SmarterMSP's Ask an MSP Expert. Volume 1

Real-world advice for tackling common challenges for today's managed service providers.

MSP Barracuda
Your journey, secured.

BarracudaMSP.com

Table of Contents

Introduction

As a managed service provider (MSP), you provide tremendous value to your small- and medium-sized business (SMB) partners. But while you know your business inside and out, there is always something new to learn along the path to business growth.

Maybe you're a tech whiz, but not as confident with marketing, sales, and customer relations Or, maybe you're a hot shot when it comes to customer relationship management, but have some catching up to do on the latest cybersecurity threats and how they impact your customers and even your own business.

The SmarterMSP blog's "Ask an MSP Expert" series has been an audience favorite for years, helping answer common questions from MSPs.

In this eBook, we are compiling some of our most popular posts, in hopes that we can help you make your day-to-day challenges easier to overcome.

Dive into this eBook to learn:

- Security best practices
- How to maximize your MSP's service offering
- Tips for best positioning your services to clients

Let's get started!

Best Practices for Securing Customers

How can we streamline our patch management process?

Moving forward, managed service providers (MSPs) will find that prospective clients are primarily searching for a service provider who can guard against and resolve any cybersecurity headaches that they may encounter. For the MSPs, this means building a "**security-centric**" service offering that can take advantage of new and existing technologies. Beyond the expected external threats, this offering also must be able to convert internal vulnerabilities into additional layers of cybersecurity defense.

Patch management serves as a key defense against cyber threats and is also required to ensure operating systems and business-critical software are maintained. However, it is not always a simple task for MSPs, especially in current times. With the new remote workforce, MSPs must develop best practices that not only ensure network servers are up to date but also that customers' endpoints are updated frequently to prevent any exploits.

A recent Barracuda MSP partner poll revealed the most common challenges with patch management include effectively testing patches before customer deployment, failed deployments, and the ability to confirm customer patches are up to date.

To streamline your patch management process, try these tips from Barracuda MSP experts.

> With the new remote workforce, MSPs must ensure customers' networks and endpoints are updated frequently.»

Get the full picture

Although there are many patch management solutions on the market, remote monitoring and management (RMM) platforms offer MSPs the most complete patch management features. However, RMM vendors often take different patch management approaches, so as you compare platforms, consider these factors:

1. **Patch sourcing.** The source from which the RMM pulls the patch is important. It tells you whether you can leverage it for all software comprehensive patch management. Also, some sources will research the validity of the patches prior release, shortening the testing cycle for MSPs and making the process more efficient.
2. **Whether the RMM platform offers granular control to apply patches**. Different devices and users have different requirements. Having granular control allows MSPs to create test groups within their customer sites to meet unique needs.

Consider automated vs. manual patch management

Whether you should invest in automated patch management comes down to your service model. If the majority of your customers fall under the break/fix service model, you may find that manual patch management is suitable because you are not required to keep patches updated for your customers, just validate whether they’re up to date when issues arise.

If you offer active monitoring and management services, automated patch management is a must. Automation will allow you to scale your technicians’ time, standardize patch management service delivery, and prevent cybercriminals from exploiting vulnerabilities.

It is worth noting the managed service approach offers several benefits when compared with the break-fix model. Not only do managed services result in predictable recurring revenue, but also enable the MSP to avoid many reactive emergencies to an extent because of the focus on upfront, proactive care.

Test, test, test

Even the most trusted vendors' patches should be tested before rollout, lest they cause catastrophic impact when they conflict with customer infrastructures. Consider the example of a company that had scheduled automatic rollout of minor Microsoft updates. A patch conflict with the company's billing software brought the entire finance team to a halt during year-end.

An easy way to test patches is to set up test groups within customer sites consisting of non-mission critical devices. As new patches are released, schedule automatic approvals for the patches for application to test groups. Once patches are successfully deployed to test groups, they can be rolled out globally.

A patch conflict can bring a company's business operations to an abrupt halt.»

Set timelines and communicate

To ensure a successful patch process, MSPs must ensure all devices are available and online. It is critical for MSPs to set the patch timeframe and communicate the patch schedule with customers. This will increase the success rate for patches deployed.

If their patch management is deployed through an RMM platform, MSPs should also leverage alerting and reporting features. Automated reports can confirm whether the patch process is complete.

Streamlining the patch management process can help MSPs ensure that patches are deployed efficiently and successfully, ensuring customers are secure against cyber threats.

How can I prevent customers from falling victim to fraudulent websites?

As cybercriminals become more sophisticated with attack vectors such as drive-by downloads and malvertising, it is increasingly difficult for users to **detect malicious websites** or hidden harmful threats in seemingly reputable websites.

In 2019, Google security researchers identified a number of malicious websites that exploited several zero-day hacks. While these websites are primarily used to hack iPhone users with iOS versions 10 to 12, it was later found the capability extended to Windows operating systems for desktop PCs.

Education is often the most effective protection you can offer your customers. Teach them how to spot phishing websites. Here are some tips you can share with your customers' end users:

> Education is often the most effective protection your MSP can offer to customers.»

Check the URL before you click

No matter how you receive a URL, always inspect the link for telltale signs of a malicious website, such as:

- **The addition of unnecessary words and domains.** To inspect the URL, simply hover the mouse pointer over the hyperlink. The URL will display in its full form. Malicious websites often mimic a reputable website—but with added words and domains.
- **The source of the link.** Do you know the person who sent you methods to get to the URL, so you have more control for URL inspection. the URL? If it came from an email, hover over the sender's name to inspect the email address. If it was a social media share, it is best not to click on the URL. Rather, explore other

Check the website before entering personal information or login credentials

Look for the following to determine whether a website is credible:

- **Is the website SSL or TLS certified?** SSL/TLS certificates encrypt sessions and protect information sent between browsers and web servers. To verify the SSL/TLS certificate, hover over the lock icon beside the URL and select certificates.
- **Is the URL a homograph?** Copy and paste the URL in a new browser to test its authenticity.

Beyond the human layer of security

In addition to educating your customers' end users, you should employ multi-layered security measures. For example, as part of your managed services offering, include **web security to alleviate the risk of human error.**

Most web security solutions work to protect users from malicious websites. Look for features such as **advanced DNS and URL filtering,** a connection to reputable threat intelligence networks, and integration with a **remote monitoring and management tool** for ease of management.

Not only can a web security solution protect users from web-borne cyber threats, but it can also help MSPs and their customers **define proper web usage** for endusers, ensuring consistent cybersecurity governance. As always, **combining security technologies and education** provides the best cybersecurity defense.

> In addition to educating your customers, you should employ multi-layered security measures.»

How do we take a “security-first” approach with our MSP offerings?

Security should be front and center in your MSP offerings. Potential clients seek to partner with an MSP to protect themselves from threats they can’t ward off on their own, yet many MSPs struggle with how to implement a successful “security-first” approach.

One of the most effective ways to establish a security-first approach at the foundational level is to **implement a remote monitoring and management (RMM) tool** and then **layer other solutions on top of it.** Incorporating an RMM tool before you evolve your security services offering can make your offering stronger. These high-level steps will help you create a security-first approach that strengthens your overall managed services offering.

> One of the most effective ways to establish a security-first approach is to implement an RMM tool.»

Define your MSP's managed security service

A **multi-layered approach** that leverages more than one solution will provide the **most effective cybersecurity** offering possible. A strong foundation is laid in your choice of RMM tool that allows those responsible to view and protect connected systems and devices. Often, RMM tools offer some level of **built-in automation** that makes them easier to use. From there, a variety of offerings, including machine learning, firewall and network security, AI-based security, and employee training, can be included for your customer's benefit.

Finding the right solutions is a balancing act. If your offering is not robust enough, it can leave your customer's business exposed to threats. If there's too much packed into the offering, your customer may be unsatisfied with the cost and feel that some aspects are unnecessary. MSPs should **communicate openly and honestly** with clients to make sure solutions are the right size.

Identify the right solutions

Once an RMM is in place, determining what solutions and services to add can feel daunting. The proper fit depends on each client's need. Many clients will have overlapping needs when you utilize a layered security model.

A layered security model identifies and protects several areas that are **particularly vulnerable when left without RMM protection,** including client perimeters, networks, endpoints, end users, and data.

For each protection layer, you can provide solutions that demonstrate the value of your MSP's security-first offering. Work with your clients to determine which protection layers are more important or leave them most vulnerable so you can build the right solution. This can be done via site visits or using **built-in RRM site security assessment capabilities.**

Rely on automation

Automating processes and security responses can save time and money and **minimize the risk of human error.** Many RMM tools already leverage automation in their processes, making it easier to extend it across the entire security offering.

Manually providing security services is difficult to manage because bad actors are always trying to stay one step ahead, making their attacks more sophisticated with each attempt, switching tactics, and attempting breaches when least expected. That's why automated security defenses are far more effective. They allow you to remain efficient in thwarting sophisticated and unpredictable attacks, while still being able to monitor the status of a customer's environment.

By leveraging tools that offer a multilayered approach to security, visibility into a customer's environment, and automation, you can incorporate a security-first approach in your managed services offering.

> Automating processes and security responses can minimize the risk of human error.»

Our MSP is known for its cybersecurity—but should we outsource our own?

Not even MSPs are immune to cybersecurity glitches and vulnerabilities. In December 2019, a major MSP headquartered in California suffered a ransomware attack and paid the ransom to get business operations back online swiftly. This MSP was in charge of its own cybersecurity. Might the outcome have been if they had outsourced?

Anne Jenner, who leads marketing efforts for MSPs in the Pacific Northwest, offers some perspective.

> Outsourcing a cybersecurity offering removes the MSP's need to train, schedule, and retain staff for those security service offerings, which creates significant savings in both budget and time.»

Be thoughtful when outsourcing cybersecurity

The answer to this question will depend on several factors, but the outcome can be favorable. After the right due diligence, Jenner says, MSPs may decide farming out their own security makes the most sense.

The most compelling reason to manage your business' internal security in-house is to **standardize your practices** with those in place for your customers. After all, if you can't offer strong cybersecurity for your organization, how could you possibly tout your **cybersecurity credentials** to others? You want to be able to stand by your skills and brand, and one of the best ways to do so is promoting how well your solution protects your network and servers.

If you are going to outsource your cybersecurity, you may want to have someone on staff (whether your own or the vendor's) doing basic monitoring. Otherwise, you can develop a false sense of security. **Data sensitivity** is another issue MSPs should consider.

Jenner points out that MSPs need to evaluate and figure out what limits them. Is it staffing? Budget issues? Hours? When you identify what is keeping you from providing your cybersecurity, you enable yourself to fix it. Several common obstacles can be addressed by securing a strong external provider.

Outsourcing a cybersecurity offering removes the MSP's need to **train, schedule, and retain staff** for those security service offerings, which creates significant savings in both **budget and time**. Ideally, the MSP will also remain informed about what's going on with their clients from a cybersecurity standpoint via **comprehensive vendor reporting.**

Consider whether you are too close

“The most powerful argument I can find for outsourcing your own cybersecurity is simply to have a fresh set of eyes on your systems,” Jenner says. There’s a “closeness” that develops with any job, profession, or craft that requires the discipline and foresight to “step back” and see the big picture, Jenner says.

“I find this is especially true with smaller MSPs,” Jenner adds. “Larger MSPs have an opposite issue; they can get so caught up in ‘following the manual’ that they overlook simple fixes, and that can lead to institutional inertia,” Jenner points out. “Still, if you are a smaller MSP, and you feel like you are **stretched too thin** and cannot objectively **evaluate your own cybersecurity** on yourself, then perhaps an outside entity is of value,” Jenner advises.

That doesn’t mean your MSP should use a cookie-cutter approach. Just as a good MSP will tailor its cybersecurity program to customer requirements, **MSPs should tailor their own cybersecurity to their unique footprint.**

What to look for in potential vendors

When choosing a cybersecurity vendor, you should be on the lookout for a few key characteristics and indicators. An **experienced vendor with a rich track record of success** is one of the most obvious indicators for a successful outsourcing partnership.

Your vendor should generate **comprehensive reports** you can **showcase to customers** to prove that you are on top of all security concerns. These reports will **demonstrate the value** of your work in a way customers can better digest and understand.

You need a vendor with a **well-rounded security offering**, with several solutions working together to stop all varieties of threats in the current threat landscape. This will not only make life easier in the short term, but also handle any emerging threats. That vendor should also offer **training and other enablement resources** related to cybersecurity, either to your MSP or your customers.

An MSP that suffers a breach faces irreparable **reputational harm,** and exposure to **costly liability**. MSP clients expect their data and networks to be kept safe. The first step is keeping yours safe.

How to Maximize Your MSP's Service Offering

How can an RMM tool improve delivery of our managed service offerings through automation?

Now more than ever, managed services businesses must take a closer examination of their service offering to ensure that it is helping them realize the full potential of their business. This goes beyond adding new technologies to fill any holes in the offering. It also includes improving existing services with adjusted sales approaches and business practices.

The rapid changes in the workplace brought about by COVID-19 are a reminder that security is an increasingly critical part of both the managed services and overall business landscapes. The pandemic has also highlighted the importance of managing employee workloads using dependable tools to handle demanding tasks and responsibilities.

Automating a security offering is an effective way to make sure an MSP can meet both needs. A remote monitoring and management (RMM) tool with built-in automation provides a simple solution for handling complicated responsibilities.

> An RMM tool with built-in automation provides a simple solution for complicated responsibilities.»

Security without automation is challenging

Leveraging automation increases the efficiency of maintaining a secure environment for customers. Manual delivery of security services is not scalable for MSPs for several reasons:

- **Cyberattacks are too sophisticated** – Hackers have spent significant time and resources in developing and evolving methods of entry to bypass traditional defenses, which often rely on human management to stop these cyberattacks. Bad actors are now able to “drill down” and identify weak links in an organization’s network that will allow them to easily gain access.
- **Cybercriminals are exploiting vulnerabilities** – More and more vulnerabilities are found in software, providing an “easy” access point for cyber attacks. These vulnerabilities are frequently used by hackers to gain network access to perform the attack.
- **New threats are constantly emerging** – New cyber threats and cyber criminals pop up all the time. These new attacks are bolstered by various resources readily available to any bad actor looking for a new career as a cybercriminal.
- **Attack timing is unpredictable** – Cyber attacks can hit networks at any time. A security offering reliant on a manual process powered by humans (and therefore subject to human error and any gaps in human oversight) will inevitably fail to stop an attack.

Automated security services' benefits

RMM tools also allow MSPs to **monitor and perform tasks remotely** to ensure the availability and uptime of their customers' IT infrastructure. MSPs often scale their resources by **leveraging RMM automation features** for routine maintenance tasks and security services, including **automated patch management**, alerts for anomalies, antivirus deployment and updates, and backup windows.

Automating security services **provides consistency** and ensures that every network and application is protected. This provides MSPs and SMBs alike with the confidence that the entire environment is being managed and that nothing is only being protected "halfway."

It also provides more **accuracy,** meeting the individual security needs of each SMB customer and their networks and applications, while leaving no vulnerability unprotected. **Automation removes the risk of human error** and ensures that there are **no deviations** from the security policy's design in delivery.

For example, as new malware is discovered, **automatic updates** to block these means of attack is a tremendous value to an offering.

Automation can help **showcase an MSP's efficiency and reliability** to customers. As an MSP business grows, RMM automation features allow MSPs to **scale services** to meet the needs of each new customer **without adding staff.** Lastly, by automating security services such as antivirus, patch management, and backup services, MSPs can expand their services, reduce human error, and provide consistency across customers.

Many MSPs already have an RMM in place, simply because it offers functions fundamental to running their business. If an MSP wants to run their business in a smart and strategic way with long-term benefits, they should look for a **security-centric RMM** that will make the MSP business faster and more successful in delivering security. All MSPs need a strong, well-rounded RMM tool, and using one that can easily incorporate automation to deliver security services can offer MSPs tremendous value.

Why is email continuity such a valuable offering?

Email continuity is a valuable resource for MSPs to employ—and for MSPs that work with SMB customers in certain specific vertical markets, email continuity is not just a nice resource to offer, it's an **absolute necessity.**

To get a better understanding of email continuity, the value it provides, and the circumstances in which it is immensely useful to certain SMB customers, Smarter MSP sat down with Kevin Davy, Sales Engineer at Barracuda MSP. In our conversation, Kevin outlined why and how email continuity plays such a vital role in keeping an SMB business active and how it can **strengthen the partnership** between an MSP and its SMB customers.

> Email continuity is a valuable resource for MSPs—and for certain vertical markets, email continuity is an absolute necessity.»

The importance of email continuity

For those who might not be familiar with it, email continuity keeps email accounts sending and receiving messages when email servers go down. Email servers, especially those on-premise, are prone to occasional outages. Users can rely on new servers provided by their email continuity service to **continue normal email activity** until their regular email server returns.

Email continuity's importance comes from its ability to **keep businesses running**. Many businesses are dependent on their ability to send and receive emails. With email continuity in place, SMBs that partner with MSPs can **maintain productivity** without missing a beat.

Many people think that because they are using cloud-based structured email services, such as Microsoft Office 365, they will never experience downtime. These email services still experience intermittent outages and will **only notify those users affected,** which perpetuates the belief there is more uptime than there actually is.

Best practices when employing email continuity

Email continuity has a very easy and simple set-up process once an MSP signs on. Implement the service and make sure all domains are added to the system to make sure nothing slips through the cracks. Make sure your systems are also properly configured with any **email security services** that you employ from a vendor.

Remember that email continuity is a fallback plan, a "last resort" option. It is **not supposed to replace your email server** whenever the server undergoes expected outages, such as routine maintenance. Email continuity should only be used when absolutely needed as a "safety net."

Best uses for email continuity

Any organization with physical, privately owned servers they are hosting themselves or that uses on-premises exchange will benefit the most from email continuity. If the power goes out, then their email is out as well. Most SMBs cannot naturally keep email servers running at all hours, which is where email continuity can fill in the gap. Email continuity vendors utilize cloud resources, such as Amazon Web Services, in their back-end pool to **keep uptime as close to 100 percent as possible**.

Even if uptime is already at near-max peak/potential, random periods of downtime can occur, and that's where email continuity proves its value. The more use and reliance an SMB customer has on email to conduct its business, the more value the customer will find in email continuity and, in turn, the MSP it partners with.

Email continuity is a simple service to add and offer to SMB customers at **limited cost** to the MSP. It provides tremendous value in protecting a customer's business, while strengthening the partnership between an SMB customer and an MSP.

Barracuda's email continuity service can be configured with all email servers and only requires users to enter their domain into the system. It also comes free with any email service that you add from Barracuda.»

How can I convince customers to add cloud backup?

As most MSPs know, cloud backup provides tremendous value in a service offering designed to help secure an organization's data. The trouble that some MSPs find with cloud backup for Microsoft Office 365 is convincing their clients and prospective customers of its value.

To figure out how MSPs can overcome this roadblock, SmarterMSP sat down with Kyle Marsan, Systems Engineer at Barracuda MSP. Kyle offered his tips on how MSPs can detail the positives that cloud backup offers, soothe customers' concerns about their need for it, and ultimately convince customers that cloud backup is something their business can't afford to live without.

The importance of cloud backup for Microsoft Office 365

Most people know that Office 365 has built-in redundancy and that if Microsoft ever has a server go down, the customer will never even notice. However, what happens if a user deletes, changes, or misplaces a file and doesn't realize that Microsoft's built-in retention period is a maximum of 93 days for emails and 30 days for Sharepoint and OneDrive data? This is a common user case heard all the time.

Cloud backup not only offers the **storage of critical business data** in a secondary location to the Microsoft cloud, but also supplements the built-in Microsoft retention periods for Exchange, SharePoint, OneDrive, and Groups data.

Anyone using Office 365 can benefit from backing up data. With the massive migration of data to the cloud, it's easy to overlook the need for a separate copy of business-critical data. This is a concept everyone became used to with any hosted on-premise servers, and the same is true for data that lives in the cloud.

Common obstacles MSPs need to prepare for

The biggest obstacle MSPs face is **explaining the value**. "Why do I need to add cloud backup for my Office 365 data—I thought Microsoft did this already?"

Another common obstacle is that customers may confuse a backup with an archive. Customers who must comply with various regulations will subscribe to an archiving service, such as Barracuda Cloud Archiving. They often think they no longer need a backup because they have an archive—but the archive and the backup serve very different purposes.

The backup contains **all previously backed-up data** and can quickly and easily be restored back into the Office 365 tenant. An archive may only contain a portion of the data required for preservation to meet regulatory requirements. In addition, you cannot easily restore data back to Office 365. Instead, you can only search and export data to a personal folder file.

Making the pitch

If you have experienced these obstacles or have heard similar objections, below are some helpful tips to guide you through the cloud backup sales pitch for Microsoft Office 365 customers:

- **Importance of all business-critical data**: Almost everyone understands the importance of email, but OneDrive and SharePoint are just as important. They often hold more business-critical data than email boxes. I often ask, "What happens if someone deletes a folder or makes a change to a file?" This is a great opening question for a cloud backup discussion.
- **Office 365 storage limits**: Just like on-premise Exchange servers, there is a limit to Office 365 storage. If an email or file is deleted accidentally, and your organization is at your Office 365 storage limit, Microsoft will often remove the deleted items on or before the data retention period. Ask your customer about their Office 365 storage limits and their growth plans. Explain the data retention periods that Microsoft has to establish the value of a separate cloud backup service to provide additional security to their data.
- **Employee turnover**: In order to preserve the data of an employee who has left the customer's organization, your customer would have to keep their Office 365 license. However, with services like Barracuda Cloud to Cloud Backup service, the data is backed up and accessible even if the Office 365 license is removed. The data can be recovered regardless of whether the user exists in the Office 365 tenant. The customer can save both the license cost and the storage cost of that data sitting in Office 365.
- **Part of a multi-layered email security strategy**: Email is still the No. 1 attack vector, and Office 365 is not immune to cyberattacks. Include cloud backup as part of your multi-layered email security service offering to show your customers that you cover every aspect of email security to properly protect them from today's email threats.

How can I persuade clients to add VPNs for a remote workforce?

Given the global response to limiting the spread of COVID-19, many businesses have transitioned their employees into working remotely, often from their own homes. Of course, many of these new "home offices" lack the technological capabilities of the regular office building to ensure that all business activity is conducted securely. While other options can work, some MSPs have heavily used virtual private networks (VPNs) to great success in securing the work of remote employees.

Smarter MSP spoke with Nathan Bradbury, Systems Engineering Manager at Barracuda MSP, and Mark Ballegeer, Systems Engineer at Barracuda MSP, to gather tips for communicating VPN recommendations to clients effectively.

Many MSPs have heavily used VPNs to great success in securing remote employees.»

Selecting the right VPN set-up

Nathan begins: “This is a question I regularly get asked by partners. Before deciding if a client needs a VPN, I always start by asking, ‘Why would they need a VPN?’ Is it for device security, securing accessing resources, or some other reason?”

Often, simply enabling DNS over HTTPs can provide similar value to what some providers offer and ensures protected access to appropriate DNS records. Nathan finds that **private VPNs** (non-split tunnel) provide far better security when appropriately maintained and secured over a public VPN.

Other options exist, one of which is a product that provides **advanced URL filtration and malware protection**. This allows providers to set granular policies to prevent users from accessing sites they shouldn’t, whether they are secured with transport layer security (TLS) or not. An additional benefit to using agent-based filtration is **reduction in bandwidth utilization**, especially when on cellular or terrestrial links. By blocking just a few common advertising websites, usage can drop by more than 10 percent.

Securely accessing internal resources would be another good use case for a private VPN. With the digital transformation of businesses to Office 365, private VPN usage has been steadily on the decline as they are no longer needed to access common unstructured data securely. Private VPNs make sense when secure access is needed for an internally hosted line of business applications that haven’t been moved to a SaaS-based solution.

> Private VPNs provide far better security when appropriately maintained over a public VPN.»

Examine the client's needs

Mark reminds MSPs to **remain customer-focused** when offering VPN set-up to clients: "Ultimately it's all about **security and productivity.** The common use case these days is that businesses need to make sure that they can continue to function in times of crisis, without risking the loss of sensitive information, and remaining compliant. This can mean different things for different organizations and businesses."

Mark also noted levels of needed user access can vary. Some people may only need to access corporate resources a couple of times a day to upload data, while others may need an experience as if they were in the office. Still, certain employees may only need access on a mobile device to occasionally retrieve information.

As always, strong **communication and teamwork** are vital for an MSP, stresses Mark. Regardless of the situation, MSPs need to work with customers to ensure their information stays secure and the right people have access to the resources they need.

Keeping the focus on the ideal VPN's specific capabilities will be the best way to persuade clients to add VPNs to the numerous new remote "home offices" of their employees. From there, an MSP can prove its worth by **limiting the cybersecurity and technological headaches** that a client experiences on a regular basis—a goal that becomes much easier to achieve with VPNs.

An MSP can prove its worth by limiting the headaches a client experiences on a regluar basis.»

Should I monitor my employees?

With so many employees working remotely, MSPs, like other employers, may wonder if electronic monitoring is a good solution to ensure everyone is staying on track. Should you electronically monitor your employees?

That is a question many business owners grapple with. There are a plethora of legal, moral, and business issues to sort through when trying to decide how much, if any, monitoring to implement.

According to data from Gartner, since the beginning of the COVID-19 crisis, almost **20 percent of organizations** have procured some form of technology designed to **monitor remote employees.** It's not just accounting firms, manufacturing offices, and publishing houses that have sent their workers home; many MSPs have also adopted a remote work strategy for their own employees. And, as many MSPs are discovering, quality work can be done remotely.

Gartner estimates **41 percent of employees will continue working remotely** even after the coronavirus crisis subsides. This means that MSPs, like other businesses, will have to come up with a long-term plan for creating community and accountability among their remote staff.

Jack Anderson, an independent IT consultant and former MSP owner in Indianapolis, offers some advice.

Legality vs. integrity

Monitoring the productivity of remote workers is legal, Anderson says. He also adds that using GPS technology to ensure your technicians are actually making a service call is legal.

In most states, employers can also monitor emails, texts, and other electronic communications. Delaware and Connecticut are two states that require notification. And there may be variations in regulations by municipality and state, so it's always best to **know your local laws** before implementing a system, Anderson advises.

"While monitoring tools are legally available to an MSP owner, just because someone can do something doesn't mean they should," Anderson says. "In the end, there is no right or wrong answer; it will come down to the specific situations at your MSP."

Trust

There is a lot to be said for trust, Anderson adds. The one thing the pandemic has taught us, he continues, is that productivity can be achieved from afar.

"If a technician or a receptionist is getting their tasks done well and adhering to best practices, what else really matters?" Anderson asks. "And if an employee is not performing efficiently, sometimes the human touch—a conversation—is more effective than monitoring with technology."

There is also the issue of interpersonal relationships at play. If your top technician is someone you went to school with and you're also fishing buddies, suddenly implementing a robust work monitoring or telemetrics program could undermine the relationship.

"In my experience—and this is only a generalization—the smaller your organization is, the more monitoring is mistrusted, it feels impersonal. Once you get above 10 employees, then it feels more comfortable as it won't look like you are targeting a specific person," Anderson says.

Selling monitoring

Still, Anderson asserts there are benefits to the employee for monitoring their keystrokes and service calls, and that is what an MSP should focus on. A robust **GPS and keystroke monitoring** program can actually help **protect employees**. It's not always about "catching" someone doing something wrong. Often, it's about supporting employees.

"MSP technicians deal with highly sensitive data sites, so having an electronic trail to document details and movements helps protect everyone, perhaps most of all your engineer. You want your engineer to have the confidence that you have their back, and the more of a trail you have, the more everyone is protected."

Productivity

What matters, Anderson advises, is that an employee, whether it is your office receptionist, accounts payable team, or technician, is getting their work done efficiently. However, what if your top engineer is getting all their work done in stellar fashion in just 15 hours a week, but you are paying them for 40? Then, Anderson says, some conversations can be had regarding the adjusting of schedules and expectations.

"So, for me, monitoring software is less about trust; it has more to do with **productivity and accountability,**" he states. "And if you sell it that way to your team, you aren't sowing mistrust. You are instead trying to make your MSP be the most efficient it can be, and that's a goal everyone should be able to get behind. Might you `catch' someone 'goofing off?' Yes, but that really isn't what this is about."

Regardless, Anderson advises that an employer shouldn't implement a monitoring program without telling the employees first. Walk them through the reasons, outline the benefits, and then everyone becomes a stakeholder instead of a slacker.

Tips for Best Positioning Your Services to Clients

Why don't customers see value in my services?

To convince SMB clients, both existing and new, to grow their partnership with a managed service business, the MSP must keep their services properly positioned in the client's mind. Much of this translates to ensuring the client understands the value that the partnership provides and what the client risks should that partnership end.

Managed service providers (MSPs) must properly demonstrate their value for clients to fully appreciate the vital role an MSP plays in their success. However, this is not a simple task and is a common struggle for those operating in any service business. How can you demonstrate the value of a long-term partnership?

Most MSPs are focused on demonstrating value, but unfortunately, they're not all equally effective at it. There are best practices, and then there are common tactics to "show value" that can often backfire. Too often, MSPs fail to realize that demonstrating value is all about the **customer's perception** of how the MSP is helping their business.

We've compiled a list of common mistakes as well as tips for course-correcting in any areas where you may be struggling.

Overtreating clients

The challenge: The saying “first impressions are everything” certainly holds true in business, so it’s understandable why MSPs are so eager to showcase their offerings to new clients at any and every chance. But offering complimentary service components or service levels beyond the scope of your agreement with a customer can hurt you in the long run. While this can initially endear a customer to the MSP, it can create expectations of service levels that are unsustainable (and actually cause them to perceive the value of the contracted services to be less than they really are).

How to overcome: Start by setting reasonable expectations. Before starting any work with a new client, service providers should outline what a “normal” level of service looks like to avoid falling into the trap of customer overtreatment. Be clear about what is included in their contract and what is not. It is also helpful to show clients what is available in addition to their contract so they can recognize the value associated with additional services and you can establish a growth path with the customer.

Missed opportunities with reporting

The challenge: Reports generated by service providers offer visual, result-driven insights into the work an MSP has done for its client. Unfortunately, the value of these reports is not maximized when an MSP simply passes reports to the client without further explanation of what they indicate. Something simple like the number of patches deployed to company devices can seem less significant to the client, unless the MSP explains what issues those patches have fixed or guarded against, and how the patches will help those using the devices to drive more business.

How to overcome: When offering reporting on their work, MSPs must provide detail and context to ensure the client truly understands how the work provides value to their business. MSPs should maintain a regular schedule of reporting and communication with clients to ensure the value of services provided stays top of mind.

Client misalignment

The challenge: When attempting to showcase value, most service providers will point to an instance(s) where they "saved the day" by, for example, recovering a client's lost or stolen data. While these instances are impressive and should not be discounted, clients will evaluate MSPs on more than just the times when disaster struck. Consistently meeting the evolving needs of clients is a constant challenge and one just as firmly linked to a client's evaluation of value as those "shining moments."

How to overcome: Service providers can avoid misalignment with clients by remaining "one step ahead" and anticipating their new needs. Customers often expect their MSP to be readily equipped with the right technology as soon as their need emerges and is identified. MSPs also need to make sure they "fit" well with the clients they support. If an MSP serves clients in a particular vertical or clients with specific compliance requirements, then the MSP must provide the level of expertise required by that customer or set expectations up front. If they are unable to "fit" well with a client on their own, the service provider should work with a third party to supplement their own offerings to make the fit work.

Equating time with value

The challenge: Many MSPs will often determine the value of their work in their internal operations by measuring the amount of time spent working with a task, project, or alert. This carries over to their discussions with customers. However, those clients really care about what the MSP's work achieved: what the client is now protected from, how much their security posture has improved, and how much downtime has been eliminated.

How to overcome: To avoid equating time with value, service providers should start by highlighting positive outcome(s) that resulted from their work. The time spent should be the last point highlighted. That way, clients won't view tasks that were completed relatively quickly as insignificant and lacking in value. If you want to talk about time with customers, aim to talk about reductions in downtime, time saved by blocking cyberattacks, and other time-savers. That way, you've framed the thinking to how you're putting time back in their day.

MSPs should remember they can increase the value of their work by approaching their tasks, projects, and services from the perspective of their clients. This will help MSPs understand and communicate with clients about their goals and how the MSP's work is critical to achieving them.

What new marketing strategies should I add?

Striking a balance

Many MSPs wonder what new ideas they should add to their marketing efforts to improve their business. Some worry that by implementing new ideas or tools, it will cause some of their other strategies to lose value or effectiveness.

To help MSPs find the right balance between marketing tactics, Smarter MSP spoke with Derek Marin, founder of Simple Selling. Derek offered his advice on how MSPs can combine new tactics with adjustments to their current strategy to achieve a higher return on their marketing efforts.

New tools and technologies to consider

Using **artificial intelligence** in MSP marketing is a very interesting concept because while it has grown exponentially, AI—for marketing purposes—is still in its infancy. One way AI can help is with **content production**—more specifically in streamlining the research process and SEO purposes. Some vendors, such as HubSpot, are integrating **machine learning** and other aspects of AI into their software to "crunch numbers" in the background to drive efficiency. MSPs can **partner with these vendors** to strengthen their marketing and overall business efforts.

Any vendor that can **consolidate several marketing tools** for specific components, such as digital, social media, and email, into one platform will be helpful for MSP marketers. This consolidation reduces the effort and resources required to move leads to an MSP's sales team, as there is no need to export and move data across multiple platforms.

LinkedIn as an underutilized opportunity

MSPs should **leverage LinkedIn** more because it is one of the most effective avenues to establishing contact with accounts. With the proper LinkedIn strategy, you can establish connections with multiple contacts within the same account. LinkedIn can also generate content ideas and for backlink and SEO purposes.

Drift is a company that specializes in **conversational marketing,** a very useful area of marketing for anyone dealing with small businesses. Conversational marketing often requires making a personal/individual connection before anything can be done. Drift recently released the ability in its platform to record and publish personalized videos within LinkedIn and embed them into posts. This will make it easier to “break down the wall” and form that personal connection with an SMB prospect.

Mistakes and misconceptions

Some MSPs want to abandon blogging because they feel like it has not generated the results they hoped to see. Marin advises reexamining your MSP blog before deciding to abandon it. Often, the strategy has simply been misapplied. A common theme is that there isn’t **differentiation from competitors.**

For example, an MSP’s blog manager will see a popular post (such as a Tech Tip) and republish it on their own blog without realizing that many others have done the same. The more that particular post gets republished and spread around, the more negatively it affects each blog’s SEO, negatively impacting the return the MSP sees from its own blog. This example illustrates the need for MSPs to come up with a differentiated strategy that will truly set them apart in their marketing.

Another common mistake is when MSPs rely solely on their sales reps to grow their business and ignore their **digital marketing** efforts. To be effective, sales and marketing strategies should be used together to attract clients. Unfortunately, some MSPs put more priority on the sales side, and as a result, their marketing is inconsistent at best.

How can MSPs use the lessons of 2020 to demonstrate value?

Businesses of all kinds were faced with new challenges in 2020. Luckily, most MSPs have positioned themselves well by **demonstrating the value** of their services to SMB customers in the sudden shift to remote work.

SmarterMSP spoke with several MSPs who shared how they have dedicated themselves to showcasing their value to customers and the **lessons they learned during 2020** that will help them prepare for future sudden shifts that could affect their customers.

> MSPs shared lessons learned in 2020 to help prepare customers for future sudden shifts.»

Demonstrating value to prospective customers

To demonstrate the value and benefits of its services and solutions, to prospective customers in the current economic climate, one MSP noted it's highlighting **backup and continuity services.** This MSP stresses how its services can help set up the customer's employees remotely to **reduce any downtime.**

Another MSP commented that they can enable customers to **continuously monitor work devices**, even without the normal on-site resources. A key customer of a third MSP focuses on the non-profit sector, specifically churches. This MSP has demonstrated its value by focusing on **network security and efficiency,** as these customers are providing services via livestream, which has required investment in modern networking hardware.

Another way MSPs can demonstrate their value is to provide **customer-friendly reporting** with valuable insights on the services an MSP has provided in a given time frame. As an example, a report could show the number of cyber threats detected and remediated, patches successfully deployed, and help desk tickets submitted by clients that were addressed.

Lessons learned

Internet connectivity for employees must always be monitored and never taken for granted, as, "redundancy is a must." Another MSP warned that others should "anticipate the unexpected and have a **contingency plan** for all situations and scenarios."

One MSP offered a highly proactive way to be ready for any and all future shifts to remote working, detailing how a "cloud-first mentality" led to customers having fewer bumps in the road during the onset of the COVID-19 pandemic: "We are a newer MSP, so we started with a **cloud-first mentality**. Our clients were already set up to work remotely before COVID hit, so thankfully our clients did not have to develop a new work-from-home strategy."

If there is any silver lining, it is that MSPs everywhere have found ways to prove their worth and adapt to new conditions. Many SMB businesses will be slow to return to their "old ways," while some may stick with their new operations and business models adopted during this timeframe. That makes advice from MSPs who have learned to prove their value and prepare themselves for change at a quick pace even more vital to follow.

Is email a useful marketing tool?

MSPs have many tools at their disposal to generate new business: word-of-mouth, conferences, websites, trade shows, webinars, social media, and so on. When you are taking inventory of the tools you are using, you may find there's one valuable tool you are overlooking that's right in front of your nose: the lowly **email list**.

Journalist Kevin Williams started an email list for his content creation company that now stands at 25,000 email addresses and counting. It has proven to be an invaluable tool for his business, and it can be for yours, too. MSPs, while often niche in their focus, can benefit from having an email list.

To grow your MSP business, you need to have a mix of marketing tools at your disposal. Word-of-mouth is indispensable and cheap, but the best marketing tool you have is your **product.**

> One valuable tool that many MSPs overlook is their email list.»

Let customers market for you

If you provide a valuable service at a fair price, your customers will do the marketing for you. But marketing is often a long game, and you'll need long-term tools to remain in play. That's where the email list comes in. You've had your MSP's website up for years, but merely putting up a "cyber shingle" with your rates and services isn't enough.

You need to use the website to **develop a relationship** with potential customers. To that end, it is important to have an **email newsletter sign-up form** on your site. There are many services out there that can be seamlessly integrated into your site. Williams uses MailMunch, but there are plenty of others.

Next, consider using an incentive to get visitors to register on your site. For instance, create an eBook of "25 Cybersecurity Tips" or "IT 101: the Basics" or, better yet, a "free IT consultation" by phone, if practical. Once the person signs up, the relationship doesn't end there—it's only the beginning.

Engagement creates customers

A weekly e-newsletter can ensure you continue to offer something of value to potential customers. Whether the newsletters are written by your marketing person, the CEO, or a rotating cast of employees, let people get to know your MSP. Post some pictures of your technicians working or bringing their pet into work. Make YouTube videos that impart simple information and showcase your MSP's expertise.

If there is a significant data breach in the news, offer your take on it and how other companies can avoid such a fate. **Provide tips** on how to avoid being caught up in a phishing attempt. **Showcase favorite products** from favorite vendors. Then, deliver all of this exciting and engaging content in a weekly e-newsletter.

As your email list grows, you'll want to use a service like MailChimp or Constant Contact to manage the list and monitor **open rates and click-throughs**. Each service offers newsletter templates.

Many email services offer similar features, some more user-friendly than others, but all of them will give you data to monitor **audience engagement**. If you see that your audience is engaged, then keep the newsletters going; if not, keep adjusting your message.

Email addresses are your road map

Each email address you collect is like a seed, and each newsletter you send out is like water and fertilizer for that seed. It may take a while for that seed to bloom, but eventually, it will. Not every single email address you collect will convert into a client, but a tiny percentage will. Given the low investment cost in sending emails, it will be worthwhile.

Make sure existing clients are on the email list too. You'll be able to introduce them to new products and services, while further cementing your relationship with them.

The biggest advantage of an email list for an MSP is control.»

Some skeptics might say, "Isn't this what social media is for?" You can create the best social media presence in the world, but if you don't have a way to deliver it, it's a waste of time and money. The e-newsletter is the delivery mechanism, and the email addresses you collect are your road map to the future. The biggest advantage of focusing on building an old-fashioned email list is **control**. Once you have that email list, it's yours.

Meanwhile, Facebook and Google change their algorithms. What may work today on social media, may not work tomorrow. But an email list is yours forever. A list of emails isn't going to change in one impersonal change of the algorithm. So, if you haven't started building your list, start, and watch your business bloom.

What should we highlight in our partnerships to maintain a high rate of customer satisfaction?

Many managed service providers (MSPs) are initially brought on board by their SMB customers to serve as outsourced IT managers for the business. In the early days of the relationship, the delivery of services themselves often served as the basis for how the SMB evaluates its partnership with the MSP.

The longer the partnership lasts, the more likely the customer is to evaluate other aspects of their partnership with the MSP. To continue investing for the long-term, they will want to determine the ultimate **value the MSP provides** to their business. This is a common problem faced by MSPs. We've rounded up best practices that can help shape how you think about how to continually add and prove more value for your customers.

> One valuable tool that many MSPs overlook is their email list.»

Six pillars of demonstrating value

- **Impact** – This is one of the most important factors clients consider when assessing the value of an MSP. It's important to be able to communicate not only the service you are providing, but also what that service actually provides the customer. For example, they may not see value in "network support," but they certainly will care about their uptime vs. downtime. If you're able to illustrate how you've limited downtime for both their entire system and individual employees, that will help them recognize the day-to-day impact you're making
- **Service** – The breadth of an MSP's service offering impacts the customers' perception of their capabilities and whether they have the skills and resources available to make the customer successful. MSPs must expand their portfolios beyond a single service or focus. For example, if an MSP only offers backup services, without also offering preventative security and security response, they will leave their customers needing more. By offering a well-rounded, comprehensive solution portfolio, an MSP will be seen as more likely to help its SMB customers in their business operations and growth, thus demonstrating the MSP's value.
- **Pricing** – Pricing plays a significant role in value perception and does not offer much room for error. An MSP must price its services to be competitive within the channel, while being in line with customers. A too-high price for managed services will dissuade an SMB for obvious reasons, but going too low can raise questions in the customer's mind about the quality they would receive. Managed services pricing should be indicative of the layers of solutions and services offered and show how seriously they take protecting their clients' operations. Clients understand that any savings from paying a cheap price can be eliminated in the blink of an eye when hit with extended downtime or ransomware.
- **Responsiveness** – How easy is it for customers to get a response from you? Part of your value proposition is likely that you're always there for them, so be sure to deliver on that promise. Beyond responding quickly and with comprehensive answers to questions, customers want to feel taken care of, so it's important to focus on customer service in every interaction. Be sure that your team checks in with customers proactively, whether it's a quarterly check-in or a quick follow-up after an issue is resolved to make sure that all is going smoothly again.

- **Reporting** – Offering services with built-in, branded reporting capabilities is another way MSPs can demonstrate value to clients. With assessment and reporting tools as part of the managed services offering, the MSP and client can work together to identify areas where improvement is needed. At the same time, this builds a system of continuous assessment and evaluation where the strengths of the MSP's service delivery can be noted. It also reinforces the concept that the MSP and client are partners in achieving success for the client's business.
- **Relationship** – A critical factor in the success of the relationship with the client is setting appropriate expectations. If you set expectations too high upfront by doing things you don't typically do, that can result in customers feeling disappointed when you're not able to sustain that service level consistently. Conversely, if you don't do what you say you will do, that's certainly not good either. The key is to let them know what you'll be doing to keep them productive and secure. If you have to go beyond that in order to deliver on your promise to secure them, be sure to let them know so they understand what you're doing and can appreciate your commitment to not only meeting, but also exceeding expectations.

MSPs who place a real focus on effectively **demonstrating the value** they provide can build strong reputations, win new customers, and enjoy business growth. Relying on these six pillars will help you enhance your current MSP business practices.

MSPs who demonstrate their value can build strong partnerships and win new business.»

About SmarterMSP.com

At SmarterMSP.com, our mission is to deliver resources and content to help you grow your managed services business. From addressing the latest threats in the security landscape to sharing business best practices and step-by-step how-tos—we are committed to creating resources to help you develop your business and make it more successful.

Focused exclusively on the IT channel, we aim to be your go-to source for the news and information you need to run your MSP business more effectively. Start accelerating your growth and increasing your profits by leveraging our tools and tips. It’s all part of our mission to help you succeed.

Visit SmarterMSP.com for valuable insights on topics involving MSP sales and marketing, building a better managed services business, and security concerns and trends. Be sure to subscribe while you’re there so you can receive daily insights and articles delivered directly to your inbox!

About Barracuda MSP

Barracuda MSP is the MSP-dedicated business unit of Barracuda Networks. Our mission is to drive the success of our IT service provider partners, delivering industry-leading security and data protection via a purpose-built MSP platform, steadfast commitment to partner success, and a wealth of channel expertise. Learn more at BarracudaMSP.com.

We believe in the managed service provider model. We understand your challenges. And, we work as hard as we can to be champions for your success.

Our Partners are also distinctly positioned to grow their recurring revenue and margins and scale their business profitably, thanks to a unique business model and MSP-friendly pricing structure.

About Barracuda MSP

As the MSP-dedicated business unit of Barracuda Networks, Barracuda MSP enables IT managed service providers to offer multi-layered security and data protection services to their customers through our award-winning products and purpose-built MSP management platforms. Barracuda MSP’s partners-first approach focuses on providing enablement resources, channel expertise, and robust, scalable MSP solutions designed around the way managed service providers create solutions and do business. Visit barracudamsp.com for additional information.

@BarracudaMSP | LinkedIn: BarracudaMSP | smartermsp.com

617.948.5300 | 800.569.0155 | sales@barracudamsp.com