our sensitive data."
–Chris Sheiban, Vice President, Sheiban Jewelers

"With Techspert's expertise and experience, we feel very secure. Techspert is the only IT firm I've worked with and I don't care to ever find out about any others. I'd recommend Techspert to anyone I know. It's invaluable to be able to go to an IT firm with problems big or small and have them fixed as quickly as possible.."
– Jonathan Collins, Diamond Steel Construction Co.

"I'm confident that Techspert is continually pro-active against threat actors. We have yearly discussions at minimum to provide updates and upgrades to our system to keep our company as safe as possible. We have trusted, and have worked with Techspert so long, there is not much of a comparison to make. Their response time is almost always immediate, and there is always someone on their team to help solve our problems. I would gladly share their expertise with anyone. I have recommended Techspert to others and will continue to do so.."
– Ben Yost, Yost Foods, Inc.

Check out many more on our website:
https://techspert-data.com/testimonials/