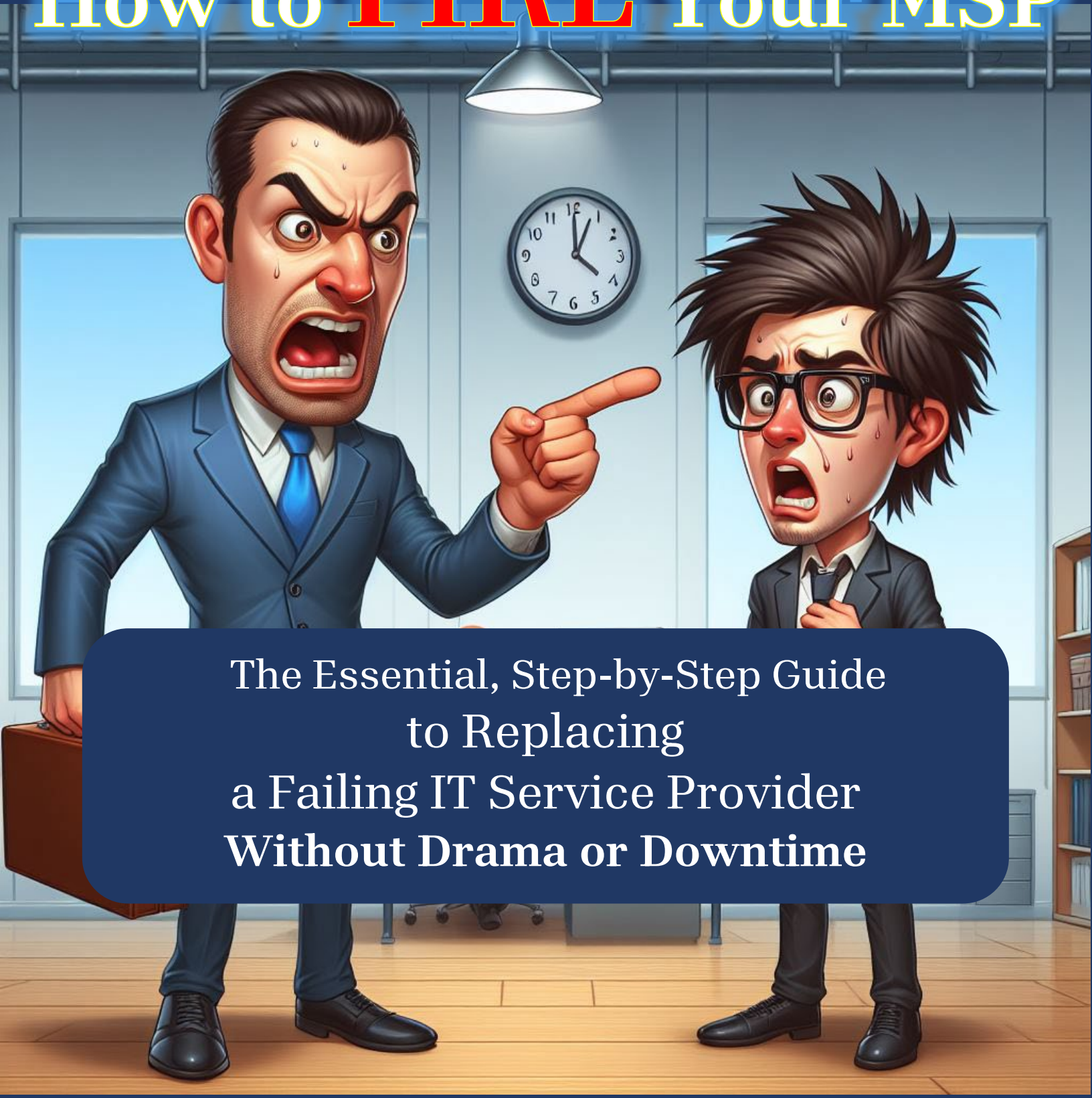
How to FIRE Your MSP



The Essential, Step-by-Step Guide
to Replacing
a Failing IT Service Provider
Without Drama or Downtime

Bryan Sullo

Disclaimer:

The information contained in this book is for general informational purposes only. It does not constitute legal advice or any other type of professional advice. While we strive to provide accurate and up-to-date information, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability with respect to the content contained herein. Any reliance you place on such information is strictly at your own risk.

In no event will we be liable for any loss or damage arising out of or in connection with the use of this book. This includes, but is not limited to, indirect or consequential loss or damage, loss of data, income, profit, or opportunity, or damage to property or reputation.

The views expressed by the author(s) are their own and do not necessarily reflect the views of the publisher or any other party associated with the creation or distribution of this book.

---

www.ClocktowerTech.com

Table of Contents

Introduction

Who should read this book?

- Does your organization utilize a managed service provider (MSP) to support and secure your technology infrastructure?
- Are you the person responsible for overseeing the MSP relationship?
- Have you ever doubted that your MSP is really providing value, really saving you money, or really keeping you secure?

If you answered yes to the questions above, this book was written for you.

Too many organizations stay in bad vendor relationships because they either don't know how bad they are, or they don't want to go through the hassle and expense of extracting themselves from that relationship. ***How to Fire Your MSP*** **presents a clear, non-technical framework to evaluate your current MSP's performance, suggestions on how to work with your current MSP to improve their performance (if possible) advice on how to vet a new potential provider (if this becomes necessary), and how to get rid of your current one.**

Why should you listen to me?

As the cofounder of an MSP, with over 25 years in the industry, I've seen the good and the bad sides of the managed services industry from its infancy. Heck, I've been on both sides—the good side more than the bad side—but there were times when our clients probably should have fired us and didn't. We learned from our mistakes, and it made us even more valuable to our clients.

You might think that *How to Fire Your MSP* is just a long-form sales pitch designed to cast doubt on your current provider so that you'll hire a new one. I've tried, throughout the first part of this book, to indicate ways in which you can improve your relationship

with your current MSP if it makes sense to do so. And . . . if you're afraid that shining a light on your current vendor's practices might make you doubt them, you might need this book more than you think.

The ultimate reason you should listen to me, though, is that I'm telling the truth. This book has been reviewed by my peers in the managed services industry, and, while we all have different approaches, we generally agree on the fundamentals of what differentiates an MSP that you want to keep from one you want to fire.

Chapter 1: Should You Fire Your MSP?

Why companies fire MSPs – the underlying cause

Companies ultimately fire a managed services provider for one of three reasons:

1. The MSP lost the client's trust.
2. The MSP did not fulfil the client's expectations.
3. The client outgrew the MSP's service model or capabilities.

Regardless of the inciting event or the reasons a client might use to justify the separation (even to themselves) the underlying cause is always one of the three items above. Let's consider each of these underlying causes in a little more detail, so you can decide which one fits your scenario.

Don't skip this step. Discovering the underlying cause of your dissatisfaction is foundational to the rest of the process.

Underlying cause 1: loss of trust

The relationship between a client and their IT service provider requires an immense amount of trust in both directions. When a client engages an MSP or other IT service provider, they are essentially handing the provider the keys to the kingdom. There is virtually nothing an MSP cannot do—no file they could not open, no email they could not read, no system they could not irreparably destroy. A client must be supremely confident of their MSP in three areas:

1. **Ethics**: The MSP must always demonstrate that they operate with the client's best interests in mind. An MSP might break this trust through behaviors such as reading client emails, making recommendations that benefit the MSP more than the client, or sneaking in unwarranted charges.

2. **Ability**: The MSP must exhibit due care in supporting the client's systems. An MSP might break this trust by losing data, causing unnecessary disruption, or failing to act on signs of potential problems.
3. **Security**: The MSP must operate in a manner that does not introduce additional security vulnerabilities to their clients' environments. An MSP might break this trust by exhibiting poor cybersecurity practices.

Often, there's no single event that leads to the lack of trust. It's generally a pattern of behavior, and one of those behaviors might simply be that the MSP is cagey when discussing their ethics, ability, or security.

If your dissatisfaction with your MSP stems from a loss of trust, you should make sure you have an accurate assessment of the situation before you decide to fire them.

Is it really a breach of trust, or is it a perception/communication problem? Examples:

1. **Perception: The MSP lost your data.**

   Possibility: The data loss had already occurred through no fault of theirs, but they were unable to recover the data.

2. **Perception: The MSP is charging you for things you never agreed to.**

   Possibility: The charges are in the contract, but the situation that warrants the charge has only recently been encountered.

3. **Perception: A recent data breach must be the fault of the MSP because it's their job to keep you secure.**

   Possibility: The breach occurred because you had previously declined to take suggested actions to protect your systems.

I'm not saying that your lack of trust isn't justified, just that you should be sure that your perception of the situation is accurate before acting.

Underlying cause 2: lack of performance

Is your MSPs response time worse than it used to be? Does it seem like you're having more problems, and they're taking longer to get resolved?

Just like any business, MSPs go through cycles. Maybe they just brought on a few new clients, and onboarding those clients is eating up their time. (Although this is temporarily unpleasant for you, we'll talk about why it may be a good thing later in this chapter.) Maybe their newest technician is not as skilled as they claimed on their resume. Maybe they are having trouble finding a qualified candidate to fill a necessary position.

Working with an MSP is very cost effective compared to hiring your own staff and purchasing your own management and security tools. One of the tradeoffs is that an MSP is a shared resource, and their ability to service you at any given time might be affected by circumstances outside your—or even their—control.

Putting up with *temporary* performance problems is *occasionally* necessary, and a frank conversation should reveal the cause and the solution. There might be a larger problem, however, if the MSP cannot identify the cause of the performance problem, doesn't offer a solution, or doesn't make good on the solution.

Underlying cause 3: growth

In business, growth is good, but growth requires change.

Advice from experience

Back in the early days of our managed services business, we didn't offer 24/7 support because we didn't have the resources to provide it. Our best client had been growing for a few years in a row, and they were at the point that they were operating multiple shifts, all of which were dependent on their technology.

A new CFO came in, and he had an IT company in mind, but he gave us the opportunity to revise our agreement to include 24/7 support. We could have tried to offer it at that

point, but we would have failed. We let the client fire us because we didn't have the capabilities to support their growth at that time.

Things that aren't true causes

Price: Despite what they say, no one fires an MSP because of the price. A client will almost always pay more to a new MSP than they paid to their last one. The true cause is one of the three items above, and price is almost always an excuse to avoid identifying the real, underlying cause. (The exception to this rule is if the company is shrinking and just can't afford to pay even the minimum amount required by the MSP to retain them.)

Merger/Acquisition: When one company is acquired by another, the acquiring company will have their own IT support. If the acquiring company is substantially larger, it may be the case that the MSP wouldn't have the capabilities to service their needs. (This is a growth problem.) If the companies are not quite as unequal, there may be an opportunity for the MSP to continue to service the acquired organization or to take over for both organizations. There is no natural barrier to this, so the true cause must be that the MSP was not trusted enough or performing well enough for the old ownership to come to bat for them in the negotiations.

If you're considering firing your MSP, you need to clarify the primary reason: Is it loss of trust, lack of performance, or growth?

Signs it's time to act

At this point, you should have an idea of why you're considering firing your MSP. We'll discuss how to do that in chapter three, and the core reasoning you defined above will inform that process.

Extracting an MSP from your organization is not easy though, and whatever reason you came up with might not be enough to justify the trouble. You might be wondering,

“Am I overthinking this?” or “Is there really a problem here?” In this section, we’ll do a deep dive into several signs that might indicate a problem.

Sign 1: They don't give you access to admin-level credentials

Security best practices dictate that no user’s everyday account should have administrative privileges. However, that doesn’t mean that no one in the company should have separate administrative access to your company’s systems.

Often, MSPs are legitimately reluctant to grant admin access to their clients because anything their client messes up becomes the MSP’s problem. An MSP with mature practices should proactively assign admin-level access for all systems to one or more designated contacts via separate user accounts. They will not (nor should they) provide their own admin-level account credentials to you or your employees because that would eliminate their accountability. (It’s also unnecessary, since you could always revoke their rights with your own admin accounts.)

A less mature MSP will share their admin-level account with you when asked. This is not ideal because no one can be held accountable for these accounts’ actions, and password management becomes difficult (leading to delays and disruption).

If the MSP has not proactively given you admin access, you might get a little pushback when you ask for it. Their first thought is always going to be that you want it because you’re getting rid of them. You can counter this objection by explaining that it’s a matter of security and business continuity, or that it’s required by your cyber insurance or board of directors, and that you understand the responsibility that comes with having administrative privileges and that you are willing to put this into writing. See Appendix B: Enhanced-Privilege Account Acknowledgement

If you receive much additional pushback, this could indicate an MSP that is not trustworthy, unsure of their abilities, or simply not very mature.

Sign 2: They know your user's passwords.

I'm not going to discuss the fact that even you shouldn't want your users' passwords, but your MSP should not keep users' passwords on file. Doing so can make service faster in some cases, but it's a security and accountability problem just waiting to happen.

Sign 3: You have never discussed RTO and RPO.

RTO = Recovery Time Objective; the maximum amount of time it should take to restore a system from backup.

RPO = Recovery Point Objective; the maximum gap between the last good backup and the time the system failed.

If you've never had a conversation about defining these values, what are they basing their backup procedures on? How do you know that what you need will be there when you need it?

Sign 4: They cannot produce their internal security policies.

It is the nature of the managed services business that your MSP has centralized, Internet-accessible systems with immediate, and almost limitless control of your IT assets. This is an enormous responsibility, and, if not properly secured, can introduce great risk into your organization.

Your MSP's internal security policies define how they keep their systems secure and how they handle your data. Their security policies are what keep you safe from a breach in their systems.

At a minimum, your MSP should be able to produce the following three documents:

1. *Which cybersecurity framework they use for their internal security*

Ask the question. The actual answer doesn't mean too much (there are several good cybersecurity frameworks to choose from), but if they don't know what you're talking about, or they answer with the name of an anti-virus or other security product and not

the name of a framework, they don't have a good handle on security. Here are some acceptable answers: (They may use more than one framework, and they may phrase the answer in the form of, "We comply with…")

- HIPAA
- CMMC
- NIST 800-171
- NIST Common Security Framework (CSF)
- GDPR
- Center for Internet Security (CIS) Common Controls
- ISO 27001/27002

They may also mention that they have undergone a *SOC* audit, which is not the same thing, but does indicate that they are serious about cybersecurity.

2. Breach response plan

This is the MSP's plan for what happens if they suffer a security breach. You want to see this **in writing**. The contents aren't what's important at this stage. Whether they have one or not is the critical part. To be effective, a written breach response plan needs to be immediately available. If your MSP takes too long to respond to a request to see theirs, it either means they can't find it or they're busy trying to write it! Either way, they are not prepared to handle a security breach, and this could affect your organization terribly.

3. Client information handling policy

This policy dictates how they handle your data. An MSP without a written client information handling policy is eventually going to lose control of your data or get you into legal trouble.

Your MSP might not have a document specifically called a Client Information Handling Policy (CIHP), but they should have policies similar to the following examples:

"All client data and information must be stored and accessed only on secured, encrypted systems owned or authorized by the organization. No client data may be stored on personal devices or uncontrolled cloud storage services."

"The organization shall implement strict access controls and logging to monitor which employees can view, modify, or download client information. Access will be granted only on a strict need-to-know basis."

"The organization will dispose of any client data or information using secure, certified data destruction methods. No client data shall be retained beyond the termination of the service agreement unless explicitly authorized by the client."

These types of statements help demonstrate that the MSP has clear, documented policies and procedures in place for properly handling and protecting their clients' sensitive data and information. Seeing concrete examples like these would indicate to the reader that the MSP has a valid CIHP, rather than just vague assurances about data handling.

4. Vendor security requirements

As stated above, many of the applications used by MSPs have unfettered access to your systems. MSPs must have a process to ensure their vendors are adhering to proper security practices. Your organization could be breached because of an irresponsible vendor's product the MSP introduced into your environment.

An MSP should have written documentation regarding how they vet and audit their vendors' security.

Sign 5: You would get out of your contract now if you could.

It's common for MSP contract terms to span multiple years. If the only thing keeping you in this relationship is the contract, that's an indication that you need to start preparing to fire them.

Sign 6: Their recommendations don't align with your organizational goals.

When your MSP makes recommendations, do you find yourself asking, "Who is the recommendation benefitting, us or them?"

If the MSP is unable to articulate ROI or risk mitigation associated with a recommendation, it might be an ethics problem, or it might be that the MSP doesn't truly understand your business. Either way, there's a red flag.

Sign 7: They do everything you ask without any pushback.

Does your MSP just do everything you ask without offering any alternatives or corrective advice? You might think that's great, but it's not. It's actually a very bad sign that could indicate one of a couple of things:

1. You might have a lazy MSP who cares more about making money on projects than keeping you operational and secure. The MSP should be the expert. If they're never playing that role, that's a problem that's going to get you in the future.
2. You might have worn them down by being too demanding. An MSP is only going to push back so many times before they give up and decide that doing what's right is not worth the argument. This could be due to a personality mismatch. Technicians tend to be compliant and conflict averse. If you're a "Type-A" personality, they may simply comply out of habit. If the MSP is big enough, you might ask for a different contact who can stand up to you. Otherwise, you're going to end up with a mess when all the things the MSP knew they should have done, but didn't, cause major problems.

Sign 8: They're not pushing you to keep current with technology and security.

There should always be some tension between the MSP and the client. I don't mean there should be a contentious relationship, but your MSP should be your technology coach. They should be pushing you to make decisions that are important but may be uncomfortable.

An MSP who just lets you coast along without making investments and improvements is setting you up for failure. This might indicate that they take your relationship for granted.

Sign 9: They don't have a recent third-party penetration test or security audit.

One of the most glaring red flags for an MSP is the lack of a comprehensive, third-party security audit or penetration test of their own systems and infrastructure. This type of independent security assessment is crucial for validating the effectiveness of an MSP's cybersecurity posture and controls.

A reputable MSP should be able to provide you with the results of a recent (no older than 12 months) security audit conducted by an accredited, third-party firm. This audit should cover critical areas such as:

- External and internal vulnerability assessments
- Penetration testing of network systems and applications
- Review of access controls and privileged account management
- Evaluation of security monitoring and incident response capabilities
- Assessment of data protection, encryption, and backup procedures

As the gatekeeper of your organization's IT infrastructure and information assets, your MSP must be held to the strictest security requirements. An MSP that cannot produce a recent, third-party security audit raises significant concerns. It could indicate they are hiding security vulnerabilities, lack the resources for proper security measures, or simply do not prioritize the protection of their own and their clients' sensitive data and systems.

Sign 10: You're not paying enough.

Wait, you're probably thinking. *Don't you mean, "You're paying too much?"*

Remember, price is never the true cause of dissatisfaction with an MSP. Everyone wants to pay as little as possible, but if you're getting an unbelievable deal, there's something wrong that you can't see.

Your cut-rate MSP may not have enough resources to support you when you need it most. When you get hit by ransomware, or have a major server outage, it may strain them to the point of breaking to be able to service you properly.

They may not be able to provide important security tools as they become available. MSPs are often forced to buy software licenses in bulk. They must pay for a minimum number of licenses (100, 500, 1000) and then they must try to resell them all to cover the cost. If your 25-user company could really benefit from a managed security product, but the MSP can't afford to buy the product until they sell it to several other clients, you'll be left unsecured until they do.

The tools that MSPs use, and the products they provide are always changing and improving. Sometimes, there are very good service and security reasons for an MSP to switch from one tool or product to another. That costs money, both in the labor to make the switch and in the overlap of services that might be incurred. You don't want your organization to suffer because your MSP can't afford to change tools when the need arises.

If you're not paying enough, your MSP likely has a very small R&D budget. If they're not innovating, they're stagnating, and this will come back to bite you later when the technology you need is not something they're familiar with.

The cheap MSP is likely not spending enough on training and education. Their technicians are stagnating, and they're dragging you down with them.

Sign 11: They're not growing.

An MSP that's not growing is dying.

An MSP that remains stagnant is a red flag that should raise serious concerns. In the highly competitive managed services industry, standing still often equates to falling behind. The most successful MSPs are continuously evolving to meet the changing needs of their clients and the rapid pace of technological change.

Growth is a key indicator of an MSP's financial health, technical capabilities, and commitment to innovation. Growing MSPs can invest in expanding their service offerings, upgrading their technology stack, and hiring top talent. This allows them to better serve their existing clients while also attracting new business.

On the other hand, an MSP that has flat or declining revenues likely lacks the resources to keep pace. They may be struggling to retain clients, falling behind on necessary infrastructure upgrades, or failing to develop new competencies. This stagnation will inevitably impact the level of service and support they can provide.

Chapter 2: How to Select a New MSP

If you've completed the evaluation process outlined in Chapter 1 and determined that it's time to part ways with your current managed service provider, the next step is to find a suitable replacement. This can seem like a daunting task, but by following a structured selection process, you can help ensure a smooth transition and a productive long-term partnership.

In this chapter, we'll walk through the key steps to vet and choose a new MSP that will meet the needs of your organization.

Identify your requirements

The first step is to clearly define what you're looking for in a new MSP. This should go beyond just the technical capabilities and include factors like industry expertise, service delivery model, company culture, and pricing.

Some key areas to consider:

- Technical expertise - Assess the types of technologies, software, and systems the MSP supports. Ensure they have experience with the core components of your IT infrastructure.
- Service offerings - Determine which managed services are most important, such as help desk support, network management, security monitoring, cloud migrations, and more.
- Industry experience - Look for an MSP that has worked with businesses like yours, ideally in your specific industry.
- Company culture - Evaluate whether the MSP's values, communication style, and overall approach align with your organization's preferences.
- Pricing and contract terms - Understand the MSP's pricing model, any minimum commitments, and the flexibility of the contract.

Document these requirements in detail so you can use them as a benchmark to assess potential providers.

Research and vet prospective MSPs

With your criteria defined, you can start researching and evaluating MSPs that may be a good fit. There are a few key steps in this process:

1. Compile a list of potential candidates. This can include referrals from your network, online directories, and vendors you already work with.
2. Review the MSP's website, case studies, and client testimonials to gauge their capabilities and experience.
3. Schedule introductory calls or meetings to get a sense of their sales process, responsiveness, and overall approach.
4. Request and carefully review sample service agreements and service-level objectives. Ensure the terms align with your requirements.
5. Conduct reference checks with current or former clients of the MSP. Ask about their experiences, both positive and negative.
6. If feasible, schedule an onsite visit to tour their facilities and meet the team that would be supporting your account.

This comprehensive vetting process will help you determine which MSPs have the right combination of skills, resources, and cultural fit to be successful partners.

Evaluate and Select the Winning Provider

Once you've narrowed down the list of prospective MSPs, it's time to make the final selection. This decision should involve key stakeholders from your organization to ensure alignment.

Some important factors to weigh in the final evaluation:

- Alignment with your technical and business requirements

- Ability to provide personalized attention and service
- Demonstrated expertise through case studies and references
- Financial stability and long-term viability of the MSP
- Overall "gut feeling" about their trustworthiness and culture

If possible, negotiate any final contract terms or pricing before making your selection. Get everything in writing to avoid any misunderstandings.

Once you've chosen your new MSP partner, work closely with them to develop a detailed transition plan. This will ensure a smooth handoff of responsibilities from your previous provider and minimize any disruptions to your business operations.

By following a structured selection process, you can find an MSP that will be a true strategic partner, helping to drive the growth and success of your organization for years to come.

Some additional thoughts on the selection process

When meeting with prospective MSPs, resist the urge to tell them all the things you don’t like about your current MSP, allowing them to regurgitate that back to you as their selling points.

When it’s clear that a prospective MSP is in the running to get your business, let them know (if applicable) that you’re giving your current MSP a chance to rectify the problems, and when you will be making the final decision. This will help set expectations, and it will ultimately result in a smoother transition.

Chapter 3: How to Fire Your MSP

You've decided it's time to cut the cord. You've had enough. Wait!

If you jumped to this chapter without reading the first two, stop. Here's why:

You might be able to save a lot of time, aggravation, and money just by having a frank conversation with your current MSP. Most bad business relationships are bad because the parties aren't communicating. Your MSP may be giving you what they think you want, or they may be providing what you needed three years ago when you first signed with them, but they may not realize that your business has changed—or that expectations were never set correctly to begin with.

As someone who has infrequently been on the receiving end of that "cancel call," my first thought has always been, *Why didn't they tell us there was a problem and give us a chance to work it out?* The answer is often that the client didn't know how to articulate the problem. If that's you—if you're feeling like you're ready to cancel that contract, but you can't clearly articulate why—go back and read chapter 1: "Should You Fire Your MSP?".

The other reason you need to take a step back before you burn that bridge is that you need to have another bridge in place (or at least in the process of being built) first. Except in the cases of gross incompetence, negligence, or unethical behavior, where your current MSP is putting your organization at risk, it's unwise to fire an MSP without lining up their replacement first.

MSP's do a lot behind the scenes and are responsible for keeping much of your IT and OT infrastructure running and secure. Canceling services without a good hand-off plan in place can leave your organization open to downtime and security breaches. If you don't have a new MSP lined up, go back now and read chapter 2: "How to Select a New MSP".

Once you've identified that firing your MSP is a viable option, there are a few items you'll want to do *before* you make that final decision.

Step 1: Review the contract.

Oh, that heady day when you signed the agreement with your current MSP: They were going to solve all your problems, and the contract was a mere formality—something to be dispensed with quickly, so you could start reaping the benefits of the services so deftly sold. Do you remember what you signed?

Or maybe it was your predecessor who made the arrangements. Do you know where the contract is?

Your first challenge at this step might be laying your hands on the current agreement. This should be something that's always available to you but given the fact that you're at the point of firing your MSP, it's likely this is an area in which they're lacking.

If you don't have a copy of your contract, the best way to get one is to ask for it. That, of course, is likely to tip them off that something is up. I recommend the direct approach:

"Hi, Jim. I'd like to set up a meeting to discuss the services you're providing. I think we can work through the issues, but they're serious enough to warrant a face-to-face discussion. Please bring a copy of the current contract."

Some MSP contracts are easy to cancel. Others can be problematic or expensive. Make sure you know the terms of the agreement and the termination requirements, including any buyout or termination fees. These will factor greatly into the timing and costing of your decision.

Step 2: Get buy-in.

This isn't a decision you want to make in a vacuum. If you're the business owner, talk to your management team. If you're in management, talk to the owner or other

executives. You may find out that your current MSP is providing a service you didn't know about that is critical to some process in your business.

Advice from experience:

Making technical decisions without consulting other members of the team often leads to disaster. Several years ago, a client's marketing director was reviewing their Internet connectivity bills. (Why the marketing director was responsible for Internet connectivity is another story.) He saw that they were paying for five, static, external IP addresses and decided that they only needed one. Without consulting anyone, he called up the ISP and put in a change order to reduce to a single address. A week or so later, the ISP removed the block of five addresses from their service and provided a new, single address. This inevitably brought down their Internet connection for the better part of a day, while we scrambled to figure out what had happened!

Getting buy-in not only makes the transition process smoother; it prevents you from being the one who accidentally saws the limb out from under your team.

Step 3: Take inventory.

There are a few items that could lead to a messy transition if you don't have them, or if you don't know about them.

Advice from experience:

We once took on a client where the former in-house network administrator simply left one day without leaving any documentation of administrator passwords or system configurations. It was difficult. There was downtime. It took almost a year before we stopped finding systems and services we didn't know about and couldn't access.

Here's the documentation you must have before you can even think about switching to another MSP:

Administrator and service account credentials for all systems

Administrator, or *privileged*, accounts are accounts on a system that can do things like creating, disabling, and resetting the passwords of other accounts on that system. These are not (or should not be) individual user accounts.

Service accounts are used behind the scenes to enable specific services to run automatically and have access to the systems and data they need to perform their functions. If you have an admin account, you can usually reset these accounts' passwords, if necessary, but it's easier to have them documented.

Your current MSP probably has (or should have) their own privileged account(s) on your systems. You do not need, nor do you want, these credentials: The primary purpose of multiple administrator accounts is to enforce accountability upon all parties. Your MSP should have one or more admin accounts that you do not have the password for, and you should have one or more admin accounts that the MSP does not have the password for. If things ever get contentious, and something goes wrong, a review of the system logs will quickly show who did what, when. If you have the MSP's credentials, or if you share an administrative account, the logs are essentially rendered useless for this purpose.

You also don't want (nor should your MSP have) the credentials for individual user accounts. This is essentially for the same purpose as above. If you ever need to review logs for legal or compliance purposes, you need to be sure that the actions performed by each account can be traced to a single individual, and not an admin (or business owner) who happened to know the account password.

A quick note on the above: You absolutely *do* want an inventory of your MSP's privileged accounts and your individual users' accounts. You just don't want to know the passwords for those accounts.

MSP's can get a little touchy about providing admin passwords to clients, and not without reason. An MSP assumes a lot of liability for the operation and security of their clients' systems. Even a well-meaning client employee who has admin access can make

a change that disrupts systems or works counter to something the MSP put into place (making a lot more work for the MSP). Add to this the security implications of another set of privileged credentials to potentially get stolen, and it's enough to give any MSP a little anxiety.

If you share admin credentials with your MSP, talk to them about the security and accountability implications of that scenario.

If you don't even have admin credentials, explain that you'd like a "break-glass" admin account *for all systems*. You've seen the signs that say "BREAK GLASS IN CASE OF FIRE"; this is the same thing. What happens if, for some reason, your MSP is unable to service your account, even temporarily? For this reason alone, you need such an account. When the MSP assigns these accounts to you, immediately change the passwords and then store the credentials in a secure location.

Here are some examples of systems for which you should have admin-level credentials:

- Active Directory (Windows domain)
- Non-domain-joined computers
- Routers, switches, wireless access points, and other network infrastructure systems
- Accounting software
- Line-of-business applications
- Web hosting (if your MSP provides this for you)
- Domain registrar
- DNS host
- Microsoft 365 / Entra ID
- Printers

Some systems (like printers) are not capable of having more than one admin account. In that case, the MSP should share the admin account credentials with you and keep them up to date if they change.

Software and Services

Ideally, you want an inventory of all software and services used in your organization. (Your MSP should be providing this for you already.) At the minimum, however, for the purpose of transition planning, you need to have an inventory of all software licenses and services that are provided by your MSP. I usually ask the question this way:

"What software or services will go away when you leave your current MSP?"

The answer to this question may be found in the contract, but it may not. You need to know the answer before you can even start talking to another MSP, because they're going to need to know which services they will need to provide.

Examples of software or services that may be provided by your MSP:

- Anti-virus/anti-malware software
- Microsoft Office licensing
- Backup systems
- Web hosting
- Domain registration
- DNS hosting
- Remote access solutions
- Other security software

Equipment

Does your MSP own any of the equipment in your environment? Does your MSP have any of your organization's equipment at their office?

This can be messy if you're in a hardware-as-a-service (HaaS) arrangement with your MSP, since you're technically only renting the hardware from them. If you are in a HaaS

arrangement, you'll need to determine what hardware is part of that arrangement and if there is a buyout option.

Assuming you don't have a HaaS agreement, your current MSP could still have their hardware in your environment:

- Many MSP's will have a "jump box" or other management PC installed on your network.
- Your MSP may have provided a loaner switch, router, PC, etc. that they will want back when you terminate the contract.

Domain registration and DNS access

This critical component should be covered in the password requirements above, but it may not be, in certain circumstances.

This is an often-forgotten part of migrating services from one MSP to another. DNS is what controls (among other things) where your email goes and where it's allowed to originate from. Without the ability to modify DNS for your Internet domain, you cannot change your email service (or your Web site, among other things).

There are two primary entities involved here:

1. The domain registrar
2. The DNS host

The domain registrar is the organization that you "buy" your domain name from. They grant you the right to select the host for that domain's DNS records.

The DNS host is often the same entity as the registrar but doesn't have to be. The DNS host maintains all the DNS entries for your domain. It's what tells email servers, for example, where to send mail that is addressed to your domain, or Web browsers how to find your Web site (among many other essential services).

If your current MSP provides domain registration and DNS hosting, they may not have the ability to grant you access to those, since that might require them to grant you access to all their clients' records.

If you control your registration and DNS hosting, you will likely get an invoice from your registrar every one to five years, depending on how long you've registered for. If you don't know, you can look up your domain's registrar using the ICANN lookup tool at https://lookup.icann.org/.

Other important information

If you have the three items above documented (admin credentials, MSP-provided software and services, equipment), your incoming MSP will probably be able to work out the rest. It will make for a smoother transition, however, if you have the following items:

- Network diagram
- Inventory of all systems (on-premises and cloud)
- Routing and port-forwarding rules
- Active Directory configuration
- Email configuration details
- Internet connectivity details
- Application inventory
- Application licensing details

Step 4: Have "The Talk."

This is where you put your current MSP on notice. Again, I strongly recommend that you don't simply fire them without giving them a chance to rectify their shortcomings.

This is a conversation you need to have face to face, if possible. If that's not practical, videoconference or at least telephone, are acceptable. You don't want to do this via email, although you *do* want to document what is said via email.

Before you call the meeting, document your grievances. (Don't present them at this point.) Be as specific as possible, and where possible reference any relevant language from your contract. The goal of this stage is to eliminate ambiguity from your relationship, so the clearer you can be about what you expect, the faster you will know whether the MSP can deliver.

As you're compiling your list, resist the temptation to start adding "wish list" items or ask for monetary concessions. A poorly performing MSP is rarely in a position to add additional services or give credits. They may do so just to appease an angry client, but the result will not be sustainable, and they may end up firing *you* eventually.

This meeting should have one of the following three outcomes:

1. Both parties reach an agreement about what needs to be improved and establish a timeline for improvement. The MSP should know that if they do not meet the measurable milestones by the allotted time, you will be hiring a new MSP.
2. The MSP suggests you part ways. Not every MSP is a good fit for every client, and most know when they need to give up a client but don't want to admit it. This meeting might be just the nudge they need. In this case, you'll need to work out a transition timeline with them.
3. The parties cannot agree on the problems or solutions. This, of course, is the worst outcome. If you can't come to an agreement, the MSP needs to know that they won't be your MSP for much longer.

Whatever the outcome, make sure you document the specifics of the meeting (avoiding any emotional, sarcastic, or non-essential language) and send them to your current MSP. I suggest using the *Realignment Meeting Agenda* found at https://HowToFireYourMSP.com.

The MSP representative may not be able to respond to all your requests in the meeting. That's okay, but they need to agree on a time frame to do so, and they need to meet that time frame.

A detailed guide for evaluating your current MSP

Before you make the decision to fire your current MSP, it's important to conduct a thorough evaluation of their performance and the services they are providing. After all, the underlying causes for dissatisfaction outlined in Chapter 1 may be fixable—if you and your MSP are both willing to put in the work.

In this section, we'll cover the key steps to effectively evaluate your MSP's performance and decide if the relationship is salvageable, or if it's truly time to start looking for a replacement.

Establish Clear Service Level Objectives (SLOs)

One of the most common issues with MSP relationships is a lack of clearly defined service expectations. If you and your MSP haven't mutually agreed upon specific SLOs, it will be difficult to objectively assess their performance.

At a minimum, your SLOs should cover areas like:

- Response times for different priority levels of support tickets
- Uptime and recovery time objectives (RTO) for critical systems
- Security monitoring and incident response protocols
- Regular reporting and business reviews

Work with your MSP to document these SLOs in writing, and make sure there are defined penalties or consequences if they fail to meet the agreed-upon standards. This creates accountability and gives you leverage if performance issues arise.

Regularly Review MSP Reports and Metrics

Most reputable MSPs will provide regular reporting on the health of your IT environment and the services they are delivering. These reports should include key performance indicators (KPIs) that allow you to objectively evaluate their effectiveness.

Common KPIs to track include:

- Ticket volume and resolution times

- Uptime and availability of critical systems
- Security events and remediation efforts
- Project delivery and milestones
- Overall satisfaction ratings from end-users

Review these reports diligently, and don't be afraid to ask questions or request additional data if something seems amiss. The MSP should be transparent in sharing this information and be willing to discuss areas for improvement.

> Some owners/managers expect to abdicate responsibility for IT to their MSP forgetting they need to review actionable reports and communicate regularly with the MSP team.

Establish Effective Communication Channels

Strong communication is essential for any successful MSP relationship. Make sure you have regularly scheduled check-ins, both at the technical and executive levels, to discuss performance, priorities, and any concerns.

Additionally, ensure you have clear processes in place for end-users to report IT issues and track the MSP's responsiveness. Consider implementing a customer satisfaction survey to get unfiltered feedback from your team.

Open, transparent communication will help identify problems early before they escalate and give your MSP the opportunity to address any deficiencies.

Enforce Accountability

As mentioned in Chapter 3, it's crucial that you have administrative-level access to your organization's IT systems, separate from the MSP's access. This ensures proper accountability and visibility into their activities.

Additionally, carefully review your MSP's internal security policies and processes. Verify that they are following industry best practices for data handling, incident response, and vendor management. Their security posture directly impacts the security of your organization.

If you uncover any red flags in these areas, it may be time to have a serious conversation with the MSP about improving their practices.

Document, Document, Document

Throughout this evaluation process, be sure to thoroughly document any issues, failures to meet SLOs, or other concerns you identify. This paper trail will be crucial if you ultimately decide to terminate the relationship and transition to a new MSP.

Keep detailed notes on your communications with the MSP, including any promises or corrective actions they commit to. This will serve as evidence if they fail to follow through.

By taking the time to conduct this comprehensive evaluation, you'll be in a much stronger position to make an informed decision about the future of your MSP relationship. It may reveal opportunities to improve the partnership or confirm that it's time to start looking for a new provider. Either way, a thorough assessment will help you move forward with confidence.

FAQ's for the firing process

Here I want to address some questions you might have about this step of the process.

What if we are the problem?

To be honest, this is a question that is asked far less frequently than it should be, but you really do need to ask this of yourself before you have a realignment meeting.

> On my wall, hangs a humorous poster that states, "The Only Consistent Feature of All of Your Dissatisfying Relationships is You." It reminds me, when I'm having a disagreement with a client, a vendor, or an employee, to perform a self-assessment and make sure that I'm not the problem in the relationship.

The MSP business, as are many businesses, is all about managing expectations. If your MSP is not managing expectations well, they're leaving it up to you to set your own. If you're not communicating those expectations, you and your MSP are likely to assume your expectations are aligned when they're not. That's the reason

for a realignment meeting, and it will help to be open to the possibility that at least some of the problems may be caused by your own lack of communication.

What if the MSP becomes uncooperative?

Most MSP agreement terminations come as a surprise to the MSP. Oh, there may be signs, but clients rarely telegraph their intention to leave until they've already lined up a replacement. You likely have several concerns that might lead you to consider the "sneak attack" approach:

- The MSP might just up and quit right there.
- The MSP might become uncooperative or put your needs at the back of the queue.
- The MSP might sabotage your systems out of spite.

First, even a bad MSP's actions will be guided by self-preservation. The likelihood that they're going to turn malicious on the way out the door is very slim as the legal and reputational repercussions would probably put them out of business.

Second, having this realignment meeting will avoid most of these outcomes. When the MSP sees that you're giving them a chance to correct perceived problems, they're going to appreciate it (even if they don't like it) and act accordingly.

If you do have evidence that the MSP may act maliciously, you'll want to engage a new provider sooner in the process and have them help you secure your systems first. This will likely mean that you'll be paying two monthly fees or at least a project fee to the new MSP.

What if they talk over my head?

One of the primary reasons that companies hire MSP's is that they don't have their own highly technical staff. I've seen owners and executives who are afraid that the MSP has a natural advantage in this kind of conversation because they understand the technology and can talk around the issues with technical jargon.

That's why we recommend being as specific as possible with your grievances and setting measurable goals for correcting the problems. If the MSP representative talks in

such a way that you cannot understand whether they agree or disagree then you don't have agreement. (You don't have a very good rep either, but that may be part of the problem.)

One option is to bring an outside peer or other trusted individual into the conversation, who knows the lingo better than you. This should not be another MSP. That will just lead to unnecessary contention.

Step 5: Give them a chance.

If you were unable to reach agreement on problems and solutions, you should skip this step and move on to cancellation. Otherwise, you need to give the current MSP the chance that you agreed to. If they can deliver, the result may be a better relationship than ever.

You may try to be nice by being lenient, but, barring extraordinary circumstances, this is not the time for leniency. If the MSP cannot live up to the agreement they made in response to the realignment meeting, it's time to say goodbye.

Step 6: Initiate the Cancellation Procedure

After giving your current MSP the chance to address the issues identified in the realignment meeting, if they have failed to meet the agreed upon milestones and improvements, it is time to officially cancel the contract and transition to a new provider.

Every managed services contract will have slightly different termination requirements, so your first step is to thoroughly review the terms of your existing agreement. Make sure you understand the following:

- Required notice period for termination
- Any early termination fees or penalties
- The process for transferring services and data to a new provider

With this information in hand, you can begin the formal cancellation process. Here are the key steps:

Notify the MSP in Writing

Provide official written notice to your current MSP that you are terminating the contract, citing the specific reasons and referencing the realignment meeting discussions. Be sure to adhere to the notice period outlined in your agreement.

In this notification, request a detailed transition plan from the MSP that addresses the following:

- Timeline for transferring all accounts, passwords, and administrative access to you
- Procedures for migrating data, backups, and configurations to the new provider
- Commitment to maintain service levels during the transition period
- Cooperation in introducing the new MSP to ensure a smooth handoff

Insist that the MSP adheres to this transition plan to the letter. Any delays or obstructive behavior should be well-documented.

Establish a Transition Timeline

Work closely with your incoming MSP to develop a comprehensive timeline for the transition process. This should include specific milestones and deadlines for completing each step.

Key transition activities may include:

- Migrating email, cloud services, and on-premises applications
- Transferring domain registrations, DNS hosting, and internet connectivity
- Ensuring all administrative and service accounts are properly handed off
- Conducting knowledge sharing sessions between the old and new MSPs
- Testing and validating the functionality of all migrated systems

Hold both your current and new MSPs accountable to this timeline to avoid costly delays or gaps in service.

Facilitate the Knowledge Transfer

During the transition, make sure there is thorough documentation and knowledge sharing from the outgoing MSP to the new provider. This will be crucial for the new MSP to quickly get up to speed and prevent any disruptions.

Some key items to transfer include:

- Network diagrams and documentation
- Inventory of systems, software, and services
- Administrative access details and credentials
- Pending projects, open tickets, and known issues

Actively participate in the knowledge transfer process to ensure nothing falls through the cracks.

Validate a Successful Transition

Before officially terminating the contract, work with the new MSP to extensively test and validate that all systems and services have been properly migrated and are functioning as expected.

Only once you are completely satisfied with the outcome should you provide final notice to the outgoing MSP and authorize the release of any remaining funds or equipment.

By following a structured cancellation procedure, you can help ensure a smooth, successful transition to your new managed service provider. Careful planning and documentation will be crucial to mitigate risks and protect your business throughout the process.

Chapter 4: Concluding Thoughts

Congratulations! If you've reached this point, you've successfully navigated the challenging process of evaluating your current managed service provider (MSP) and transitioning to a new partner. This is no small feat, and you should be proud of the due diligence and careful planning you've undertaken.

Throughout this guide, we've covered the key steps involved in this process - from identifying the underlying causes for dissatisfaction with your existing MSP, to vetting and selecting a replacement, and finally, executing a smooth transition. However, the work doesn't stop once the new MSP is in place. Maintaining a healthy, productive partnership requires ongoing effort on your part.

Reinforce a Culture of Accountability

The foundation of a successful MSP relationship is clear accountability. Ensure you have established proper administrative access and visibility into your IT systems, separate from the MSP's access. Regularly review activity logs and performance reports to verify the MSP is adhering to their commitments.

Additionally, maintain open and transparent communication channels. Schedule recurring meetings to discuss progress, identify any issues, and collaborate on continuous improvement initiatives. **Remember, your MSP should be a strategic partner, not just a vendor.**

Continuously Optimize the Relationship

As your business evolves, so will your technology needs and the services required from your MSP. Don't become complacent. Regularly re-evaluate your MSP's performance against your current and future requirements.

This may involve renegotiating contract terms, adjusting service levels, or even considering alternative providers down the line. The key is to stay proactive and adapt the partnership as needed to ensure it continues delivering maximum value.

Prepare for the Unexpected

Even the most carefully planned MSP transition can encounter hiccups or unforeseen challenges. Maintain comprehensive documentation of your IT environment, administrative access, and the transition process. This will be invaluable if you ever need to make another change in MSP providers.

Additionally, have a clear plan in place for quickly restoring critical business operations in the event of a service disruption or security incident. Your MSP should play a key role in this business continuity planning.

Parting Advice

Selecting and transitioning to a new MSP is a significant undertaking, but it's one that can pay dividends for your organization in the long run. By following the structured approach outlined in this guide, you can help ensure a smooth, successful outcome.

Remember, the MSP you choose will be a strategic partner responsible for a core function of your business: the health and security of your technology infrastructure. Take the time to get it right, and you'll be rewarded with a productive, long-lasting relationship that supports the growth and success of your organization.

Appendix A: Glossary

Credentials : A username-password combination or other secret information that allows an individual to sign in to a computer system.

HaaS : (Hardware-as-a-Service) - A service model where the MSP provides and manages the hardware infrastructure for the client, who pays a monthly fee rather than a large upfront capital expense.

ICANN : (Internet Corporation for Assigned Names and Numbers) - The global non-profit organization responsible for coordinating the Domain Name System (DNS) and IP addressing.

ISP : (Internet Service Provider) - A company that provides internet access and related services to individuals and businesses. ISPs are responsible for providing the physical infrastructure, such as fiber, cable, or DSL, to connect users to the internet.

IT : (Information Technology) - The study, design, development, application, implementation, support, and management of computer-based information systems. IT encompasses hardware, software, networking, and the people who work with these components.

KPI : (Key Performance Indicator) - Measurable values used to evaluate the performance and effectiveness of an MSP in meeting service level agreements and other objectives.

MSP : (Managed Service Provider) - A company that remotely manages a customer's IT infrastructure and/or end-user systems. MSPs take on the responsibility for monitoring, maintaining, and

supporting a customer's technology environment, typically for a recurring fee.

MSSP : (Managed Security Service Provider) - A specialized type of MSP that focuses on providing comprehensive cybersecurity services, including security monitoring, threat detection, incident response, and regulatory compliance management.

OT : (Operational Technology) - The hardware and software that monitors and controls physical equipment, processes, and events in industrial environments, such as manufacturing, energy, and transportation systems.

Privileged Account : An administrative or service account with elevated permissions on a system or network, beyond those of a standard user.

RPO : (Recovery Point Objective) - The maximum targeted period for which data might be lost from an IT service due to a major incident.

RTO : (Recovery Time Objective) - The maximum targeted duration for restoring a business process or system after a disruption or disaster.

SLA : (Service Level Agreement) - A contract between an MSP and client that defines the level of service and support to be provided, including performance metrics, responsibilities, and consequences for not meeting agreed upon standards.

SMB : (Small-to-Medium Business) - A business entity that maintains revenues, assets, or a number of employees below a certain threshold. The definitions of "small" and "medium" vary by

country and industry, but they generally refer to companies with fewer than 500 employees.

SOC : (System and Organization Controls) - An audit report that demonstrates that an organization has been evaluated against a set of rigorous control standards for managing data, security, and other operational processes.

Appendix B: Enhanced-Privilege Account Acknowledgement

I, [Name], acknowledge that I have been entrusted by [Company] (hereinafter, "Organization" or "the Organization") with access to certain, elevated technical privileges allowing me to perform administrator-level tasks on one or more Organization systems. In accepting these privileges, I acknowledge and consent to the following:

1. I understand that the use of elevated privileges may allow me to bypass security safeguards, and that this introduces risk to the Organization. I will exercise due diligence in electing to use elevated privileges and due care in the execution of any task performed while using elevated privileges.

2. To prevent an accidental or opportunistic security breach, I will use a privileged user account only when the privileges granted by that account are necessary. I will not use any privileged user account for tasks that do not require elevated privileges (e.g., reading email, general Web browsing).

3. Privileged accounts assigned to me are for my use alone. I will not share credentials for privileged user accounts that have been assigned to me.

4. When selecting a password for a privileged account, I will not reuse a password I have used for any other account (privileged or non-privileged).

5. I am responsible for the security of any privileged account credentials I have access to. If I suspect a privileged account may have been compromised, I will change the password, disable the account if possible, and inform IT support immediately.

6. The granting of technical privileges does not entitle me to access Organization information I would not otherwise be privy to. I will not use elevated privileges to

view, copy, transmit, modify, or destroy data, unless such action is required to fulfil the duties for which I was granted the elevated privileges.

7. I will not arbitrarily bypass security practices for the sake of expediency, secrecy, or any other reason.
8. I will not install, uninstall, or modify software, change settings, or perform other actions counter to the written information security policy of the Organization.
9. I understand that the privileged account assigned to me may be disabled after a period of inactivity or that the account may be revoked at any time by the Organization.

I understand that failure to adhere to the above can lead to system downtime, data loss, or security breaches, which could result in significant expense or irreparable harm to the Organization, and that inappropriate or malicious action could result in disciplinary action, termination of employment, or civil or criminal charges, pursuant to Organization policies and relevant state, federal, or local law.

Appendix C: Important Credentials You MUST Have

As the owner of a business, the director of a non-profit, or in any other position where you are ultimately responsible for the operation of your organization, there are several critical, administrator-level, account credentials that you need to have available to you—even if you never use them. These are systems that are difficult or impossible to recover credentials for, which means you have to start from scratch if they are lost.

Best practices dictate that, for each system, you should have a separate account from your MSP. Avoiding shared accounts helps to maintain accountability and prevents situations where someone changes a password without informing the other party.

The following list may include items that are not applicable to your organization, or there may be other important systems, not listed here. These are guidelines that require some analysis to implement properly.

1. If your computer network utilizes an Active Directory domain for centralized authentication, you must have an account with **Domain Administrator** privileges. (If you utilize some other centralized authentication system, you should have an administrator account for that system.)
2. If you do not utilize Active Directory or Microsoft Entra ID, you should have an account on each computer with **local administrator** privileges. (This can get messy to maintain, and there are other ways to recover or create an admin account in an emergency scenario, so it's not entirely necessary.)
3. If your organization uses Microsoft 365, you must have an account with the **Global Administrator** role. Similarly, if you use Google Workplace, you should have an account in that system with **Super Admin** privileges.
4. You must have credentials for your **domain registrar** and **DNS host**. These are usually the same service, but don't necessarily have to be. This is a

situation where you might have to have a shared account with your MSP, as many domain registrars don't offer the ability to create more than one account.

5. You must have administrator credentials for your network infrastructure equipment such as **routers**, **switches**, and **wireless access points**.
6. If you use industry-specific software that is hosted on a server, you should have administrator-level credentials for this.
7. If you use cloud-based systems that require separate credentials for individual users, you need to have an administrator account for each of these.