Kraft Kennedy

24 QUESTIONS TO ASK WHEN CHOOSING A MANAGED SERVICE PROVIDER



JUDE TRAVERS-FRAZIER

24 QUESTIONS TO ASK WHEN CHOOSING A MANAGED SERVICE PROVIDER

by **Jude Travers-Frazier**



Jude Travers-Frazier is the Chief Operating Officer and Associate General Counsel at Kraft Kennedy. He develops and implements internal procedures, resources, and training to equip Kraft Kennedy consultants with the necessary tools and processes to complete projects efficiently and successfully.

You've got enough on your plate dealing with current business demands. If you haven't already done so, it's time you considered hiring a managed service provider (MSP) to handle your IT needs and keep your systems secure.

Whether you're engaging an MSP for the first time or considering switching from your current MSP, ask yourself the following questions before you make your choice. The answers will help ensure you're choosing the right partner that will help your business succeed.

CONTRACT BASICS

1. What is the pricing structure?

It's important to have a very clear understanding of what your MSP is offering for the price you're paying. Is there a monthly recurring charge? Are there time and materials charges? Some MSPs sell blocks of hours, others price their services per incident or on the number of open tickets at any given time, and some offer a combination of pricing models. There's no one right approach to pricing, but you should know exactly how the MSP will charge you so you can set appropriate expectations for a successful working relationship.

2. What are your cancellation options?

Cancellation options are a critical aspect of any MSP contract, and not all contracts

have the same terms. Some seek to lock you in for a period of time at a set price, while others are much shorter in duration. Some MSPs believe that locking clients into contracts causes unnecessary friction. Like pricing, there are several options when it comes to contracting for cancellation. You just need to understand what expectations the MSP is setting for how the business relationship will unfold and how you can get out of it if necessary.

3. What does your contract cover?

This may seem like a straightforward question, but again, there are many variations when it comes to what MSP contracts contain. Some offer unlimited support, but there are typically exceptions you'll need to understand – commonly things like not covering hardware or software that's out of warranty or not provided by a reputable third-party vendor. You'll also want to get a handle on what additional charges might be incurred above and beyond the monthly cost of that contract – for example, if a consultant has to go on-site or has to contact a vendor to purchase a part that's no longer under warranty.

4. How and when is support provided?

You need to understand how support requests get made. Does the MSP only respond to email and phone calls or is there a service portal for opening tickets? Do all service requests have to come from a designated person in your organization or can any user request support? You also need to understand how the MSP will address those requests. Is support given via telephone or will consultants come on-site? After-hours support is also a crucial factor. Some vendors only offer support during typical working hours, some offer true 24/7/365 support, and some fall somewhere in between. There are numerous ways MSPs can structure their support function, and it's important that you find a model that works for the unique culture of your firm and users.



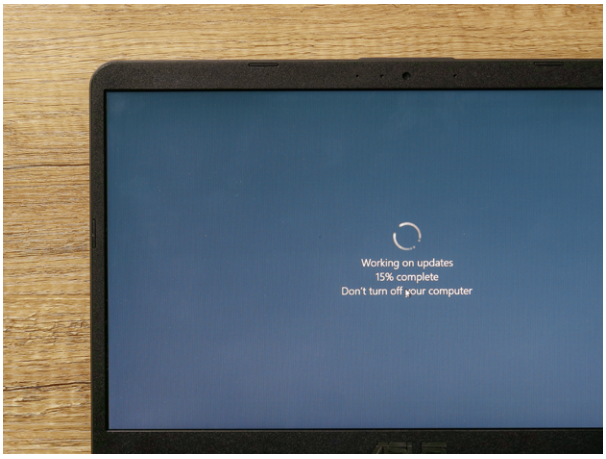
5. What is the response time for support?

Once you pin down exactly how you request and receive support, it's also important to understand how quickly that support will be provided. Look at what the MSP is committing to in terms of response times when you open up a ticket and ask for help. Response times are different than resolution time frames – the latter refers to how long it will take to resolve an issue, and certain IT issues can be complex and unpredictable. Any guaranteed resolution time frame should be viewed with

skepticism, but you do want to understand how quickly the MSP is committed to reacting to your service request and starting to address the problem.

6. How does priority impact response times?

Most MSP contracts will vary response times based on the criticality or priority assigned to the issue (typically high, medium or low). You should understand how response times are based on priority, but also how those priorities are defined and assigned. You'll also want to know what your recourse is if you disagree with the priority the MSP assigns to your issue and how you can communicate urgency if something is critical.



7. How does the MSP handle patching and upgrades?

Patching is something that most MSPs say they do, but contracts have a lot of different definitions and implementation strategies. If your organization is potentially open around the clock with employees handling late filings or working through the night, you'll want to understand exactly how and when the MSP plans to take down your servers to perform patching. Is there flexibility in terms of how it schedules things, are you given advance notice, and can you request a reschedule if absolutely necessary? The MSP should be willing and able to balance your work needs against the security needs of regular patching.



8. What is the team composition at the MSP?

The composition of the team that will be serving you is important, and it's a factor too often overlooked during the initial phases of assessing an MSP relationship. Before you sign on, you should request specifics on the nature of the team that will provide you support – are your requests just referred to a large support pool, meaning you could get any member of its team, or are they divided into smaller teams that are each responsible for a subset of the MSP's clients? Are there nontechnical contacts you can go to for things like

accounting issues? What's the process for escalating an issue? Your understanding of how the MSP operates needs to line up with your culture and your expectations, so there aren't any surprises once you begin working with them.

ONBOARDING

9. What is the plan for initiation and onboarding?

In vetting an MSP, it's of critical importance early on, especially if you're transitioning from an existing MSP and replacing it with a new one, that there be a strategic onboarding plan in place. You want to have a very clear understanding of the onboarding process that your new MSP will undertake before you sign up. If you have questions about the onboarding process, can adjustments be made if the MSP agrees they make sense? If your MSP doesn't have a clearly defined onboarding plan, you'll want to consider looking elsewhere.

10. What is the time frame for onboarding?

While you understandably want to get up and running as soon as possible, onboarding can and should take a little bit of time if it's done right. If an MSP claims it can just gather your information and start providing support, that's a red flag. You want to ask how the onboarding plan factors in time frames for getting up and running – ideally, there will be milestones of where you'll be at 30 or 60 or 90 days, with consistent progress until you're fully onboarded.



11. Will the MSP perform a technical assessment?

You should ask the MSP what factors about your network or your environment are relevant to the plan for onboarding. If the reply is it doesn't matter and the onboarding time frame works no matter what, that's another red flag. Every IT environment is going to have certain elements that could disrupt even the most well-intentioned onboarding plan. An MSP should be asking you questions in order to understand what kinds of surprises might be lurking and impacting their ability to onboard you effectively.

12. How do you transition from one MSP to another?

Switching MSPs has additional implications. You'll want to understand your new MSP's

expectations regarding participation from your current MSP in the onboarding process. You're going to need to decide for yourself whether you're going to inform your current MSP about the transition or not, and what your new MSP requires will be pertinent to that decision. A sudden switch where you lock out your old MSP is going to be a very different onboarding process than one where the two companies are able to work together for you.

13. What are the MSP's expectations for your involvement in onboarding?

You'll want a very clear understanding of what the MSP is expecting from you and other members of your firm in terms of your time and effort during the onboarding process. Are you expected to participate in daily or weekly meetings or does their team expect you to gather documentation about your network and aspects of your practice in order to make onboarding smoother? You need to understand how much of an imposition onboarding is going to be on your regular job responsibilities during the transition period.

SECURITY

14. Are they an MSP or an MSSP?

An MSP is a managed service provider. An MSSP is a managed security service provider. These historically have been two different things. While MSPs have been around for 10 to 15 years, MSSPs are a much newer concept. An MSSP focuses solely on providing security services, which is important for helping firms ensure their environment is as secure as possible. However, most MSPs today are also MSSPs, because it's virtually impossible to be an effective MSP without having a very firm



grasp of the current threat landscape and how to protect technology assets, environments and clients. In this day and age, it should be considered suspect if an MSP doesn't have an advanced understanding of security.

15. What does the MSP's security stack look like?

In addition to basic technology services, you want to ask what the MSP has in their security stack – what tools do they use and what services do they provide in the area of security? Today there are many different approaches to providing differing types of security to protect against the range of threats that exist. Your MSP needs to have thought through those various threats and made decisions about what tools to use to protect against them. It's no longer a matter of just having a firewall. MSPs should have tools for intrusion detection and intrusion prevention, vulnerability scanning, email threat monitoring, phishing protection and more, and they should be continually evaluating and swapping out those tools to ensure the best possible security stack.

16. Which cybersecurity frameworks does the MSP follow in providing service?

Your firm is likely subject to at least some regulatory requirements (HIPAA, GDPR, PCI, etc.). Complying with those regulations requires adherence to the right cybersecurity framework – a system of standards, guidelines and best practices designed to meet specific regulatory requirements. Other CSFs are intended to cover a broader set of controls and risks (NIST CSF, CIS, ISO/IEC 27001, and 27002). You should ask the MSP what CSFs they adhere to. Are they able to provide service in adherence to the CSFs that cover the regulations to which you are subject? If they follow NIST or ISO or SANS, why was one chosen over another? There are many different CSFs and reasons an MSP might pick a particular one, but you want to know that your MSP is following at least some standards. This will tell you that the security they are providing is following a defined and vetted framework that's continually being revised by outside experts.



17. Has the MSP achieved certified compliance with a security and risk framework?

Beyond adhering to a nationally recognized CSF in providing services to your firm, the MSP may also have obtained a security and risk certification, such as SOC 2 or ISO 27001. Completing an external audit and

achieving formal certification according to one of these frameworks may be beyond the capabilities of many MSPs/MSSPs, and that is not necessarily a barrier to working with that company. Achieving and maintain such certification, however, is a positive indication of its operational maturity level and focus on maintaining exemplary internal data protection practices.

18. How does the MSP approach cloud security?

If you use cloud-based tools – which you likely do – you'll want to ask the MSP how those cloud assets are secured. The MSP needs to be able to talk about things like single sign-on, zero trust or other security methodologies and approaches that can be implemented to protect your cloud-based assets. The cloud is not inherently secure on its own, so the decisions that an MSP makes about how to implement security within your environment can impact how safe your cloud-based assets are against an attack.

19. How does the MSP secure backups?

Backups are not as simple as they used to be. Hackers who commit malware attacks will attempt to go after your backups as well as your production network, because they know that if they can encrypt your backups on top of encrypting your production environment, you'll have further incentive to pay whatever ransom they're demanding. Therefore, it's important to understand if the MSP will be responsible for your backups or even recommend backup solutions of their own, as well as how they plan to protect you from attacks.



20. What is the plan for password management?

You should ask the MSP how your passwords will be managed, where they'll be stored, and what system will be used to protect those passwords. Your passwords should be handled and stored separately from the passwords of the MSP's other clients. The unfortunate reality is that MSPs are also now targets for hackers, because they've figured out that MSPs can be an open door to their end clients. You should also know what the protocol is in the event that the MSP is breached.

21. What is the MSP's approach to intrusion detection and incident response?

The MSP should have an intrusion detection and incident response plan as part of their security stack, but their preparations should go even further. Ask what the MSP does to monitor their own environment

and how they would respond if it appears there may have been a breach. Is the incident response plan they have the same incident response plan if you were breached? The MSP should be willing to share their plan with you so you have a very clear understanding of what will unfold if a situation develops, and regular tabletop exercises should be conducted to walk through an incident response situation and identify any gaps.

OTHER CONSIDERATIONS

22. What is the MSP's subject matter expertise?

Most MSPs have a bench of L1s, L2s and L3s – generalists and specialists with varying skill levels covering a wide range of most standard technologies. You may, however, want to ask about the depth of expertise in your business-critical systems. Does your firm use a particular accounting package or document management system? If so, does the MSP have subject matter experts in those specific areas and/or with those specific applications? If email is essential to your business, does the MSP have SMEs with certifications from your email vendor and/or access to the vendor's premier support teams? You should also ask if any of those experts will be on your assigned team and what the escalation procedure is if you need to tap into that expertise. How this is handled can impact how long it takes for a resolution and how frustrated your employees might be with service requests. Some MSPs are only MSPs, while others might be part of a larger organization that does more than just provide day-to-day end



user support and offers a greater scope of services with deeper benches of SMEs available to cover all of your mission-critical systems.

23. Does the MSP know your business?

Some MSPs work with a broad range of clients across many different verticals, trusting that their general expertise enables the ability to provide adequate support to any given client. Other MSPs have chosen to focus on a particular vertical or perhaps multiple related verticals. You should decide whether it's important to you for your MSP to be familiar with *your* business. Will knowledge of how your company operates, what stresses and challenges *you* face day after day, have an impact on how they interact with your users and the level of service they provide? If so, you'll want to look for an MSP with an established client base serving companies in your same industry.

24. Does the MSP have good referrals?

One of the things that ends up mattering most for people in choosing an MSP is whether they can get a good referral for that MSP from someone they trust. Don't be afraid to ask around to friends and professional peer groups for recommendations or opinions if there's an MSP you're already considering working with. Ideally, you want to seek out a referral from a firm that's similar to your own and has similar needs – try to get a feel for the relationship, the pros and cons and the



service level experienced with the MSP. Insight into how well regarded the MSP is by similar firms is a big indicator of how likely they will be to serve you well over time. In addition to speaking with a client of the MSP, review success stories and testimonials on the company's website.

Engaging an MSP is a great way to be sure that someone is diligently attending to your IT and security needs, while you focus on running and growing your business. There are many MSPs out there today, but if you take the time to ask the questions outlined above, you'll find the right one that aligns with your needs and goals and will help you succeed.

Contact Us

kraftkennedy.com
hello@kraftkennedy.com
(800) 523-3081