Last Update: July 7, 2023

Hiring, Managing and Firing MSPs

Essential considerations in MSP relationships

By Ray Hutchins and Mitch Tanenbaum

AI Statement: This document was written by a human being ***and not AI***. While we may use AI for aspects of our research, we find that AI is (thus far) incapable of writing a document of this kind.

Table of Contents

Introduction

In the course of our cybersecurity and privacy practice, it has become apparent that many new clients don't have a clear understanding of the responsibilities of their Managed Service Providers (MSPs). This lack of understanding of responsibilities and requirements for these key IT resources translates into Service Level and other agreements between these service providers and the customers that are not accurate and do not serve the interests of the customers. This can be a fatal flaw which makes managing and/or terminating these relationships unnecessarily difficult. In the end, the MSP relationship, which should have been all about reducing risk…actually increases risk for the customer.

This research paper is intended to create a roadmap for creating sound and productive relationships with these key providers.

NOTE: You will see a common thread in our research papers–it is impossible to build a successful cybersecurity and privacy program without the FULL, COMMITTED support of top management. Therefore, while others in the organization may implement the following guidance, we urge top management to read and understand this document before committing to the process.

Preparation

With respect to MSPs, clients come to us with one of two problems:

- # 1: They have already engaged a MSP provider, but there are problems in the relationship that must be resolved.
- # 2: They need a new provider and have decided that they require assistance in the process.

Many times, the MSP is technically capable of managing the client's infrastructure, the problem is that they are not being led and managed correctly by the client.

So, let's deal with this issue.

Assemble the MSP management team.

The MSP is a critical vendor and thus your company's interaction with it should be at the highest levels.Management of this relationship cannot be shunted off to whomever has the most IT experience. Whoever has the most IT experience should definitely be on this team, but the risk to the company related to not correctly managing the MSP is such that the team should include folks who understand the current cybersecurity and privacy posture, contractual responsibilities, compliance requirements, and business needs. Senior leadership must be involved.

Remember, IT and security are business issues more than they are technical issues.

A team may be comprised of two people or five people. If you are a client of ours, we'll also be on your team. The people in your company who are most responsible for risk management and the *company valuation* should be on this team.

Establish Your MSP Requirements

This starts with a list of all the services that MSPs typically offer and then you select those services that you think you need. MSPs offer different services depending upon their experience, staffing, and core expertises. And sometimes their service offerings are targeted to one commercial product family, like Microsoft. In that case, as long as you operate your company with Microsoft resources, they have you covered. If you are doing things that are not in their wheelhouse, they may not be positioned to give you the most value.

This task is not a straight-forward as you may think. MSPs are a complex business and engaging a partner like us will reduce your brain damage and enhance the odds of your success greatly.

When you are done with the above, now you have your requirements list…or at least the first draft.

As part of the process above, you need to establish *exactly* what software, hardware and services you plan on having the MSP provide. For example, if your MSP is providing your Internet connection and something goes sideways with the relationship, you may no longer have any Internet service and it may take days, weeks or even months to replace.

There is a convenience factor of having a third party provide a variety of services from phones to software, but if you are not the "customer of record" with the original provider, those services can get shut down and potentially, you could lose all of your data.

Establish Correct Expectations of Costs

It's our experience that the core conflict between the MSP and the customer is that the customer expects more service for their money than the MSP thinks they were contracted to provide and hence, does not perform. This typically happens as a result of:

- Incorrect definition of customer requirements and needs
- Incorrect contract drafting
- Incorrect matching of customer needs with MSP capabilities
- Poor documentation of customer requirements and/or MSP responsibilities in the governing agreement
- Inconsistent/weak management of the MSP relationship by customer
- Inconsistent/weak reporting by MSP to customer
- Inconsistent/weak/incomplete communication between customer and MSP

Usually, the customer and the MSP have good intentions and goals. The problem was that weak processes were used during the vetting and management stages.

While there are other models (all inclusive, hourly, break-fix, retainer), most MSPs today use the Fixed/Base fee/ Plus Hourly model.

Fixed / Base Fee plus Hourly: In this pricing model, the MSP will likely include some proactive work in their fixed fee. Pricing for this fixed fee plan can vary greatly, but typically we see this base fee come in around $75 – $150 per user/per month. If you have 20 employees your base fee might be somewhere between $1,500 – 2,500 a month. The more users you have, the more this number can be reduced. Again, it is critical to define in writing what is and what is not included in this base fee.

Note that if you are paying less than $100 per user/per month, it is uneconomical for a MSP to invest anything substantial in the proactive services part of the package. And without significant preventative work, there will be increased demand from you for various *reactive* services which will likely increase your out-of-scope charges-and your shock factor when you open your invoice.

This can be a good model for you, but again in depth, detailed documentation is required. Paying someone like us a few hours to set up this type of arrangement and a couple hours a month to help you manage it greatly increases your chances of success.

Vetting Process

The first step is to send your MSP candidates a MSP Vetting Checklist and analyze the results. This is where someone like us is really important. A few hours consulting time with us can save you a lifetime of pain.

Building an Effective Agreement/SLA

Most businesses depend upon the MSP to provide the agreement that will govern the relationship between them and you. And most businesses have neither the knowledge nor the will to truly question this agreement. But, if there is a problem, this agreement will control the resolution of that problem.

As in all such business relationships, your greatest power is *before* you sign the agreement. Now is the time to establish your expectations and requirements.

The most important sections of the MSP agreement to focus on are:

- A very specific delineation of services and support to be provided. If the MSP offers a Base fee plus hourly model, then you need to know what SPECIFICALLY is included in the base fee and what is to be charged hourly. If there are different hourly rates for different services, this should be clearly articulated.
- Response and repair time requirements
- Support availability hours and contact info
- Pricing details
- Process for reporting problems
- Procedures for escalation if the problem is not satisfactorily resolved
- Issue remediation process
- Reporting procedures and frequency
- Contract termination procedures
- Contact information for routine services, cyber incident issues, billing issues, and reporting issues.
- “Ownership” of third party product licenses (ex: in whose name are your Microsoft Office licenses; if you leave the MSP do the licenses go away.)
- If the MSP is providing software licenses, how do you move those licenses to a new MSP when you change providers and is there a cost to doing that because of losing prepaid license fees that are not transferred. Do you understand what licenses the MSP has acquired on your behalf?

Management Process

Once you have an MSP selected, you need to manage that MSP forever. One problem that we often see is that companies think that once they have selected a service provider they can check the box and move onto important work. This is a mistake. It's important for top management to have confidence in the MSP management process before actually engaging this critical vendor. Here are the basics:

Establish responsibilities and processes

Your Risk Management Program should include written procedures for managing the MSP relationship. Who is responsible for this relationship, what are they responsible for managing, and who will they report to and with what frequency? Obviously the MSP relationship process should be mapped to the MSP agreement as described above.

Engage a vCISO

Odds are your company does not have a Chief Information Security Officer (CISO) and the great majority of companies do not need a full-time CISO. But virtually all companies need a part-time, virtual CISO. This is the ideal individual to help manage the MSP. We offer an excellent vCISO program and the best vCISO in the country for SMBs-Mitch Tanenbaum. Please check us out.

MONTHLY management meetings

The MSP is, in truth, the IT department for the organization or, in a co-managed environment, a significant player in the IT operation. It should be carefully and continuously monitored and managed. It is MANDATORY to have at least one monthly management meeting during which all aspects of the relationship and the MSP's activities are reviewed and discussed. If this meeting takes any less time than an hour, then it is not adequate. At each meeting, there should be an official meeting scribe who will collect all reports, document all activity and discussion and document task assignments on both sides of the agreement. There must be no hedging on this matter-it could save your butt in a crack.

Relationship documentation

This may run against the grain in your organization, but when it comes to MSP management…*if it isn't written down, then it does not exist.* If management does not fully support this philosophy, might as well go to the beach. If there is a cyber breach and your insurance company, lawyer, state attorney general, or any other regulatory bodies get involved, then the only thing that might save the company will be the strength of the documentation. Of course, that assumes everyone was doing their jobs in the first place. If there is one lesson you take from this research paper, then *documentation is it*.

Reporting to upper management and the board of directors

The top leaders of the company MUST know what is going on. If upper-level management reporting is not part of your organizational culture with respect to risk management and MSP management, then it falls to readers of this document to get that changed ASAP. Share this document and make your opinions known and document any such activity. Otherwise, your tush could be on the line if the proverbial excrement his the rotational air movement device. Here is an excellent piece we wrote on that very subject: ***When Management Fails: How the IT Folks Can Protect Their Jobs After a Breach.***

Co-Manage vs. You-Manage vs. They-Manage

There are basically three relationship management models possible with any MSP:

1. They manage everything and you are hands off
2. You manage most things and only call on them when needed
3. You and the MSP co-manage your IT

The downside of option 1 is that you can get locked out of your assets (data, network, cloud) because you don't have credentials to access the administrative interfaces. If something happens to the relationship with the MSP you are counting on them acting professionally (or alternatively, going to court).

You should decide (before entering into the relationship) exactly which of these options you are going to operate under and adjust your MSP agreement accordingly.

Remember, most people do not consider the divorce option prior to getting married (rich people do; that is why prenups were invented). Assuming you have nothing that you

care about (data, software, hardware, services), then not planning for a divorce is okay. However, that does not fit most organizations.

Terminating an MSP With Minimal Risk

Hope for the best. Plan for the worst

An MSP almost always has the keys to your kingdom. They may have passwords to many or all of your systems and they know the architecture and operating systems that make up your company's IT infrastructure. If the MSP ever becomes your adversary, then you could be exposed to serious risk. In fact, in many cases we have seen, you don't even have those passwords at all. On top of that, if the MSP wants to make a case, they even lock you out of your own systems.

Tips for reducing risk during termination and/or separation:

- Implementation of a strong vetting/hiring process in the first place
- Make sure that you have a professionally created service agreement/ contract that addresses the following:
    - Establishment of the chain-of-command
    - The MSP's written acceptance of responsibility for protecting company data and systems
    - The MSP's acknowledgement and acceptance of all company operational, cybersecurity, and privacy policies
    - Termination/separation procedures including the disengagement process with IT systems and data
    - The MSP's written acceptance of termination/separation procedures
    - Documentation/agreement regarding system credentials and system access by you
    - Documentation of all third party applications you will be using via the MSP. This is important because the license you are using in order to use (let's say) MS 365 is actually owned by the MSP. Things you need to know now:

        -What is the start date and the annual renewal date of all licenses
        -If it is necessary to dis-engage with the MSP, how is this handled via the various third party application licenses you are paying for?
        -Will you be given a credit for unused time?
        -Will the MSP let you out of that licensing agreement?
        -Is it possible to transfer the licenses from the old MSP to the new one?

  - Where are all backups stored? Who has access to the backups? Can you transfer the backups to the new MSP or to you? Can old backups be deleted?
  - Is the MSP providing any hardware? If yes, how is that transferred?
  - Is the MSP providing the Internet connection? Can that be transferred? Sometimes a new Internet connection to replace one owned by the old MSP can take weeks to months to get installed, depending on what is available. Plan for that.
  - Establish a process that guarantees minimal user disruption if a MSP change is required.
- Provide strong, on-going management that includes formal documentation of the MSP's workflows and activities.
- Perform quarterly, documented performance reviews
- If possible, segment company data and control who has access to what. Why would an MSP need access to employee non-public information? Or financial data? It is complex to create access control rules, but it is more expensive not to. It blows our minds how few companies think this through and/or do anything about this.
- Make sure executive management retains super admin rights to all systems and master passwords. THIS INCLUDES CLOUD SYSTEMS AND NETWORKS.
- Determine how much notice you have to give the old provider (MSP or other) of your intention to cancel or renew (for example, you might have to give them notice no earlier than 180 days prior to the expiration date and no later than 90 days prior to the expiration date). This includes hardware (like maybe firewalls and switches) but also software like (Office or Adobe Acrobat).

- What attestation will the old MSP give us that they have deleted all of our information and no longer have access to any of our systems, either in the cloud or on premise.

- Purchase cyber liability insurance that covers risks associated with the MSP (we review cyber liability insurance policies as part of our vCISO services).
- Listen to the MSP. Respect them and their work. It is much easier to separate on amicable terms if this is the case.
- Monitor network activity so you know what is going on. If your MSP does not provide this service, we sell very cost effective, easy to use tools which give you insights into what is going on. See our research paper written for executive management: ***Monitoring Your IT Systems-The Best Tools That Meet Compliance Requirements and Which are Affordable for SMEs*.**
- If you have an acrimonious separation situation, plan things carefully in advance and bring your attorney into the conversation early.

THE Most Important Piece of the Puzzle

As with all things risk management related, the only way to maximize your odds of success is to have ***committed*** management. If your management thinks of cyber, privacy and other risk management as a pain and something they do not want to talk about…and if your company has something real to protect…then you have problems. In today's IT centric environment, good risk management is foundational to higher company valuations, breach avoidance, incident response and business continuity. We helped establish this principle with the folks who create valuation standards-the NACVA. Please see our article HERE.

Want more info? Would you like to meet our lead vCISO? Please watch the video on this page: https://www.cybercecurity.com/virtual-ciso-services/

Or contact Mitch directly at:
Mitch Tanenbaum
720-891-1663
mitch@cybercecurity.com

Did you find this research paper of value? Here are some of our other research papers.

1. IT Infrastructure Monitoring Issues-Making the Best Choice for Your Company
2. Secrets of Hiring and Firing vCISOs
3. CMMC Compliance-The New Enclave Approach
4. The "NEW" CMMC 2.0 (AKA 800-171): Not the Right Way to Fix the DIB Security Crisis
5. When Management Fails: How the IT Folks Can Protect Their Jobs After a Breach
5. Monitoring Your IT Systems-The Best Tools That Meet Compliance Requirements and Which are Affordable for SMEs