


5 Compelling Reasons to Switch IT Providers



How to Tell if Your
Current MSP Is Letting
You Down

HOW TO TELL IF YOUR CURRENT MSP IS LETTING YOU DOWN

Many companies are frustrated by their IT managed services providers (MSPs) for four main reasons:

- 1. Rework** – Problems continue to occur after repeated repairs and maintenance
- 2. Billing** – You have to pay your IT provider every time they come to your site to fix a problem
- 3. Response time** – Service requests take days or weeks to resolve
- 4. Communication** – Questions go unanswered or services are not clearly explained

However, many companies don't know where to start looking to switch IT providers. They're afraid of making the change due to fear of the unknown and the fear of something going wrong if they decide to change MSPs. They also might feel like they're being held hostage by their MSP, who controls their sensitive data.

WHY WE WROTE THIS GUIDE

We wrote this guide to help you determine whether your current MSP is letting you down with their service offerings, and to help you find the right IT provider for your business.

- 1 Response times and knowing your business**, which explains how an MSP should respond to issues and work to support you
- 2 Fixing it right the first time**, which outlines what is likely happening today and your MSP can't seem to get it right the first time
- 3 Billing**, which states why you should seek out an MSP that offers a fixed monthly cost per user
- 4 Backup management and security**, which describes what an ideal backup solution looks like
- 5 Technology – cloud / speed / quality / maintenance and support**, which discusses how to have a conversation about your technology needs and when to migrate your services to the cloud



RESPONSE TIMES AND KNOWING MY BUSINESS

Responsiveness is an essential quality for IT providers. When technology goes down, it can greatly affect a company's ability to function. You need to be able to reach out to your IT provider to get the problems resolved as soon as possible. Response times for different MSPs can be incredibly inconsistent from call to call, and can extend over days (or weeks).

Response times often depend on the size of the IT service team. While a small IT provider can work if you're a small company, once you reach a certain size (say, 20-30 employees), you cannot rely on a one or two-person IT team to be sufficiently responsive to your needs. What happens if one of them goes on vacation, becomes ill or leaves the company? You will likely have to wait a long time for a response.

Conversely, you don't want to partner with a large IT provider, where they have 15 or more IT professionals on their support desk. Every time you call in with

an issue, you'll have to educate a new person about your company, applications, and specific problems. It's not likely that every IT professional will know your business needs. This will slow down the process, and can extend the time to get a proper response to your issues.

The ideal scenario is to partner with a small team within a larger IT provider. The individuals on the team will get to know the nuances of your business, employees, applications, and needs. They'll learn what's important and not important, what's critical and what's not, and what's happening on a day-to-day basis.

This small team within the larger IT provider will get to know the differences between what's important and what's urgent for your brand. By being familiar with your business, they'll also know when an issue is urgent, and will be able to put the necessary resources in place to address emergencies or urgent matters as quickly as possible.

CALLOUT

Ask your MSP how they respond to issues, and how well they know your business.

- Do they have a dedicated support team for you? Will you be dealing with the same IT professionals each time you reach out for help?
- Do they document exchanges to help them deal with recurring concerns more quickly?
- Do they have an urgency assessment process to determine what issues to expedite and which resources are needed to solve the problem?
- Do they offer a 60-minute response time for emergencies, 24 hours a day, 7 days per week? Simple requests can go through email or voicemail, but is someone available by phone to deal with urgent issues at any time?
- Do they have a ticketing or tracking system to stay on top of service requests?



FIXING IT RIGHT THE FIRST TIME

A common source of frustration is an IT provider's failure to fix a problem the first time around. Many companies have to deal with repeatedly contacting their MSP to rework a problem. They call their IT provider to get something fixed, and not long after, something else breaks or the problem recurs and they have to call back several days later.

Many MSPs do not address the root cause of a problem. They address a symptom or apply a temporary fix rather than identifying and solving the core issue. They do not have sufficient understanding of the client's needs.

This is common when partnering with a large MSP, which might have 15 or 20 IT professionals dealing with different clients. With this type of provider, no one person is responsible for your company's IT needs, so no one takes ownership of your issues. There's no incentive for an

individual IT professional to identify the root cause of your problem, as they probably won't be handling your issue the next time you call.

One way to ensure problems are fixed right the first time is to establish processes tied to major changes that happen within your business. For example, many common problems can occur when an employee either leaves or joins the organization. Simple issues, such as a printer going down, can recur and become more serious following these changes. Establishing a company-specific recipe to address common problems can reduce rework in the future.

Partnering with an IT provider that assigns a dedicated team to your company ensures that each person understands your company's nuanced needs, equipment, employees, and situations.

CALLOUT

Ask your MSP how they ensure issues are fixed correctly the first time.

- Do they document issues and set up processes to address the root cause of problems?
- Will they assign dedicated personnel to servicing your company's technology and systems?
- How will they take ownership of the problems and offer long-term solutions?



BILLING

Many MSPs follow a "break/fix" billing model, charging clients each time they are called to repair technical issues. The problem with this format is that IT providers are not incentivized to prevent problems. In fact, they are financially rewarded every time you have a problem that requires their attention. With this service model there is no incentive to reduce the number of technical problems that you will face over the life of the contract. You could end up being billed two or three times to repair a single problem.

Another issue with the "break/fix" model is that you end up paying the IT provider to learn your business while they're repairing and maintaining your systems and technology. There's a learning curve when working with a

new MSP, and to charge hourly rates for time spent learning your systems just doesn't make sense.

MSPs should be reducing the number of your technical issues, and keeping your systems running. Reducing or eliminating technical issues will help to keep your employees and company running at peak efficiency.

A fixed monthly cost model ensures that MSPs focus on reducing the number of technical issues and breakdowns that occur. Fewer site visits means less travel time, lower HR costs, and fewer operational expenses for the IT provider. The fixed monthly cost model provides greater transparency as you will know exactly how much you're spending for IT services every month.

CALLOUT

Have a conversation with your MSP about their billing structure.

- How do they bill for their services?
- Do they charge every time they visit your site or handle an issue?
- What's included and what's extra in the contract?



BACKUP MANAGEMENT AND SECURITY

Every company should have backup systems and plans in place. Any competent MSP will help you to set this up and maintain it. However, there is often a disconnect between what the business expects to happen when a disaster occurs and how the backup has been designed to manage a disaster.

Two key objectives for a backup system are recovery points and recovery time.

- Recovery point refers to how many points in time the backup system is expected to have copies. Do you need the backup to go back 90 days to retrieve some files because you accidentally deleted them 63 days ago?
- Recovery time refers to how long it takes to get back up and running when a disaster happens. How long do you expect to be out of operation if there is a fire that destroys your computers? What happens if an employee accidentally deletes all your files?

The MSP should have a plan – or help you to create a plan – to deal with different types of disasters and ensure they understand your recovery time objectives. There should be no disconnect between your current backup system and your expectations of how long it will take to get up and running again. And if there is a disconnect, the IT provider should help to create a financially feasible solution that meets your business requirements.

The MSP should also have a restore period attached to different types of disasters. For example, if a ransomware attack occurs, once you contact the IT provider to inform them of what is happening, they should follow set processes and restore operations within the established time. They should also be able to explain what will happen following different emergency situations.

CALLOUT

Have a conversation with your MSP about your backup and security plans.

- Do they know how long it will take for you to be back up and running after a fire, ransomware attack, or a hardware failure?
- What is the recovery time with the backup system? Have they discussed and met your recovery point objectives?
- What is the restore period for different emergency situations?



TECHNOLOGY – CLOUD / SPEED / QUALITY / MAINTENANCE AND SUPPORT

Most people don't understand the technology that backs up and secures their data. They don't know how the cloud works or what's involved in cybersecurity. These are highly specialized fields, which is why companies hire an IT provider in the first place. However, when something goes wrong with the technology, companies often blame the MSP, as they equate the problem with the service rather than the systems or equipment.

It is the MSP's responsibility to educate clients on the technology they need to back up their systems, maintain their cybersecurity, and support their business needs. Too many IT providers do nothing more than maintain the existing equipment and provide support. They don't lead conversations on equipment and technology upgrades. They don't discuss how clients can improve the speed and quality of their systems. They don't talk to their clients about cloud-based and cybersecurity options. All they do is maintain the status quo.

Cloud-based services have advanced their capabilities in recent years, and the costs have dropped significantly as well. However, many MSPs are not keeping up with innovations and are satisfied to maintain on-premises servers and equipment as long as they last. They're not helping clients to leverage cloud-based services, solutions, and applications, which can reduce their cybersecurity risk and increase productivity. They're stuck in the past, forcing offsite employees to use a VPN to gain access to the office's systems while working from home.

Some IT providers don't stay current with what's happening in cybersecurity. It requires a combination of offense and defense to protect clients from imminent threats. Too many MSPs take a passive approach, installing basic protections and reacting only when systems have been compromised. This lack of motivation and innovation leaves clients vulnerable to cybersecurity attacks.

CALLOUT

Ask your MSP about how they will manage your technology requirements.

- Are they on top of technological trends, particularly cloud-based systems and cybersecurity?
- Do they have a plan to update and migrate your systems and services to the cloud?
- Are they simply maintaining your equipment or looking for ways to improve your current technology?
- Are they initiating discussions on how to make you more productive and the cost/benefit analysis of making the switch?
- Are they taking a proactive approach to managing your cybersecurity needs?



CHEAT SHEET TO SCORE CURRENT MSP

Issue	How to have the conversation	How your current provider should respond	What to do if they don't
Response times and knowing the business	<ul style="list-style-type: none"> • Do you have a dedicated support team for us? • Do you have an assessment process to determine what issues to expedite and which resources are needed to solve the problem? • Do you have a tracking system to stay on top of our service requests? 	<ul style="list-style-type: none"> • They should assign a specific team of IT professionals to handle your needs and systems • They should have a handle on your recurring issues • They should have a system in place to track and respond to service requests 	Partner with an MSP that will assign a dedicated team of IT services professionals to your company, who will get to know your company, employees, technology, and needs.
Fixing it right the first time	<ul style="list-style-type: none"> • Do you document issues and set up processes to address the root cause of problems? • Will you assign dedicated personnel to servicing my company's technology and systems? • Will you take ownership of the problems and offer long-term solutions? 	<ul style="list-style-type: none"> • They should keep track of all issues to maintain a history of service requests and identify root problems • They should assign a dedicated team of IT professionals to manage your account • They should take ownership of your situation and needs 	Partner with an MSP that will take ownership of your IT service needs and ensure that problems are addressed correctly the first time.



Billing	<ul style="list-style-type: none"> • How do you bill for your services? • Do you charge every time you visit our site or handle an issue? • What's included and what's extra in the contract? 	<ul style="list-style-type: none"> • They should charge a set monthly rate for IT services • They should not charge anything extra for emergency service or repair • They should be transparent in explaining all the costs involved in providing IT services 	Partner with an MSP that employs a fixed monthly cost model, so you will pay the same amount for IT services every month.
Backup management and security	<ul style="list-style-type: none"> • Do you know how long it will take for us to be back up and running after a fire, ransomware attack, or a hardware failure? • What is the recovery time with the backup system? What are the recovery point objectives? • What is the restore period for different emergency situations? 	<ul style="list-style-type: none"> • They should work with you to develop a comprehensive backup plan • They should discuss your recovery time and recovery point objectives • They should set up restore periods for different emergency situations 	Partner with an MSP that will develop a backup plan that covers all possible emergency scenarios to return you to full operational status as quickly as possible.
Technology – cloud / speed / quality / maintenance and support	<ul style="list-style-type: none"> • Are you on top of technological trends, including cloud-based systems? • Do you have a plan to update and migrate our systems and services to the cloud? • What is your approach to managing our cybersecurity needs? 	<ul style="list-style-type: none"> • They should consistently review your existing systems • They should discuss plans to migrate your systems and services to the cloud when it makes sense • They should be proactive in protecting your system's cybersecurity 	Partner with an MSP that will regularly evaluate your current technology situation and needs to make sure that you are operating at peak efficiency and staying current.



NAVIGATING "NO MAN'S LAND"

Some companies get nervous about making the switch to a new MSP because they don't know what to do first. Who's responsible for supporting the transition? What will they do if things go wrong?

When switching to a new MSP, it's the new MSP's responsibility to reach out to your current IT provider to help support the transition. They should provide a sufficient notice period (such as 30 days), during which time you will be paying both companies to ensure a smooth transition. Your new MSP should set up a meeting, either online or in person, to introduce themselves, explain the situation, and formalize a transition plan. The new IT provider should be prepared to provide full support during this 30-day period, should your outgoing IT services provider drop the ball or decide to vacate the agreement early.

The new MSP should make the transition proceed as smoothly and quickly as possible. There should be a transfer of technical documentation, passwords, and other content from the original IT provider's control. The new IT provider should also remove the outgoing IT provider's tools and permissions from the environment to effectively take control of the network.

While most transitions go smoothly, issues can arise. The outgoing IT provider could become unresponsive, or be incapable of making a proper transition go smoothly. Whatever the case, the new IT provider should be able to take control from the moment they begin the contract, figure out how to make the transition work well, and ensure your company is running smoothly within a reasonable amount of time.

HOW BRITECITY CAN HELP YOU TRANSITION

BRITECITY can help you to make the transition from your current IT provider. We know it can be stressful for clients to make the switch, so our streamlined process will make sure it goes as smoothly as possible.

We are experts in the transition process. BRITECITY has been involved in more than 200 transitions from existing MSPs. We handle every step of the transfer from your outgoing IT provider to BRITECITY. We take responsibility for your IT services and security from Day 1!

In our experience, most transitions are relatively seamless. We ensure that everything works out in our clients' favor.



WHY SHOULD YOU SWITCH TO BRITECITY?

There are five compelling reasons to switch to BRITECITY as your MSP.

1 RESPONSE TIMES AND KNOWING YOUR BUSINESS.

BRITECITY will assign a dedicated team of IT professionals to your company who will get to know your systems, employees, technology, and unique needs. We're a phone call away 24 hours per day, 7 days per week when you have an emergency situation. We guarantee a response within 60 minutes for any urgent request.

2 FIXING IT RIGHT THE FIRST TIME.

BRITECITY will take ownership of your IT service needs and ensure that problems are addressed correctly the first time they arise. We will set up processes to understand the core causes of your tech issues, so we won't have to keep making the same repairs over and over.

3 BILLING.

BRITECITY employs a fixed monthly cost model, so you will pay the same amount for IT services on a month-to-month basis. You'll never have to pay for emergency site visits and unexpected repairs. This ensures total transparency in your IT service costs, consistent uptime, and fewer site visits.

4 BACKUP MANAGEMENT AND SECURITY.

BRITECITY will develop a backup plan that covers all possible emergency scenarios to return you to full operational status as quickly as possible. We'll discuss your recovery point and recovery time objectives to ensure the backup plan matches your business needs. We'll also detail what's involved in the restore period following disaster situations.

5 TECHNOLOGY – CLOUD/SPEED/QUALITY/MAINTENANCE AND SUPPORT.

BRITECITY will regularly evaluate your specific needs to make sure that you are operating at peak efficiency. We'll migrate you to cloud-based systems where they make operational and financial sense. We'll also take the lead in maintaining the cybersecurity of your systems and data.

Are you tired of your IT services? We have you covered in Orange County! Speak with an IT professional today. Call 949-243-7440 for more information or to book an appointment.

We can't wait to hear from you!

