THE MY MSP SUCKS PLAYBOOK

SEE THROUGH THE MSP LIES

We give away all the industry secrets MSPs don't want you to know so you don't get scammed (again)

WHAT TO LOOK FOR

How to pick the right provider for your company and what questions to ask to test their knowledge.

ON THE COVER

Frustrated, Pissed off, & Fed up With The MSP Bullshit

www.mymssucks.com

PROTECTED HARBOR

INTRODUCTION

If the thought of trusting your IT solutions to an MSP (Managed Service Provider) intimidates you or having to find a new MSP infuriates you, you're not alone. You may wonder what exactly an MSP can do for your business.

No two MSPs are the same, so this can be a messy answer. Most MSPs offer Break Fix IT, Software as a Service, Desktop as a Service, Managed Security Services, Managed Support Services, Managed Networks, and Infrastructure, Managed Cloud Infrastructure Service, and Datacenter Infrastructure Managed Services.

The better question is, which type of service is best for you? That depends on what you are looking for from an IT support company. MSPs help you avoid risk, reduce costs (and headaches), and leverage your resources by offloading IT tasks to IT professionals. But finding an MSP you can trust with this vital aspect of your corporation is not always easy.

HERE IS A QUICK OVERVIEW OF THE TYPES OF I.T. SERVICE PROVIDERS YOU COULD ENCOUNTER:

- **Break Fix IT-** Break/fix services are designed to address the issues; when you have a problem with your technology, you don't have to go without it for days or weeks. Instead, you can receive support to fix the issue as quickly as possible.
- **Software as a Service-** SaaS is a software delivery model that allows users to access data from any device with an internet connection and a web browser. Software providers host and manage the servers, databases, and code that make up an application under this web-based approach.
- **Desktop as a Service-** Desktop as a Service (DaaS) is a cloud computing service in which a service provider delivers end users with virtual desktops via the Internet, which are licensed per-user basis.
- **Managed Security Services-** Managed third-party companies provide security services to oversee and administer a company's security operations. Managed security service providers (MSSPs) deliver services in-house or remotely, most commonly through the cloud.
- **Managed Support Services-** Managed Support Services is the practice of outsourcing the responsibility for sustaining and anticipating the need for various processes and services, ostensibly to improve, support, and minimize budgetary expenditures by reducing directly-employed people.

- **Managed Networks and Infrastructure-** The monitoring and maintenance of a company's network technology is part of managed networks and infrastructure. You can either employ a network management provider or establish an in-house network management team.
- **Managed Cloud Infrastructure Service-** This could include migration, maintenance, and optimization of a client's cloud platform and partial or complete management and control. A provider may ensure that its cloud resources work well by utilizing a managed cloud service provider.
- **Datacenter Infrastructure Managed Services-** DCIM (Data Center Infrastructure Management Services) is the result of combining Data Center Operations and IT to achieve optimal data center performance.

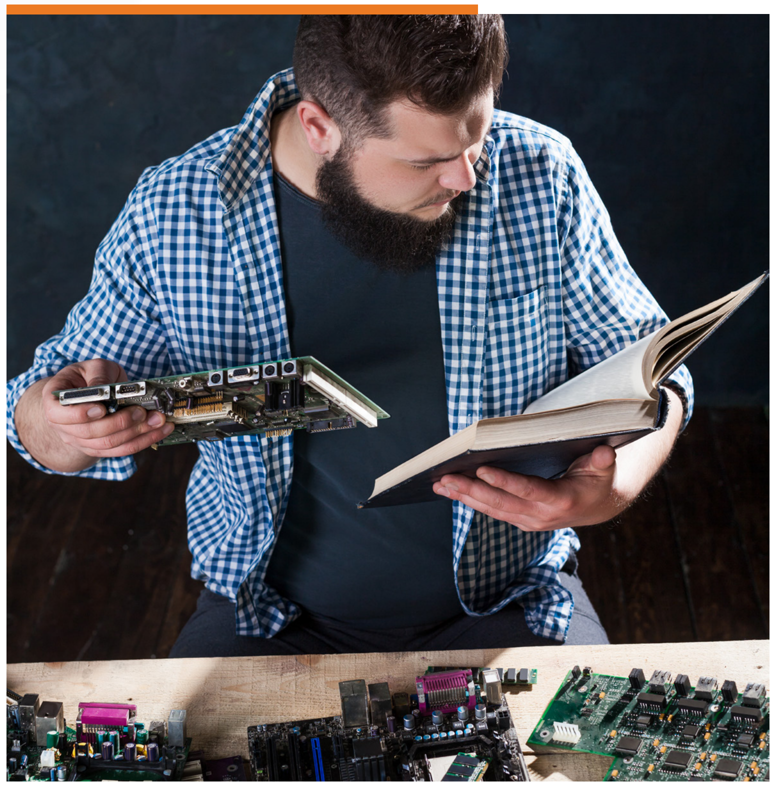
MSPS EXPOSED:

HERE'S HOW YOU CAN STOP GETTING PLAYED

If you've recently tried exploring new IT service providers, there's a fair chance you've been misled. Today, we're calling b.s. on these lies so you can steer clear of these unethical practices and make fully informed decisions.

Many MSPs have shifted their focus from technology to sales, becoming Managed Sales Providers. Instead of spending their weekly meetings talking about improving their service, downtime, and SLAs, they're reselling a series of disconnected third-party services or, even worse, outsourcing the service you are looking for. Sales have their place, but many have lost sight of the services they were created to perform and have become product experts instead of tech experts. Ultimately, this causes their security to suck and leaves your business and your customers at risk.

The saying goes, "you don't know what you don't know." Have you ever wondered what you don't know about MSPs and what those gaps may cost you in the long run? We're pulling back the curtain, exposing it here and now!



EXPOSED: They claim to be "experts" who can provide any solution you need, which is not true. If you've been told their tech is so sweet it can solve your problems—without even asking what challenges you're facing—run, run fast!

- **What it looks like:** When you ask about remote access for your employees working from home, the MSP you're considering says with confidence, "Oh yes, we can take care of that with a VPN or a remote access package."
- **The truth is**, they only know how to offer remote access with one product, or worse assume they can "figure out" how to install, configure, or troubleshoot the system. They are blindly moving clients to remote access without planning for equipment failure and data security, creating problems in the future.
- **The solution:** Don't take "yes" for an answer. It's ok to ask for specific instances and examples of when and how an MSP has done what you need to demonstrate that they can do the job. They should also be able to highlight the pros and cons of each solution to help you make an educated decision. Sometimes the best answer is an honest "I'm not sure if we can do that; let me find out and get back to you."

EXPOSED: Hiring an MSP will NOT make all your IT worries disappear. (In fact, they sometimes lower your level of security by reselling services to you.)

- **What it looks like:** Your service provider may offer cloud storage. Sadly, some MSPs just resell the storage they purchased from another cloud service.
- **The truth is**, deploying a cloud storage system without taking backup, revisions, and security into account will expose your company to repeated attacks and data loss. Also, cloud storage providers charge when the data you are storing is modified or accessed, which means you are more likely to receive surprising high bills you didn't expect.
- **The solution:** Find an MSP that is clear on what they provide and can give you an answer that frees up your team to focus on their functions. Your employees should find the company's tech helpful, not distracting. Considering a mid-level or higher MSP can help you ensure they can give you what you need today and in the future. An MSP who understands how a company works and offers the client several approaches without creating new security issues or new costs.

EXPOSED: The cookie-cutter package presented to you is not a one-size-fits-all solution and will not meet all of your business's unique needs.

- **What it looks like:** You get a quote from an MSP, and it seems like all features are included, but you'll find out later there are surprise costs and missing parts.
- **The truth is** since MSPs are now reselling cloud packages, they do not disclose or understand the impact of cloud service limitations, often resulting in unexpected costs or operations problems.
- **The solution:** Starting with a clear idea of what you do will save you lots of grief and money. Some service providers have all-encompassing suites, and others offer solutions a la carte. Asking what is not covered by your agreement early is the best way to protect yourself from hidden fees and unplanned expenses later.

EXPOSED: Your MSP may be "monitoring" your system, but you may not realize that they simply k a server or service is up or not. They are not monitoring for vulnerabilities and operational priorities.

- **What it looks like:** An MSP who is always reactive, only responding after a failure. This means downtime for your business.
- **The truth is**, MSPs of today do not understand how to take apart an organization and look for the key components. Instead of mitigating a failure, they wait for it occurs.
- **The Solution:** Look for an MSP who creates customized response plans and then backs those plans up with a guarantee that downtimes are reduced.

EXPOSED: Their "24/7/365" support might be a third party that the MSP has outsourced.

- **What it looks like:** It's 4 pm on Friday, and one of your employees is putting the final touches on a proposal for a big fish client, and it's down to the wire. A file in your cloud storage needs to be used, but everyone gets an error message. You try a few ways of your own to get into the cloud and find that you have no access and no idea why.

  You call your MSP and get a bottom-level tech who can't fix your issue, so he files a ticket and tells you someone will look at it on Monday. You dig through your contacts and send your account manager an urgent—rather scathing—message in hopes he's working late and can pull some strings.

  Now what? You managed to find an older version of the file stored locally, but it will take a lot more work to finish this proposal now. You do not feel supported.
- **The truth is** that provider has not only outsourced their after-hours support, but they also do not have escalated support around the clock, so problems cannot be resolved promptly.
- **The solution:** Let's face it. There's never a good time to have tech issues. Even if your office isn't supposed to be open on weekends, you should know what support you have available and when. Get answers in advance. Ask your MSP for their closure and escalation rate. What is the rate quoted in their contract?

SIGNS IT MAY BE TIME TO FIND A NEW PROVIDER:

- It seems every week there's a new IT-related issue in your office.
- Technology is slowing your team down instead of helping them work more effectively.
- You often feel like your IT company should be doing more, and frankly, you often wonder what they do for your business.
- You lose sleep at night wondering how secure your network is.
- Problems are not being solved. You are having the same issues over-and-over, again.
- When you reach out, the tech support specialist does not know your company or systems.
- It feels like there is always an extra cost.
- You have plans to grow in the future, and you're not sure if or how your current MSP can support that transition.

You want to feel like you're getting what you need, being heard, and getting sound recommendations from your service provider. It's NOT too much to ask.

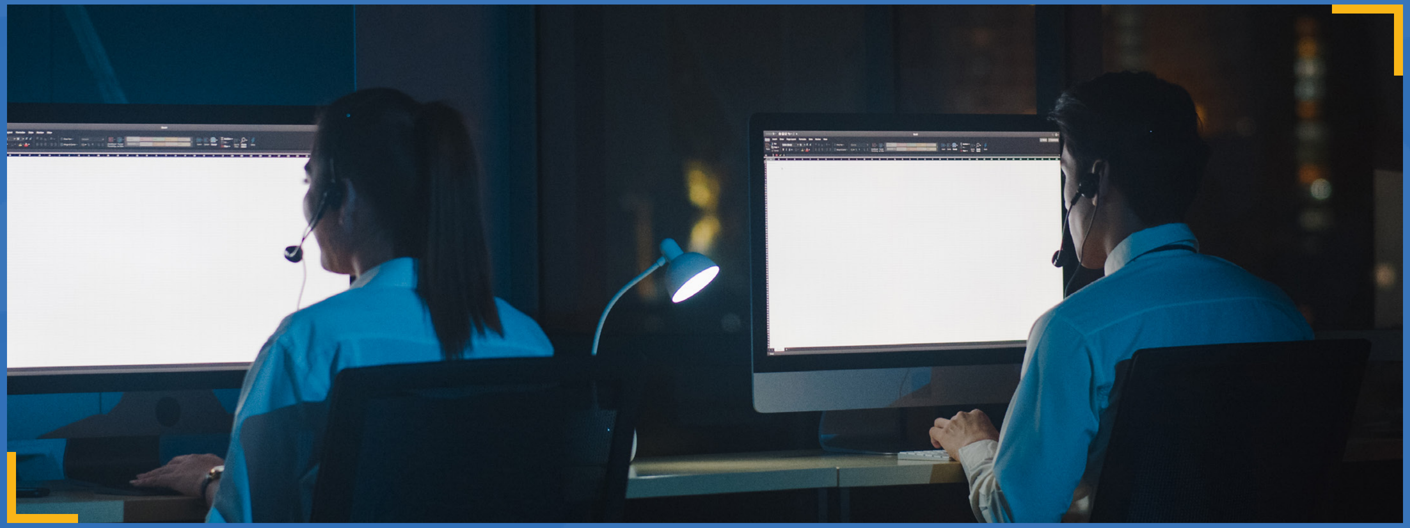
Working with the right MSP allows you to stay at the front of technology, reduce your costs, and offload tasks to professionals who know what they're doing. If you're not getting this from your provider, it's time to find a better solution.

SO HOW DO YOU PICK THE RIGHT MSP?

Finding the right MSP starts with knowing who to talk to. Different MSPs target different markets, so what works for one company may not work for yours. Consider your business's needs, which levels best fit your current operation, and where you're growing.

Below is a list of MSP types and some typical characteristics:

Basic MSP, primary focus on startups and small businesses.	Provides basic technical support, typically on laptops and desktops. Little to no experience with complex deployments, servers, or database applications. Charges on a per desktop or per device basis. Typically charges per hour or under a block of hours system. Support is provided by remote access to laptops or desktops. All support requires user initiation; MSPs can't provide automated support. They typically take no responsibility for your business concerns or IT planning; monitoring is basic, and updates are additional. Little to no future planning.
Reseller MSP uses a series of cloud-based to provide support.	Resells and has become a representative of cloud-based products. They typically make more money from reselling products than from customer payments. Has reduced their technical staff in favor of additional sales staff. Some MSPs have taken this approach to the extreme, to the point of outsourcing the actual support. This MSP has virtually no internal team, resulting in longer customer support calls and low client satisfaction. Projects are often delayed or never complete because there is simply no one internal to the MSP who can make all of the products they resell work together. Support often doesn't include an on-premise license; on-premise is additional or unavailable. This MSP will have a meager internal technician-to-sale person offering.



Full-Service MSP	This type of MSP is still focused on customer value by understanding the client and is staffed correctly to provide good support. This type of MSP may represent a few cloud-based applications, typically those that clients request, which is the most significant difference between Full-Service and a Reseller MSP. Typically offers inclusive support and service packages, including backup, detailed monitoring, remote access, etc. This type of MSP will have a high tech-to salesperson ratio.
Enterprise / Data Center MSP	This service provider focuses on larger corporate deployments involving large virtual server deployments. Typical deployments will be 300+ servers. The more skilled MSPs work to understand their clients and augment the clients with MSP executed routines, updating client profiles, for example, or performing database maintenance. This service provider focuses on larger accounts, understands the power of scripting, and can be faster at creating and deploying custom-made solutions that perform maintenance, data exchange, etc. These service providers are typically the more expensive, but they can be of significant value for a more extensive account with specialized applications. This type of MSP will have a high technician to salesperson ratio and additional staff experts, such as a database administrator.

WHAT TO LOOK FOR IN AN MSP

You've found a couple of MSPs and are ready to meet with them! Use the list below to ensure you ask the right questions and get the best answers. It may take a few tries before you find a company that meets your needs, but the payoff will be well worth the effort!

What is the average time they notify you of a low-priority alarm?

Ask your MSP if they will include an average response time guarantee in their contract. The average initial response time for non-critical responses should be 15 minutes or less. Mission-critical issues like ransomware attacks or failed disks should be responded to in under 5 minutes.

How long is the onboarding process?

This will vary depending on how much rebuild is required. It may be only a few hours to several weeks, but it is essential to know how long it will take so you can understand the process. A good MSP will build an onboard plan – ask to review it before the process starts.

Do they outsource their support?

An MSP that outsources their helpdesk means the client will rarely get a technician who knows their system, and rarely will the client speak to the same technician more than once. Each support call is longer than is needed and often needs to be repeated. The best answer is that all of the support staff are direct employees, not outsourced or contracted workers.

Technical Staff to Sales Staff Ratio?

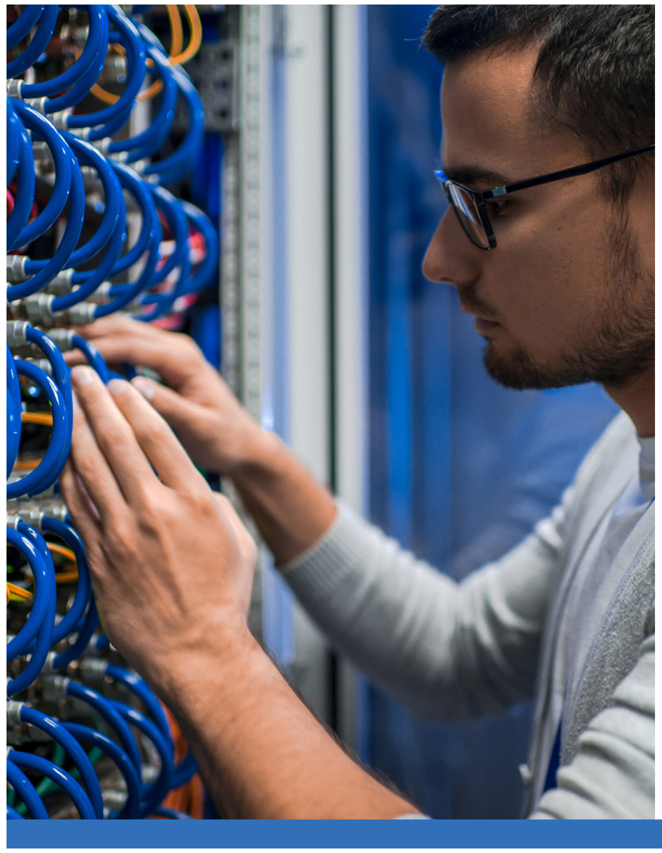
A Good MSP will have a high technical staff to sales staff ratio, at least 4:1. Anything less means the MSP is focused on reselling products and not on solving client problems. Ask if the staff included in the count are contacted, workers, or direct employees.

What is included in the support packages?

Ask specifically what are the limitations of the support packages. Is licensing included in the packages? What about backups? If so, it is isolated from the production network, and what are the limits? A good MSP should include some monitoring and backup; the backup should be a minimum of 7 days.

How will they help prepare for future needs?

Your MSP should understand where your technology is today and where you want it to take you. For example, you may need to plan for infrastructure changes and storage increases. With customer growth comes the need for heightened security; make sure your provider is committed to monitoring. Partnering with an expert will ensure your company's future success and safety.



How will they help reduce IT costs?

A good MSP will review your current IT expenses and document the duplicate expenses and, if so, how much can be saved. Your IT support costs should be more like insurance payments than bleeding repair costs. Get a flat-rate plan that ensures you are protected in the event of an issue.

Does the company have experience within your industry?

A provider with experience in your industry is helpful, but very few MSPs are single-focused businesses. This means the best MSPs service a broad and diverse background of clients.

Do the technicians have experience supporting your company's software?

Many MSPs have shifted their focus to selling new products and services and not on understanding your needs. Your MSP should know your applications (or learn them). How could they support software they do not know?

How fast can an expert provide service when you need it?

Not all questions are the same, and neither are all technicians. Some situations need an immediate response; other times, a delay may be acceptable. A good MSP will get to know your needs and be able to provide the support that suits your business while keeping costs low.

Is outbound traffic monitored, and if so, what is observed?

All outbound traffic should be monitored, and unexpected or unusual traffic patterns should cause an alert. Ransomware attacks typically start with a downloaded agent contacting the attacker for instructions. Those connections should trigger a warning and immediate action from the MSP.

How do they protect data from unauthorized access?

You are looking for a cloud vendor or MSP that will enable instruction detection, event log monitoring, and geo-blocking to build a flexible inbound shield. The MSP must have a plan to protect from overseas destructive actor attacks.

What is the MSP's standard actionable incident response plan?

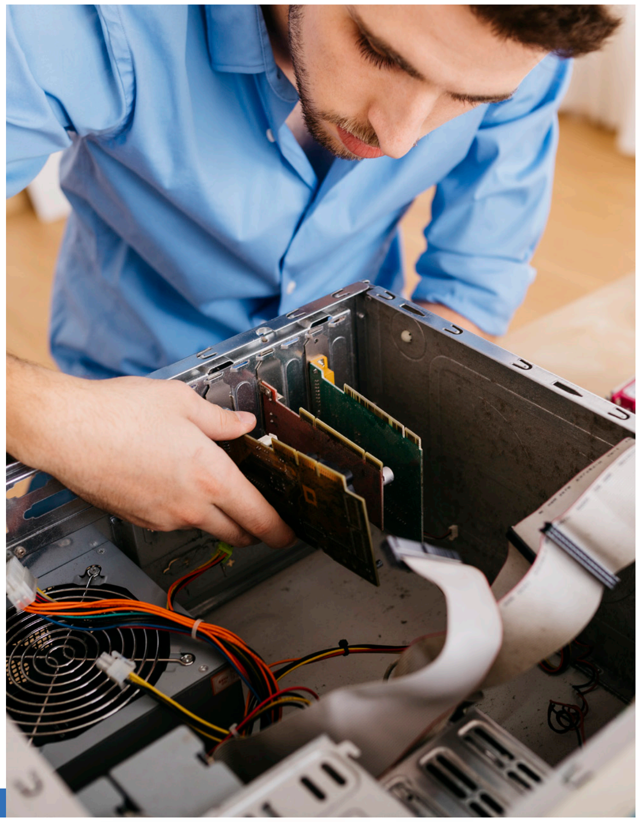
Ask for an example plan that they use to support other similar clients. They should have a good, flexible response plan custom-designed for you.

Do they conduct automated security scans?

There should be a constantly running filter and scan on all inbound and outbound traffic and a detailed hidden trojan scan to be used as needed.

What is their disaster recovery plan?

You need to know exactly what to do if and when things go awry. The plan may be as simple as booting up a different machine or from a different location. It is essential that your MSP blend response and application support provide immediate application and desktop access from anywhere.



WHAT IT LOOKS LIKE WHEN YOUR MSP IS A GREAT FIT

Esbin & Feinmesser, PLLC is a boutique law firm that prides itself on offering legal and advisory services that match those of large corporate firms while crafting a more personal experience for its clients.

Being in practice for over 20 years, they have a lot to protect. Partner Scott Esbin explains, "is a law firm, we're just inherently conservative about putting our data and files in somebody else's hands. There's a whole host of rules that we have to abide by in terms of client confidence and security.

Law firms can be brought down ultimately, and lawyers could theoretically be sanctioned if they're not careful about how they treat their data."

With all the news in 2019 of the cyber-attacks on corporate giants like Facebook and Citibank, his firm's security was heavily on his mind. Esbin knew that they would likely close the business when client confidence was lost. He would have to have many very tough conversations with clients and employees.

Challenges

Despite the trend at the time toward cloud-based storage, Esbin wasn't convinced it was the proper course for his firm. He found an IT provider he thought could help.

The vendor seemed like a good fit for Esbin & Feinmesser initially, but things began to shift over time. There was no cohesive, intentionally-developed plan to achieve the organization's goals and satisfy its security needs. The proposed solutions were often a quick-fix of new software with more equipment.

Esbin & Feinmesser housed their data in the office to circumvent Esbin's fears about cloud technology. They had more machines in the office than employees. There was way too much volume with no design, so it was not enough to keep the business safe—and those choices cost Esbin dearly.

"We had to pay for our licenses. We had to pay for people to come in. We had to pay for hardware when a computer would bust. It was expensive. I would have spent $50,000 - $100,000 more on computers and, licensing, other costs." Esbin recalls.

Then in 2020, what Esbin had always feared happened.

"We got hacked," Esbin shared. "We couldn't access email. We couldn't access our servers. It was like somebody came in and put a giant padlock on all of our stuff. We still, to this day, don't know exactly how it happened. We think it was a bad attachment somebody opened."

Esbin immediately knew he needed a new IT provider that could help him regain access to his business. Still, more than anything, he needed better protection so this could not happen again. Keeping the servers in his office did not prevent intruders, but he still had doubts about cloud-based storage.

Protected Harbor sat down with Esbin and listened to his concerns. He worried if his data was safer sitting next to him in the office or the cloud. How could the firm stay safe? How can he make sure this doesn't happen again? How could he keep an employee from making a mistake that may take down the company?

Solutions

Protected Harbor calmed these fears quickly by explaining how the process would work, why cloud-based storage was safer, and how they would protect him from future attacks with monitoring and redundancies. Then they worked as a team to put the pieces of Esbin & Feinmesser back together.

Nick Solimando, Director of Technology at Protected Harbor, said he believes "ransomware hit the servers in our client's office. It got down to cryptic system files to the point where servers wouldn't even function properly and wouldn't boot up properly. None of their file shares were functional."

Fortunately, none of their data was leaked, and some of the data were not infected so severely that Protected Harbor could look at those files. The equipment, on the other hand now essentially scrapped metal.

Solimando illustrated Esbin & Feinmesser's new security measures saying, "Our goal is to put clients in a protective bubble. We don't want you to worry about the IT—so you can focus on your business."

Protected Harbor always starts with an audit of the client's current system and what their needs are. But this migration was unique because Esbin came with only pieces of data, and the plans were down. So Protected Harbor analyzed the entire picture to see what was salvageable and asked Esbin what functions were most important for recovery.

"We have a lot of unique programs that we use that are proprietary," Esbin immediately answered. "They're unique to us; we own them. If I don't have them, I don't operate."

In the end, Protected Harbor worked with Esbin's programmers to reconnect and successfully integrate the custom application. Then they managed to retrieve a suitable backup file about two months old, but it was valid and able to be restored. So out of roughly ten years' worth of data, in the end, Esbin was only missing a fraction of data, but their system was restored, and they could continue operating.

Protected Harbor even worked with end-users to recreate their environments so that their files and access were back to normal after less than a month.

As Esbin & Feinmesser's systems returned online, they needed to be fully protected. "We put them in a virtual environment in our data center and gave him his dedicated virtual network. So it's just him in there, nothing else. He's segregated and isolated." Solimando elaborated. Malware scanning and monitoring are a part of Protected Harbor's default environment.

The monitoring services are comprehensive and prevent threats instead of reacting to them. Esbin now benefits from constant monitoring for things like RAM, CPU, and disk space to ensure everything is performing as it should. If it's lagging, Protected Harbor is already looking into it and resolving the issue before the end-user is impacted.

Known malicious IP addresses, attack vectors, and even whole countries are blocked out, not allowing anything to penetrate the network. Redundant internet, firewalls, switches, virtualization nodes, backup architecture, and mechanisms help prevent errors and maximize uptime. If there is an issue, the backup files are completely inaccessible from where the admin users are.

"Most likely, the ransomware they got hit with before would never even reach the server today," Solimando assures. "It would get stopped by one of the protections upstream from them. If it got through all of that, we would be able to recover them inside of a day, probably less than 12 hours."

Results

Today Esbin is grateful that the hack happened when and how it did. He quotes, "'Fear is the mind-killer.' It's a line from a movie called Dune, but I think that's probably the biggest lesson I've learned from this.

I think that we were lucky that we got hacked. It's true because having what we have now works better than anything we've had in the past."

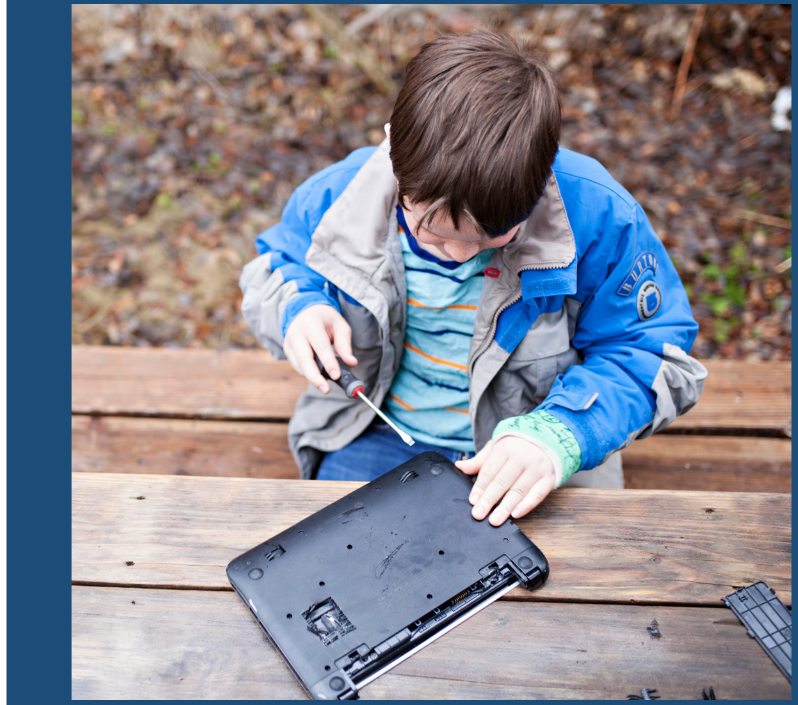
The lesson cost was high, but Esbin recognizes that the infiltration they experienced could have been much worse. Fortunately, none of his client data was taken or accessed. It was locked away, so they could not access it without Protected Harbor's services.

Esbin has a new confidence level as he knows his business is adequately protected. He has the support he needs, and when his company grows or changes, Protected Harbor will design a solution for him based on his individual needs.

There's always someone to answer Esbin's calls, even for help with the simple things that cause significant problems, like figuring out how to print on both sides of the page. He's received all the personal service and hands-on assistance he needs.

The cost savings with Protected Harbor is also significant. Esbin was pleased that while he's reduced his IT costs by roughly 50%, he has gained security, expert assistance when needed, and more peace of mind.

Highlighted Quote somewhere in the above section: "We've slashed our technology budget by half, sending it back to the employees. We've redeployed those funds to things like healthcare, salaries, and bonuses for the staff." - Scott Esbin, Partner at Esbin & Feinmesser, PLLC



IF YOU ARE UNSURE OF YOUR MSP, WE WILL AUDIT AND DISCOVER YOUR POTENTIAL AREAS OF IMPROVEMENT.

We start every engagement with a discovery process to identify your business goals, risk areas, and technological priorities. We then create a strategic plan that is mapped to your business goals and provide ongoing monitoring and measurement to track the success of our solution. Protected Harbor's team of engineers, consultants, and certified technicians work with you to implement the best-fit technology to meet your organizational goals. You benefit from working with one trusted partner who understands your unique organizational goals.

Protected Harbor manages your IT infrastructure from soup to nuts. We've covered you from email to teleconferencing, website hosting, cloud storage, computer repair, etc. We stay on top of your technological demands daily, keeping the lights on and providing strategic guidance to higher-ups.

We offer customized IT solutions to businesses looking to scale their technology, and we're on a mission to give you the best customer service possible. We are constantly innovating to ensure you have the best experience with our products. As one of our customers, you can expect excellent service, quick response times, and an eager team to help. We are not your average MSP. We are engineers, software developers, analysts, designers, and lifelong learners. We offer a tailored approach to managed services designed to meet each client's unique needs.

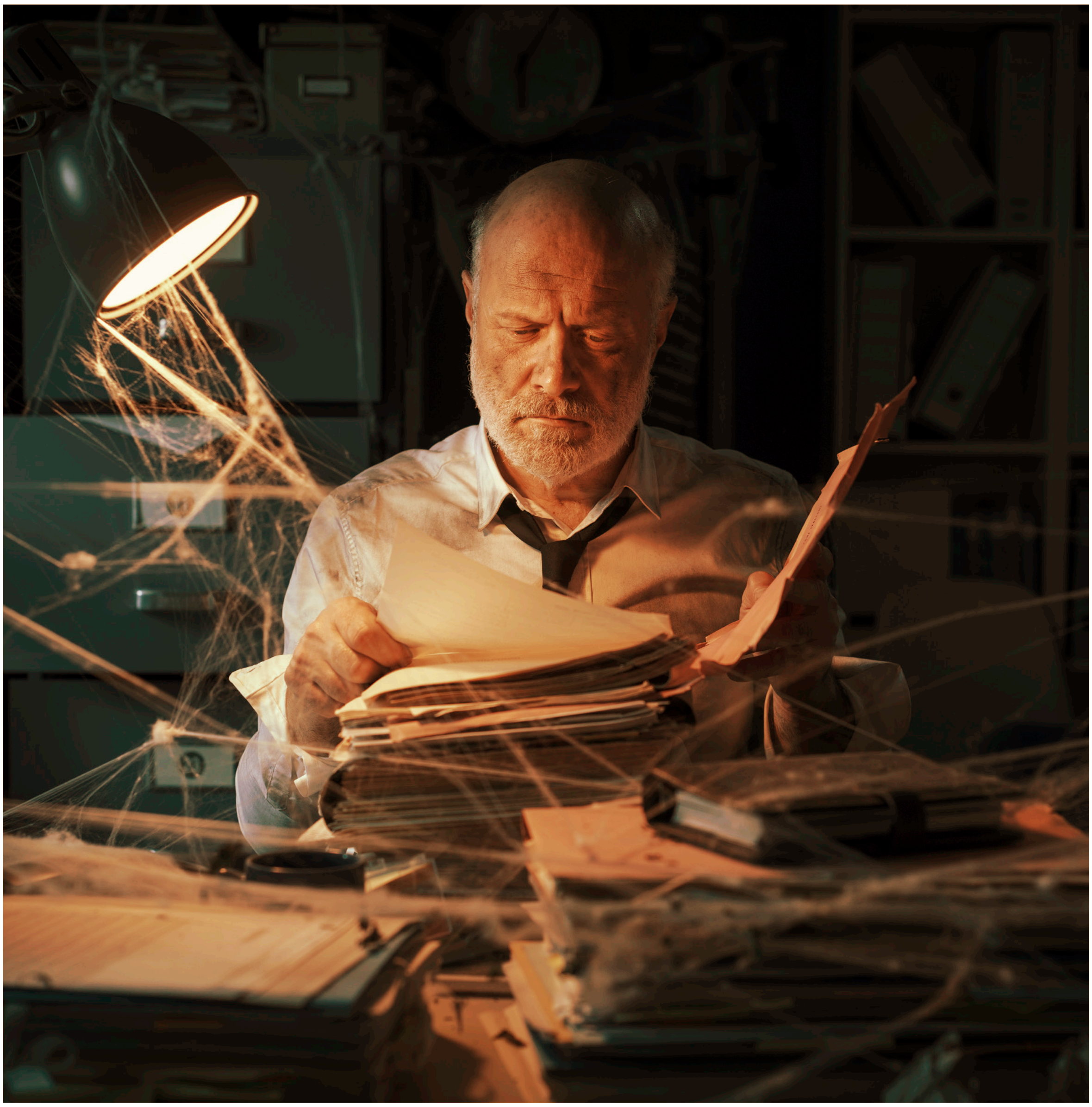
ABOUT PROTECTED HARBOR

We are a trusted IT management and technology durability partner for companies across the US. We take responsibility for the technology and applications that keep your business moving forward.

With over 15 years of service and a 99.99% uptime record, our team is fully committed to creating, maintaining, and managing the highest quality application operations environment experiences. Your uptime is our focus. Our 90+ Net Promoter Score and 95% client retention rate back up our claim of being a go-to provider for companies looking to improve their technology.

Protected Harbor provides a range of I.T. support, infrastructure management, and application durability support for businesses looking to scale their technology. We are the IT vendor of choice for companies looking to get the most out of their technology at the lowest possible cost, regardless of location and cloud provider. From infrastructure design to cloud migration, including security, storage, connectivity, remediation, monitoring, etc. Protected Harbor offers a full range of data center solutions backed by our 24/7/365 support team dedicated to exceptional customer service.

www.protectedharbor.com



PROTECTED HARBOR