MSP Hiring Guide: 30+ Questions You Must Ask Before Hiring a Managed Service Provider

Hiring has always been challenging for businesses large and small. Yet small business owners, especially, have a knack for hiring within their niche. Their experience and passion for their industry make it easier for them to spot similar-minded talents. Hiring an IT managed services vendor for the first time on the other hand, can be an intimidating and colossal challenge. How do you hire an IT services firm when the reason you need them is you are not an expert in information technology? After you hire them, how do you really know they are doing a good job for you?

An IT crisis can cripple a small business so you need to get it right. Making the wrong choice can lead to costly disasters and even more time spent hiring another vendor. It is imperative that you pick the correct firm that will enhance your productivity, support your vision, be easy to work with and steer you away from disasters like ransomware.

This guide helps you confirm which MSPs are high quality and a good fit for your company, versus others that are just trying look good, hide their faults, and close the sale. These 30 questions enable you to have an open and transparent conversation to confirm whether each MSP is a good fit for your company.

We're Brian and David. Both of us have been in the IT industry for decades. We are NOT an MSP. However, we each have worked with hundreds of U.S. and international MSPs. Founded in 2004, Brian's company (Gillware) is one of the top-rated data recovery and data forensics experts worldwide. David's company (Manage 2 Win) started in 2006. It has helped thousands of MSP's hire, manage, develop, and retain top employees.

We believe every small-midsize business should outsource some or all of their IT to an MSP. Why? Because a good MSP has a broad bench of capable, certified technical people. More than any one business can typically afford on their own. Your MSP does what they do best (IT), so your organization can focus on what it does best. Read on to learn the best way to successfully hire the best MSP for your organization.

Pre-Meeting

1. Do your homework: Before we meet with an MSP, we study their company website and the LinkedIn profiles for their company, key officers, and the person with whom we're about to meet. We take notes to confirm their answers in our interview match their online data. Here are some questions to consider:

a. Do they have a professional website?

b. Are team members' photos featured on the website?

c. Do they have a secure domain (https:// instead of http://)?

d. Do they seem to have any certifications and IT security experience?

e. Are client testimonials featured on their website?

f. Do they have good online reviews?

g. Does anything negative come up when you Google them?

h. When you call, do they pick up the phone, and provide friendly, professional informa tion, or does your call just go to voicemail or an unhelpful employee?

i. Take a peek at some of the employee's profiles on LinkedIn. Can you find multiple technical assets that have been with the firm for more than 5 years?

Does their website look stale and dated? It is common for an MSP to choose to be busy in their business and not maintain current company information online. However, it's a yellow flag of caution when this happens. If they do not make it a priority to maintain the most public information about themselves, then how well will they maintain your company's technology?

David teaches his clients the #1 objective when you're hiring is to save time. It's the same when choosing a MSP. This means if your preliminary research indicates an MSP is not a good fit with your firm, then stop considering them.

2. If your company uses specific vertical market software or an application that's critical to your success, then consider asking that company for a referral to one of their top partners.

If you company uses a specific software suite, like a CRM or POS system built for your industry, you could ask if they have a referral to a local MSP. You may even strongly consider an MSP remote to your location if they have strong experience with your industry and product stack, especially if most of your critical systems will be managed by them in the cloud. We don't recommend you limit yourself to their recommendations, but this may help you identify other MSPs to consider.

Basics

3. Go to the MSP's office to meet with them.

You need to observe their offices. Is the office messy? How is it decorated – personally, inspiring, or cold and lackluster? How many people are working in the office versus onsite at clients?

It's also better to read their body language and non-verbal cues as you interview them. Even if you're a small company and may only spend $1,000 a month for their services, that's $36,000 over three years. It's a significant investment of money, plus the time you'll spend involved in the relationship.Complete a thorough hiring process because you're relying on the MSP to protect your business from cybercriminals and create opportunities for growth.

Don't take shortcuts.

4. How long has your company been in business?

Ideally, they've been in business for at least 3-5 years.The less time their business has been established, the higher the value they need to deliver and the risk they may not fully deliver on their promises.However, please remember there's a lot of dysfunctional businesses that survive. Longevity is one piece of the puzzle, not absolute confirmation the MSP is a good match for your organization.

5. How much did your company grow each of the last two years?

We prefer the company is growing consistently, at least 10% annually.

6. How many full-time IT staff do you have that have passed at least one certification in the past year?

There needs to be a minimum of 3-5, however if your organization is more than 20 employees then you may require more.This shows the organization is committed to continuous education, which is critical in the fast paced world of IT. With many dozens of popular product stacks typically supplying free training and certifications for their platforms, this is not a very high bar to have a technical asset achieve one certification annually.

7. How many employees do you have, and in general, what are their responsibilities?

We want to know how many people they have to support our IT needs, but also the rest of the business. For instance, IT help desk, IT projects, sales, marketing, admin…

Tech Support

8. How do my people contact you when they're having a tech issue?

The MSP should have a ticketing system, and the option for your people to call if there's an emergency. It's common, and in our best interest, if the MSP requires a ticket be submitted except in the case of an extreme emergency.

In general, people in their 50's like to call, 40's like to email, 30's like portals, 20's like to text or chat.

9. What's the typical response time to our requests for assistance?

There should be an autoresponder confirming the submission of each ticket. In addition, we prefer a human response from the MSP within 30 minutes, even if it's only to confirm a time when they will work on an issue.

Option: Ask the MSP to show you this real-time data in a report on the software that runs their business, which is often ConnectWise or Autotask.

10. Do you offer 24x7 support and if so how?

The MSP should explain if the services are being provided in our country, or overseas. Also, how many people provide support during business hours, and separately during evenings and weekends. What are the skill levels of those people?

NOTE: Most MSPs provide after hour support through a messaging service, which has guidelines to follow. They may say the issue has to wait until normal business hours. However, if a system is down, they will track down an on-call engineer to resolve the issue. That engineer has an escalation process to more senior engineers if she/he cannot solve an urgent issue.

24x7 Support is becoming more of a requirement for companies. This is because more employees are working flexible schedules that include evening and weekend work time.

Infrastructure

11. What RMM (remote monitoring and management) do you use?

Make sure the RMM tool the MSP is using is listed as a top 5 or top 10 list you find on an internet search. This is a foundational tool that all reputable MSP's have. They utilize it to protect and maximize the efficiencies of the technology supporting your organization.

12. How do you do patch management of our laptops/desktops/servers?

Patch management is an automated process that acquires, tests, and installs multiple code changes ("patches") on a computer's software applications and tools. This enables systems to stay updated on the latest security and functionality releases, and also determine which patches are appropriate. What process does the MSP follow to test critical software applications are up to date?

NOTE:Some MSPs only patch Microsoft Windows and Office.How will they help you monitor your other business applications?

NOTE:Beware of "Patch and Pray." This is a haphazard approach to cybersecurity where there's a data breach or other type of malicious attack. he MSP resolves it, does damage control, and implements a solution to avoid a recurrence.

There are three problems with this approach: (1) It's often a partial solution rather than fully integrated into a complete cybersecurity strategy; (2) It doesn't evolve as the hackers adjust their technology; and (3) It's impossible to maintain as the number of individual patches grows.

Automated patch management with manual oversight and intervention is a requirement for any reputable MSP.

13. What suite of security tools do you implement your clients?

The brands are not as important as the functionality and the expertise of the MSP to implement and manage their security tools. Here are a few of the key areas to consider:

For each area, ask what vendor they use, and how many people are certified in the technology?

a. Access control. This controls which users have access to your network, especially sensitive sections of your network.

b. Antivirus / malware software. This software monitors network traffic in real time for malware, scans activity log files for suspicious behavior or patterns, and offers ways to stop the threats.

c. Application security. This is a combination of hardware, software, and best practices to confirm software is up to date, monitor issues, and close gaps in security coverage.

d. Behavioral analytics.This software enables you to establish a baseline of typical software use, identify indications of abnormal behavior, more quickly spot problems, and isolate threats.

e. Data loss prevention. DLP tech helps prevent your people from mistakenly exposing data to cybercriminals outside your network who are posing as trusted individuals.

f. Distributed denial of service prevention. This is often a hardware appliance that scrubs incoming traffic before it reaches your firewalls to remove illegitimate activity that could threaten your network.

g. Email security. This software filters out incoming threats and can be configured to prevent outgoing messages from sharing dangerous data and links.

h. Firewalls.This is a combination of hardware and software that acts as a gatekeeper between a network and the internet, based on predefined rules and policies.

i. Mobile device security. All security technology must extend through every device that can access your network, including your mobile phones, tablets, etc.

j. Network segmentation.These networks make it easier to assign or deny authorization credentials for employees, limit access to sensitive information, and block potentially compromised devices or intrusions.

k. Web security. This stops employees from visiting sites that could contain malware, blocks other web-based threats, and protects your web gateway.

14. What active certifications do your full-time employees have, by vendor and technology? We're particularly interested in your certifications with security solutions.

If none, then why? It makes no sense.

Furthermore, they may have network, system, and software certifications, but none specifically in security. If that's the case, then do they have a strong partner they work with that provides high level to perform security assessments, and help them provide your organization with a thoroughly secure IT environment?

Be aware that a CISSP (Certified Information Systems Security Professional) certification is good and sounds impressive, however it focuses more on security governance than actual tangible current knowledge.

15. How do you assist with asset management and my software licensing? Can you show me some example reports?

This is important. Often organizations are paying for software they're not using. Your MSP should help you find ways to save money and only pay for technology you're using. They should be able to quickly provide a sample report.

16. Show me a disaster recovery procedure for one of your client's critical business systems. Show me the paperwork of a documented audit.

They should be able to provide a sample documented audit within 1-2 business days, if not the same day. Many MSPs only do this for larger clients. They should have a process in place, including an audit report.

DEFINITIONS:
Data Protection = Backups
Business Continuity = IT environment keeps running while primary systems have failed
Disaster Recovery = Getting back to Pre-Disaster State.

17. How do you back up my critical systems?

The automatic backup process should occur daily, if not several times a day.The data must be encrypted on a different computer network and different physical location.The MSP should require clients to use two-factor authentication for anyone to access those backups.

Game Changers

18. How often do you meet with your clients to discuss high level issues/strategies?

We prefer a minimum of quarterly meetings. However, it depends on the size of your organization. Some MSP's have strategy meetings with smaller clients once or twice a year. Other MSPs who are actively involved in higher strategic projects and ongoing work may meet monthly, or even weekly at times.

One way to consider the best schedule for your organization is based on your monthly billing from the MSP. Meet once annually for every $1,000 they charge you for monthly services. For instance, if you're paying $1,000 a month, then meet once a year. If you're paying $4,000 a month, then meet quarterly. Increase their involvement in strategic business decisions, your communication with them, and mutual accountability the higher your investment in the MSP's services.

19. Send me a sample monthly or quarterly report from a recent meeting with one of your clients.

They should send this to you immediately because it exists. How comprehensive is the report? Does it match the sample report one or more of the references showed you?

NOTE:Typically, monthly reports are only valuable when the MSP is truly engaged as a strategic partner in your business. If they're doing projects, those have their own meetings and reports. Don't waste time by requiring redundant meetings and reports.

20. I heard of someone whose entire company is running on a Windows Server 2003 and they don't want to upgrade. Will you support that?

We want them to say "no." MSP's that try to support any type of technology are forced to provide lower quality service. It's positive when they refuse to support outdated hardware or software.

21. How often do you audit each client's backups, and what's the process?

The MSP must be confirming the backups they're maintaining for your organization can be used to fully restore data that's lost. It also confirms how quickly data can be restored. A quarterly audit is our preference. Be prepared to pay for this service, which is typically 4-8 hours of billable time. It's a mandatory "fire drill" to confirm a hacker or ransomware demand cannot shutdown your organization for more than a few hours.

22. Pricing

You get what you pay for in IT services when you choose a reputable MSP. If you want the cheapest provider, then plan for poor service. Confirm the MSP can deliver the value and be willing to consider an MSP that charges above the average rate. The additional services may eliminate bottlenecks and computer downtime so your organization has a competitive edge to crush your competition.

23. Please supply 2-3 client references. We prefer companies of similar size to ours, and in our industry.

Don't skip this step. It's foolish to not confirm how well they're currently serving their customers. Why gamble? Do not waste your hard-earned money on a unqualified MSP, or simply one that's not a good match for your company, because you were too lazy or claimed to be too busy to check references.

Your choice of an MSP is a long-term, strategic decision. Invest the time to make it a wise one. Our suggested questions for references are below.

Reference Questions

Here are some key questions to ask the MSP's references:

24. How long has (MSP company name) been serving your organization?

The reference should have worked with the MSP for at least one year.

25. How has your organization grown, and how has (MSP company name)'s services expanded to meet your needs over the past three years?

Ideally, the reference company has grown during the past three years. It's even better if they expanded their work with the MSP to help them grow.

The key here is to discern how much of any additional MSP services are tactical, such as simply expanding the number of seats being supported, versus strategic.A strategic investment might be to implement significantly more complex security technology, move data and applications to the cloud, or better connect people across multiple geographies.

26. How do you login to your network when you are at home? How do you authenticate when you log into any cloud services?

This is a problem if it's only by entering their username and password. It must be multi-factor authentication, such as username, password, and Microsoft / Google Authenticator or text code to their mobile phone or email. Less common are virtual private networks ("VPN") and encryption.

27. I'm curious about your last quarterly or annual meeting with the MSP? What was the agenda? What are the content areas of the report they provided you?

Confirm the meetings are happening, involve strategy as well as tactical work, and how the meetings/reports are providing value to the reference company. They may be willing to share parts of a report in a screenshare during your meeting. Don't push for this because it may violate confidentiality.

Yes, we asked for a similar report from the MSP. In general, our objective here is to confirm the sample report from the MSP matches the content discussed and reported to the reference company. If the meeting agenda and/or reports don't sound like they match, then ask the MSP why.

28. How often are they performing a full security assessment for your organization? May I please briefly see the report?

The report should exist. Hopefully, it's been done within the last year. Some MSP's complete security assessments monthly or quarterly, whereas others do it annually. If they haven't done a security assessment for more than a year, then is that because the client wouldn't pay for it, or a lapse by the MSP?

29. How much spam email or junk email do you get?

They probably get some, but it should be minor. Otherwise, the MSP is not properly monitoring and adjusting the individual's security settings. It may also be an issue with the employees of the company because they haven't been trained properly, or they didn't implement what they were supposed to do after the training.

30. Has your MSP done any social engineering training for your employees? This is training to teach your employees what to click on, and how to not be fooled by a cybercriminal. How is this training done? How often are your people trained, or tested with fake phishing emails?

The MSP should be doing this or have a partner they recommend to their clients for this training and testing.The client should have regular reporting on the training that's occurring, and how well their people are passing any testing.

NOTE:Social engineering training, or security training, is not a one-and-done experience. It should be ongoing with testing monthly and training monthly or quarterly.

31. What are the three biggest issues you've had in your relationship with (MSP company name)?

We don't expect any MSP to be perfect. There are reasons some service challenges can be acceptable. For instance, a problem was due to a software update or glitch, outdated system the client had refused to replace, or the client did not respond promptly to questions a technician needed to resolve an issue more quickly. However, we do need to discern the weaknesses of each MSP and consider whether a mistake was a unique situation, or an ongoing issue. In many cases, we discuss these issues with the MSP to confirm their explanation matches the reference's story.

32. How much coverage would you recommend in a Cyber Insurance policy for my business? Do you have a particular cyber insurance vendor you typically recommend and why?

This shows they have their finger on the pulse of one of the biggest emerging threats in IT, data breach and ransomware. Showing they have spent time thinking about this topic and have an answer, is more important than the coverage amounts or particular vendor

We hope this helps. This is not every question you could ask an MSP, but it is a solid list that most companies fail to consider. We want you to partner with an IT managed services organization that helps your company thrive. It should be a win-win, long term partnership. Following this guide can get you there.

Don't hesitate to reach out if you have any questions.
Sincerely,

David Russell, CEO
www.manage2win.com

Brian Gill, CEO
www.gillware.com