

The Managed Service Provider— An Invaluable Ally in the Quest to Improve Your Organization’s IT Resilience

Today more than ever, companies need to make smart investments in technologies and processes that prevent security breach events and reduce the impact of planned and unplanned downtime. But these investments alone aren’t the answer to IT vulnerabilities. The weakest link in the IT-resiliency chain is often the skills of IT staff and the increasing demands on their time. With the pressure to trim budgets, IT professionals are increasingly spread thin and often don’t have the time to develop expertise in various resilience technologies, let alone afford the time to consistently perform the monitoring and auditing required to optimize each area of the IT resilience stack. That’s where a managed service provider (MSP) becomes a truly valuable ally in an organization’s overall resilience strategy.



MSPs are experts whose sole mission is to provide the highest levels of expertise and oversight for the technologies and processes they are charged to manage. By taking bottom-line responsibility for the smooth functioning of the technologies under their charge, an MSP is able to free your IT staff to focus on more important projects. With the expertise and attention of an MSP as part of your resilience infrastructure, you significantly reduce the chances your organization will face an IT outage or a security issue that negatively impacts your business.

Let’s look closer at what managed service providers do and how best to engage them, particularly in regard to reinforcing your organization’s IT resiliency assets.

MSPs Differ from Traditional Outsourced IT Services

Managed services are an alternative to the “break/fix” or “on-demand” models of IT outsourcing. These traditional models of outsourced IT services typically involve contracting with a company to resolve issues as they arise; in other words, when something breaks, the service provider stands ready to fix it.

By contrast, MSPs offer an ongoing engagement to take bottom-line responsibility for the optimal performance of a designated element of hardware or software. This usually includes 24-hour monitoring, updates/patch management, stress testing, and problem resolution. This represents a significant change in philosophy regarding how a company outsources technology services, which is why a growing number of IT departments are moving to the MSP model.

With an MSP relationship, the focus on outsourced IT services shifts from being reactive to proactive. This means that the MSP typically sets up all necessary monitoring functions to see the state of the technology it's contracted to manage and receive real-time alerts should something not function as it should. Moreover, the MSP is responsible to make sure regular maintenance is performed on the technologies under its charge, including implementing updates and patches in a timely way. This last piece is critical because the odds increase of facing some kind of an outage or other critical issue when organizations fall behind in keeping up with needed maintenance. And proactive maintenance not only adds another protective layer to your infrastructure but also ensures you benefit from the latest features and functions.

All of this means MSPs typically cost less than traditional “break/fix” services, especially when you take into account the cost of disruptions caused by systems not functioning, staff not being able to do their jobs, frustrated customers, lost business opportunities, etc.

When to Consider Engaging an MSP

As you go through the process of looking at whether there is value in bringing on an MSP, it's critical is that you first do an honest assessment of your IT operations in the following areas:

IT Challenges

If the difficult or otherwise challenging initiatives within your IT department are utilizing more than their fair share of IT staff hours, it makes sense to consider bringing in outside experts to help resolve these challenges and then keeping these areas of IT well-managed so staff can focus on other priorities. Security and corporate compliance is a good example of this. Given the critical, ever-changing nature of these areas, having experts in place who are up to date on threats and who consistently monitor for and mitigate vulnerabilities can make all the difference. Smaller IT shops often struggle with devoting the needed personnel and expertise to this area. Bringing in an MSP with proven capabilities is often more effective and cost-saving than investing in additional training or adding new headcount to meet and sustain compliance.

Strategic Impact

When strategic IT initiatives are not moving forward at the pace they should, utilizing an MSP to cover non-strategic infrastructure aspects of IT—and thus moving more internal IT staff to these strategic initiatives—can have a very real, positive effect on the bottom line. In fact, when CFOs put a pencil to the increased revenue or reduced operating costs that would result from adding more internal resources to the implementation of a particularly high-value or urgent initiative, they often find the cost of an MSP to be a no-brainer.

Another benefit that companies often don't consider when utilizing an MSP to free up existing IT staff for strategic projects is it gives IT staff members who would otherwise be working on mundane areas of IT the opportunity to contribute to more-visible IT initiatives. By doing so, these folks gain increased self-confidence and find new opportunities to shine while the company benefits from their increase in productivity and loyalty to the organization. It's a win-win for all parties.

Workforce Vulnerabilities

IT departments at smaller organizations often include one or two people who possess all of the institutional knowledge about a company's most sensitive systems, which presents a real vulnerability when one of these people leaves. This is particularly true with IBM i shops, where many of the most talented, experienced people are nearing retirement age and there isn't a large number of people available in the marketplace with similar skills and experience levels. IT leadership can gain significant peace of mind by knowing it's possible to outsource critical functions to an MSP partner that delivers the consistency and expertise these important IT operations require until replacement staff can be found and brought up to speed.

Specialized IT Skills and Frequency of Use

It's wise to look carefully at the IT skills you have in-house and consider how often these skills are used. Some technologies demand a high level of skill, yet those skills are used infrequently, which makes for a prime opportunity to consider an MSP relationship. An old Norwegian proverb says, "Experience is the best teacher, but the tuition is high." Becoming a highly skilled IT professional takes time, and no one can avoid the mistakes that come with gaining experience. And if an employee, even a highly skilled one, isn't called upon frequently for a difficult or otherwise critical task, skill degradation can result. It happens to the best of us.

To illustrate, a recent survey of IT executives conducted by Vision Solutions revealed that nearly half of all IT departments had experienced an IT migration failure at some point, and of those that did, 17% blamed the failure on their staff's lack of skills to properly manage the migration process.

Then there is the procrastination factor around tasks that don't necessarily need to be performed with regularity. For instance, it's not uncommon to have software that largely runs without intervention after it's installed yet does require some regular checking of logs, etc., and it may even require occasional testing of key functions to verify readiness for possible events. In time-strapped IT departments, there's a greater risk of these essential tasks being put off, which can create big problems down the road. High availability software is a prime example of this as there is great benefit in consistently performing monitoring, fine-tuning, and testing to ensure the system is optimized and ready for a successful switchover should a planned or unplanned downtime event occur. Unfortunately, this fine-tuning and testing tends to be put off when other IT urgencies arise, which can often result in a number of unexpected surprises should an issue occur that requires a quick switchover.

Selecting the Right MSP

Once you have considered the areas of IT that make the most sense to outsource to an MSP, the job then becomes finding and evaluating potential vendors. It's no surprise there are various kinds of MSPs you can engage for IT projects, and they range from VARs/system integrators to large IT consulting groups to the software and hardware vendors that created the technologies whose management you are looking to outsource.

Experience and Resources

Each type of MSP has its place, depending on the type of expertise and range of services you need, but regardless of who you choose, you must be assured the vendor brings the knowledge, experience, and service levels your organization requires. And always consider the breadth of services and resources an MSP can provide. Smaller MSPs might be more agile and cost less, but their smaller staff and limited technical resources (e.g., bandwidth, IT redundancy, data center agility, etc.) could become an issue if they get stretched thin or suffer their own IT issues. Of course, be sure to verify an MSP's track record by speaking to its customers. If the MSP is providing resources in their or another entity's data center, verify that those resources are sufficient and the proper redundancies are in place. If the MSP partners with another entity to provide certain portions of its services, be sure to review the reputation of that partner and its relationship to the MSP. Finally, see what industry certifications the MSP has, and verify it follows all necessary industry guidelines and principles.

Cost

Certainly you want to be sure you get a good value, but don't negotiate solely around cost. If you fixate on driving cost down, you might not end up with the MSP that is best for what you need. Seek the sweet spot where capabilities and breadth of coverage meet cost efficiency.

Regarding cost, there's one side benefit worth mentioning that's likely to appeal to your CFO: Engaging an MSP means the cost for managing a designated technology becomes a fixed, rather than a variable, monthly expense, which can have significant benefits from a budgeting perspective.

The Case for Application Managed Services

The term Application Managed Services corresponds to an MSP engagement that's provided by the ISV who created the software you want managed. There are distinct benefits of application MSPs over other vendors of managed services:

Highest Level of Application Expertise

Nobody can be an expert at everything. Application providers, on the other hand, focus entirely on their own offerings, which brings the highest level of knowledge to their technology. In addition, application providers are also the most knowledgeable about best practices when it comes to use of their software, and they often proactively work with customers to implement these best practices within their organizations, all of which results in a greater return on the MSP investment.

Hands-Off Maintenance

Every application requires some level of system maintenance or updates, and these usually require a manual verification that nothing went askew, all of which can be time- and resource-intensive. Application providers are always the ones best equipped to handle maintenance and verifications. And by having technology updated regularly, your organization more quickly benefits from the latest features of the software, thus increasing the value you get from the software.

Peace of Mind

Again, the expertise and regular maintenance provided by application providers gives IT departments the highest level of assurance that critical tasks are handled correctly, which in turn puts the minds of executives and IT staff at ease so they can focus on other priorities.

Application Managed Services as a Piece of a Broader MSP Offering

For many companies, there are advantages to engaging an MSP that provides a broad range of services, and in these cases, Application Managed Services can be a component of the broader MSP offering. For instance, an MSP might be brought in to provide services that cover a wide swath of a company's IT security and compliance needs, and as part of that broader service, there are distinct advantages in engaging the ISV of a particularly critical piece of security software to provide managed services around that. Larger MSPs are often happy to work in lockstep with the application provider to ensure the services are coordinated and can even provide oversight of the application provider's services.

Keys to a Successful MSP Relationship

As with any other relationship you have with an IT vendor, it is essential to undertake due diligence before selecting an MSP and then put all necessary agreements and controls in place once you agree to the MSP engagement. Be sure to address, define, and document the following:

Communications

Determine in advance all points of contact and designate who in your organization is to receive updates and status reports, and with what frequency. Set up regularly scheduled meetings with stakeholders from your IT department and the MSP, and involve your MSP in all pertinent discussions that relate to the technologies they are managing. Provide the MSP with as much information as possible —without, of course, violating any confidentiality, data, or security policies. If the engagement of the MSP relates to your company's strategic technologies, share your organization's business plans with the MSP (when appropriate) as their input on strategic IT decisions related to these plans could prove invaluable. In short, helping your MSP better understand your organization and its plans allows the MSP to better contribute to your longer-term goals.

Strive to create an environment of trust between your IT department and your MSP. All relationships encounter issues, obstacles, and challenges as well as opportunities. Setting clear boundaries and keeping communications open and clear will build and preserve a necessary level of trust between all parties. Encourage collaboration wherever possible; MSPs have significant knowledge and experience in their niche—make the most of it.

Roles and Responsibilities

Define exactly what the vendor is to provide as well as what your IT staff is to provide in the relationship. Make sure the MSP takes bottom-line responsibility for the optimal running of the technology. Verify the service being offered is not a traditional “break/fix” arrangement that’s disguised as an MSP. Get everything in writing. Also be sure you know in advance if the MSP will be providing their services along with partners or subcontractors. If so, make sure you know and document their roles and responsibilities.

Service Definitions

Nail down Service-Level Agreements (SLAs), including application up time, support response time, frequency of system monitoring, delivery of reports, management updates, etc. Be sure the MSP vendor spells out specifically what services and technologies are included and excluded as part of the cost; never assume that a service, a level of responsiveness, or a technology is included.

Contract Duration

It is prudent when starting out with a new MSP to begin with a short contract period and then extend the duration as you become more comfortable and confident in the MSP’s capabilities. Set in advance the frequency of performance reviews to be conducted with the MSP, and during each performance review, fine-tune SLAs and other benchmarks as needed.

MSPs and the Cloud

Particularly for SMB companies, it's not unusual for corporate IT staff to lack the necessary skills to effectively monitor and maintain applications in a cloud environment, which is why many SMBs and even larger organizations turn to engaging an MSP to help manage cloud-based security, computing, storage, applications, disaster recovery, and more. Cloud MSPs are often able to manage the related vendors that are part of a company's cloud initiative, and some MSPs offer their own cloud services and applications.

DRaaS

Disaster Recovery as a Service (DRaaS) is a rapidly growing offering in which an MSP provides a backup/recovery environment in its own or a third-party data center or through a contracted cloud provider. A recent survey of IT executives conducted by Vision Solutions found that 24% were utilizing some form of DRaaS; in addition, many industry analysts are expecting this sector to grow dramatically over the coming years. The adoption and growth of DRaaS is not surprising as it relieves the organization of the capital costs of implementing its own backup/recovery environments, while relieving staff of much of the time and stress to manage and monitor these environments and processes. The service is typically priced on a monthly subscription basis, which includes all necessary software licenses as well as related services for all monitoring, management, and testing of the DRaaS environments.

Of course, DRaaS offerings always include some method for maintaining a copy of your protected data in the vendor's recovery environment. The frequency with which that copy is updated can range from periodic snapshots of data to real-time replication of each change within a data set as it occurs. DRaaS is offered by numerous IT services organizations as well as many of the ISVs that develop backup and high availability technologies. The latter generally utilizes its own technology, its own technical services teams, as well as backup environments that range from its own data centers to those from a third party to those from a cloud provider.

The level of recovery capability can vary with DRaaS offerings as well. Some will provide the capability to restore data and applications to another server in the event of a disaster so that business can be resumed on the new server until the production server is restored. Other offerings provide a recovery time measured in hours or even minutes by switching your operations to a fully synchronized backup server so business can quickly resume as usual.

For many companies, especially those that fall into the SMB category, the benefits and cost-savings of a DRaaS program can be substantial, particularly if the company is looking to achieve high availability, because creating and maintaining an in-house disaster recovery infrastructure is significant. The cost of the high availability software is just the start. Then there's the required backup set of hardware and the software licenses for servers, storage, and more. Plus there's the cost for a space for your secondary or backup machine. Your company may have an offsite building that can be used to house this equipment, but then you have the added costs of power, cooling, and other infrastructure requirements. If you don't have another facility, there's the cost of leasing space at a third-party data center. Either way, you also have costs for bandwidth. And then there's the cost of having staff travel to and from data centers and/or keeping on-site staff at the secondary data center.

By utilizing a DRaaS vendor for high availability, you eliminate these capital costs as well as the complexity that comes with building out and managing your own DR infrastructure. Everything is rolled into a fixed monthly expense, which in itself benefits corporate balance sheets.

When evaluating DRaaS options offered by an MSP, there are several critical capabilities to look for, particularly if you intend to incorporate high availability as part of the service:

Data Protection and Security

Find out how well your data is protected in the MSP's data center or cloud service. Does the MSP have its own redundancies in place in the event of their own disaster? How solid are these redundancies? Also ensure your MSP has all necessary data security and encryption protections in place so that breaches are prevented and, if one does occur, that your sensitive data is encrypted.

Data Integrity

The MSP needs to provide you with assurance that it will constantly validate the accuracy of the data on the recovery server to ensure that it is in sync with the production server. If desired, you should be able to participate in monitoring your solution through a browser-based interface, and regular, detailed reporting should be provided by the MSP regarding the status of data protection and switch-readiness.

Scalability

Make sure your DRaaS solution can grow as you grow, whether you are a small business with just a few servers or your data center is expanding to thousands of servers.

Multi-platform Support

It can be an added benefit if the MSP you choose can protect all of your on-premise and cloud-hosted production servers. That way, you may need to contract with only a single vendor.

Disaster Recovery Consulting

The DRaaS service is only one component of a true disaster recovery planning strategy. In addition to providing and managing the technologies for data backup and recovery, it is an added benefit if the MSP you engage for DRaaS is also able to guide you through a comprehensive disaster recovery planning process so your IT department can be as prepared as possible to quickly and fully recover operations should a disaster occur.

In Summary

With increased frequency, organizations are adding MSPs to their mix of IT resources to ensure the best experts—both internal and external—each focus their valuable time and attention on the right areas of your IT mix. This can be especially important when it comes to system availability and IT security operations. Enlisting the expertise and focus of an MSP for these critical infrastructure functions adds an invaluable ally to your IT team, making the most of your existing resilience-technology investments.

The benefits are significant:

- Increased operational efficiency, including more flexibility and scalability of IT resources
- Reduced operating costs, especially when taking into account the prevention-centric nature of MSP offerings
- Cost-effective access to best-in-class expertise
- Reduced downtime and disruption
- More focus of internal staff on strategic IT initiatives
- Added peace of mind

MSP Checklist

- Determine where an MSP can best supplement your IT team. Non-strategic, high stakes infrastructure challenges are often the best areas for consideration.
- Evaluate potential MSPs based on expertise, reputation, resources, level of service and cost. Where appropriate, give higher consideration to application-specific MSPs.
- If the MSP engages subcontractors as part of its offering, evaluate the subcontractor's credentials
- If you're choosing an MSP for a DRaaS engagement, be sure to verify the resiliency of the MSPs data center or cloud
- Once a decision is made to select an MSP, clearly define roles and responsibilities, SLAs, and communication expectations
- Where practical, contract initially with the MSP for a trial period to evaluate performance

Easy. Affordable. Innovative. Vision Solutions.

Vision Solutions is a leading provider of business resilience solutions – high availability, disaster recovery, migration, data replication and security – for IBM Power Systems. For more than 25 years, customers and partners have trusted Vision to protect and modernize their environments, whether on-premises or in the cloud.

Visit visionsolutions.com and follow us on social media, including Twitter, Facebook and LinkedIn.

Find us on:

Facebook: <http://www.facebook.com/VisionSolutionsInc>
Twitter: http://twitter.com/VSI_Power
YouTube: <http://www.youtube.com/VisionSolutionsInc>
Vision Solutions Blog: <http://www.visionsolutions.com/blog>



15300 Barranca Parkway
Irvine, CA 92618
1.949.253.6500
1.800.683.4667

visionsolutions.com