The Goshen's Business Owners' Guide To IT Support Services And Fees

What You Should Expect To Pay For IT Support For Your Small 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.

✓ 5 ways "cheaper" IT firms hide the TRUE cost of their services in their contracts.

✓ 20 critical questions to ask your IT support firm BEFORE signing an agreement.

Provided as an educational service by:
Graham Pearson, Owner
Ma3sp, LLC
57405 Horseshoe Court, Goshen IN 46528
574-385-9996 / www.ma3sp.com

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*?"
And <u>Know</u> What To Look For And What To Avoid
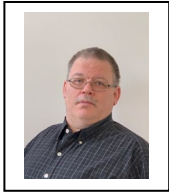
From The Desk Of: Graham Pearson
Owner, Ma3SP

Dear Colleague,

One of the most common 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 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 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 IT services companies, <u>even though most of the services appear to be the same</u>. That's why it's impossible to compare IT providers on their fees alone. In this report I'll explain the most common ways IT 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 IT service contracts and SLAs (service level agreements) that "cheaper" IT 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, cyber protections 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*** IT 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 <u>most informed decision possible</u> 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,
Graham Pearson, Owner
Ma3SP, LLC

About The Author

My early exposure to technology came in 1982, when our family acquired a Compaq Portable, a revolutionary computer with a groundbreaking 5-inch green screen monitor. In the sixth grade, my father insightfully predicted that technology would shape the future. Being an introverted student, I preferred the solitude of home to explore the digital realm through trial and error which lasted until I graduated from High School.

My learning style for technology centered on a hands-on approach, meticulously experimenting with various tasks until I fully comprehended the underlying principles and methods. I believed that a thorough understanding of these concepts would enable me to effectively impart the knowledge to others, enhancing their overall technological experience.

My professional career in the K-12 technology sector commenced in 1992, operating as a technician contracted by local schools on an ad hoc basis to tackle complex technical issues that exceeded the capabilities of in-house IT personnel. The diverse needs of each school district, each with its unique student population size, presented a compelling challenge. However, this experience has honed our ability to tailor solutions to specific requirements, distinguishing our company from the competition. We have effectively transferred the budgeting practices we developed in the K-12 education sector to the commercial realm, demonstrating a seamless transition between these distinct domains. We excel at identifying cost-saving measures that do not compromise the functionality or features of our clients' IT infrastructure. This allows them to focus on achieving their core objectives and enhancing their bottom line.

Founded on July 1, 2019, in response to the transformative impact of COVID-19 and a departure from the K-12 sector after a distinguished 25-year career, Ma3SP is a managed service provider that empowers small and medium-sized businesses to thrive by alleviating their IT burdens and enabling them to focus on their core business objectives. Leveraging extensive expertise gained in the K-12 education sector, Ma3SP seamlessly integrates cutting-edge technology solutions with a deep understanding of the unique challenges faced by growing businesses. Our comprehensive portfolio of services encompasses everything from proactive network maintenance to cybersecurity fortification, ensuring that your business operations remain uninterrupted and secure. In today's hyperconnected world, cybersecurity is no longer a question of "if," but rather "when." The pervasiveness of digital technologies leaves no business immune to the risk of cyber threats.

Guided by an educator's ethos, we strive to impart technological knowledge to our clients in a clear and concise manner, eschewing the jargon-laden terminology often employed by technology companies. We firmly believe that plain English facilitates comprehension and retention, empowering your employees to optimize their productivity.

We would love to discuss how we can be your preferred technology solutions provider.

Graham Pearson, Owner
Ma3SP, LLC

Comparing Apples To Apples:
The Predominant IT Service Pricing 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 $75.00 to $200.00 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 IT projects for organizations that have internal IT 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 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 outsourced IT department. In this model, they handle everything related to your IT "infrastructure." That includes things such as:
    - Troubleshooting IT 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 IT problems.
    - Setting up and supporting your phone system.

- Monitor and maintain the overall health, speed, performance and security of your computer network on a daily basis.
- Vendor Management to resolve issues which frees your staff up from waiting on hold or not asking the right questions to get issues resolved in a timely manner.
- Training staff on technology procedures to improve daily productivity.
- Provides Cybersecurity Training to staff to improve security posture within business.

In addition to managing your IT, a good MSP will provide you with an IT Road map 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, cyber security, backup and employee (end-user) support most businesses need.

As a small or midsize business looking to outsource your IT 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 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 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:

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.

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 is, by far, the most cost-effective, smartest option for most businesses with 5 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 $50 and $150 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 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 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.

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 cyber security 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 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 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" IT Firms Hide The TRUE Cost Of Their Services In Their Contracts

As we said previously, no 2 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 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" 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 Cyber Security 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 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 IT 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 IT 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. **Non-existent 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). As a client of ours, you get all of that INCLUDED, without extra charges.

5. **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, cyber security, the more expensive they are. Make sure the company you are outsourcing to has technicians who are experienced.

   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.

The following are 20 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 cyber security 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.

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

Customer Service:

Q1: How do you request support?
Our Answer: 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? Make sure they explain exactly how they handle IT support requests. *Ma3SP offers multiple convenient channels for submitting support requests. Clients may choose to email their inquiries to our dedicated helpdesk address or contact our support team directly via our helpdesk phone number.*

Q2: Do they offer a written, guaranteed response time to your requests for support?
Our Answer: 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. *This is why we are committed to providing timely and effective support to our clients. We offer a tiered support system with varying response times based on the severity of the issue. For critical emergencies, we guarantee a response time of 15 minutes or less. For high-priority requests, we guarantee a response time of four hours or less. For moderate-priority requests, we guarantee a response time of 24 hours or less. And for low-priority requests,*

we guarantee a response time of two business days or less. These are listed within our Statement of Work

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 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 cyber security, 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?
Our Answer: 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. We provide detailed invoices that show the level of service you are paying for plus and Third-Party Services that are tied to your business organization. We also double-check our invoices for accuracy before they are sent to our clients.

Q6: Do they have adequate insurance to protect YOU?
Our Answer: 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.

Cyber Security And Compliance:

Q7: Do they insist on providing security that meets FTC Safeguards rules?
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 IT 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. That's why we have our security stack of software with tools tailored to help protect our clients from a cyber attack.

Q8: 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.

Q9: 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 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 person to have that much control over your company. If you get the sneaking suspicion that your current IT 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!

Q10: Do they, and their leadership team, understand regulatory compliance such as the HIPAA, PCI compliance, FTC Safeguards Rule?
Our Answer: We include resources that provides comprehensive compliance support to guide our clients through the complexities of regulatory requirements.

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?
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 cyber security protections be implemented BEFORE they will cover you. 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 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 cyber security requirements that are in most insurance policies.

Backups And Disaster Recovery:

Q12: 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 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?
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.

Q14: Do they insist on backing up your network BEFORE performing any type of project or upgrade?
Our Answer: We do, and that'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, 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: All our clients receive a simple disaster recovery plan for their data and network. We encourage them to do a full disaster recovery plan for their office, but at a minimum, their network will be covered should something happen.

Technical Expertise And Service:

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

Our Answer: We provide our own in-house help desk and make sure the folks helping you are friendly and helpful. We consider this 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?
Our Answer: Our technicians are required to keep the most up-to-date vendor certifications in all the software we support. Plus, our hiring process is so stringent, 99% of the technicians who apply don't make it through. (Guess who's hiring them?)

Q18: 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.

Q19: 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.

Q20: 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"?
Our Answer: We feel WE should own the problem for our clients, so they don't have to try to resolve any of these issues on their own – that's just plain old good service and something many computer guys won't do.

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 <u>trust</u> to do the right thing, the next step is simple: call my office at **574-385-9996** and reference this report to schedule a brief 10- to 15-minute initial phone consultation.

You can also go online and schedule the call here: **www.ma3sp.com/discoverycall.**

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 Network Assessment

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:**

- Whether or not your IT systems and data are *truly* secured from hackers and ransomware, and where you are partially or totally exposed.

- If your data is *actually* being backed up in a manner that would allow you to recover it quickly in the event of a data-erasing emergency or ransomware attack.

- How you can get more for your IT investments, improving communication, security and performance, as well as the productivity of your employees.

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 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.

Dedicated to serving you,

Graham Pearson, Owner
Ma3SP, LLC
Phone: 574-385-9996
E-mail: info@ma3sp.com