EGNYTE

The Modern IT Playbook for Managed Service Providers

Cloud, Governance, and Hybrid Work

Table of Contents

Introduction

The global managed services industry is built on change—and how to adapt to it. This playbook was built to help you, as a managed service provider (MSP), to confidently help your clients navigate an increasingly complex business landscape.

As an MSP, you're tasked with helping organizations navigate worldwide changes in technology deployment, infrastructure, telecommunications, and so much more. In a very real sense, you enable forward momentum. You are the guides for growth.

Speaking of growth, the global managed services industry was valued at $152 billion in 2020. That figure is expected to expand by 11.1% each year in the next six years, reaching $274 billion by 2026.

Clearly, MSPs are in demand, and the suite of services you offer is evolving to meet the new requirements of modern businesses—an evolution that has been exacerbated by the unprecedented events of 2020 related to the COVID-19 pandemic.

To keep pace with the ever-shifting needs of your clients, you need to stay ahead of the curve on technology, security, and best practices.

Here's a glimpse of the concepts and useful information you'll learn in the pages ahead:

Chapter 1: Regulation, Compliance, and Cybersecurity. Perhaps nothing is more important for MSPs than to demonstrate a thorough knowledge of governance, compliance, and cybersecurity within specific industries. Even the smallest data breach can wreak havoc and damage the relationship with your clients.

Chapter 2: Cloud Migration and Digital Transformation. MSPs are expected to guide clients through technology shifts, seamlessly adapting to new processes and trends. This chapter will explain how you can help clients contend with fast-changing requirements.

Chapter 3: Adapting to a Remote Workforce. The shift to remote work had already begun before COVID-19 changed everything. This chapter will help you guide your clients through the transition from an office-focused workforce to a one that can function digitally and seamlessly in a remote setting.

Chapter 4: Building Trust in a Changing Landscape. Changes in the workplace in 2020 created the need for expanded and completely new services to meet workforce demands. To build and maintain trust and educate clients about shifting requirements, you must evaluate your current services and maintain solid communication with your clients.

Smart, well-established companies struggle the most with change. These companies do not have internal champions to drive security and transformational change when it comes to technology. The role of the MSP, as trusted advisor, is to advocate both the security and digital transformation initiatives to help them evolve. By following the lessons of this playbook, you can help businesses establish and maintain best practices to position your services for future success.

Chapter 1: Cybersecurity, Regulation, and Compliance

Your clients are concerned about cyber attacks. They want reassurance their data is safe, and their hard-earned success will not be compromised by a digital thief.

It also is vital for business owners to remain informed about regulations and compliance, which are always subject to change. A company that fails to adapt to new rules risks potential penalties, which could affect the bottom line.

It's a lot for an organization to manage on its own. As an MSP, you can help by sharing resources and providing action steps for a company's decision makers to become educated about the risks inherent to digital operations, as well as the rules that govern how their industry operates. What follows is an overview of topics you can help clients learn about, as well as practical tips to share with your clients as they navigate these potential stumbling blocks.

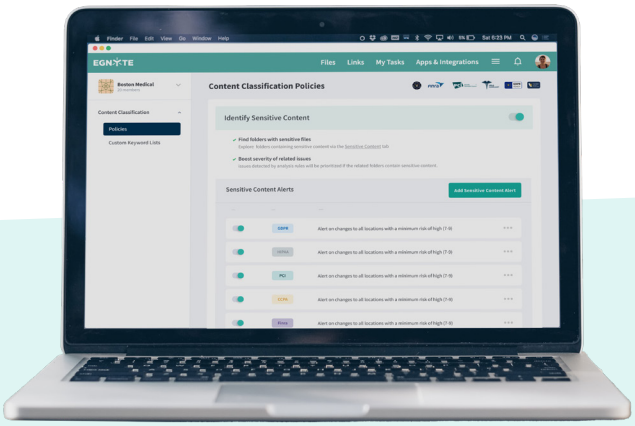
Cybersecurity: Risk Recognition and Mitigation

Once you've gained the trust required to help protect an organization from cyber attacks, any data breach will have a direct, negative impact on both their relationship with current clients and also the perception of their brand in the market.

A spotless reputation is important. Any MSP that is perceived as contributing to a company's digital vulnerability won't be in the industry for long. Nearly two-thirds of MSPs are "very concerned" about cyber attacks that use MSPs as an access point to larger companies, while 30% are "somewhat concerned."[1]

With so much at stake, you need to take a "zero-trust" approach to cybersecurity strategy. Users must be verified with multi-factor authentication when accessing any organization resources. And you need to understand where and how cyber attacks originate.

Most of the time, the risk comes from inside the business. Employee are vulnerable to ransomware attacks, email phishing, and other nefarious attempts to take down the company. These employees don't have to be bad actors; more often they're careless or uneducated about best practices.



[1] https://connect.comptia.org/blog/msp-trends-and-opportunity

Make monitoring for ransomware attacks easier using Egnyte's ransomware detection tools. Sharing recent data with clients or potential clients can help explain why cybersecurity monitoring and mitigation are so important:

- Ransomware attacks increased 105% in 2020 as organizations moved more of their services online and to the cloud.
- Phishing attempts increased by 667% and remained the most common data breach for users who work at home.
- Brute force attacks on remote desktop protocol (RDP) systems jumped by 400% during the early stage of the pandemic in spring 2020 as more workers were forced into quarantine around the world.

While knowing about the threats is half the battle, the other half is risk management and mitigation. This is an area where—as an MSP—you can render truly useful assistance with tactics designed to identify threats and fight them off before they do serious harm.

Action Step

Utilize resources from the U.S. Cybersecurity and Infrastructure Security Agency (CISA), which provides valuable resources and updates to help organizational leaders stay informed about emerging risks and how to avoid them.

Steps to Help Clients Avoid Cyberattacks

The zero-trust approach is a must to ensure your clients' digital assets are protected from external and internal threats. Multi-factor authentication for sign-ins and smart password protection are a good start, but you can help organizational leaders develop a cybersecurity strategy and employee education that goes far beyond the bare minimum of measures.

It's important to remember your clients are generally more receptive to solutions-oriented steps rather than focusing on the potential for frightening consequences. While scare tactics might get someone's attention, what they really want to know is how you're going to protect them.

To that end, it's vital to offer practical risk mitigation steps as part of the education process. Here are a few ideas to help you emphasize the importance of digital diligence without triggering a panic response in your client:

- **Conduct a risk analysis.** Determine which digital assets are most valuable, which assets are most at risk, and what must be done to protect them.
- **Use data loss prevention tools.** Once you've identified the most valuable data, protect it from potential erasure or theft at every stage of use—at rest and in motion.
- **Provide security awareness training.** Make sure employees understand the inherent risks involved with moving digital data. Reinforce the steps they can take to protect the company and themselves from cyber attacks.
- **Implement a permissions management system.** Protect an organization's data by limiting access to only those who are authorized to view it.
- **Protect data at rest and in flight.** When data moves, make sure it's encrypted and protected from interception. For added security, use passwords when sharing files with intended recipients.
- **Conduct ongoing monitoring.** Compliance requirements change often and new risks evolve every day as cybercriminals seek more creative methods for breaching digital defenses. Security and compliance must be maintained to remain effective.

Action Step

During your QBRs or Technology Business Reviews with clients, include a cyber hygiene report that includes installation of antivirus protection, network firewalls, regular software updates and audits, password strength requirements, encryption methods, employee training programs, and regular data backup and cleaning protocols.

Cybersecurity Trends to Watch

Here are a few emerging ideas and concepts to consider for 2021 and beyond:

- **Cybersecurity Mesh.** Gartner's 2021 Strategic Technology Trends guide explained the advent of the cybersecurity mesh as a way to keep up with shifting demands on the digital infrastructure. The mesh enables "any person or thing to securely access and use any digital asset, no matter where either is located, while providing the necessary level of security."

- **Specialization and Teams.** It wasn't long ago that companies began to hire the first Chief Information Security Officers to combat cyber attacks. The emergence of the CISO position led to further specialization within the cybersecurity profession. This, in turn, led to internal staff expansion by hiring individuals with expertise in threat management and response, proactive testing, and employee training or ongoing education.

- **XDR and SASE.** In addition to the zero-trust strategy of cybersecurity, managers are turning to advanced network security systems like secure access service edge (SASE) and extended detection and response (XDR) to strengthen their defenses against cyber attacks. These systems provide deeper insight into potential threats throughout a network.

Monitoring and Responding to the Regulatory Environment

In addition to helping clients understand and protect their organizations from cyber attacks, you play a valuable role in helping a company comply with federal, state, and local regulations related to their industries. Some industries present greater compliance challenges than others. Regular and automated compliance audits are the key to ensuring your clients are up-to-date with all important protocols.

For example, organizations that work in life sciences are subject to more regulatory scrutiny than other types of companies. These businesses make medicine, manufacture medical devices, and program medical software. They deal in sensitive research and development information and intellectual property, and they rely heavily on large amounts of sensitive data.

The goods and services provided by life sciences companies also are highly regulated and must meet stringent compliance requirements to be deemed suitable for public distribution. It is your job as an MSP to be aware of all potential threats and the changing regulatory landscape, regardless of the industry.

Life sciences offers an example of a complex compliance and regulatory environment. The U.S. Food and

Drug Administration (FDA) issues approval for medicine, medical devices, and other products associated with life sciences companies. There are GxP guidelines that dictate processes throughout your client's entire technology stack.

Requirements related to FDA Title 21 Code of Federal Regulations Part 11, which regulates electronic records, have changed considerably over the years as medical establishments have adopted more advanced technology for storing and communicating patient information.

In addition, the establishment of the General Data Protection Regulation (GDPR) in 2016 created layers of additional compliance for companies like Google to avoid fines and other penalties. The California Consumer Privacy Act (CCPA) followed in 2018, creating even more compliance concerns for companies to navigate. And additional states have enacted their own regulations, like New York's SHIELD Act, which makes the evolving landscape of data privacy laws even more complex.

Company owners and anyone with a vested interest in the success of an organization will rely on your knowledge to understand the regulatory landscape and potential cybersecurity threats. It's one of the chief reasons businesses seek the assistance of MSPs to combat cyber attacks and maintain compliance —peace of mind.

Industry leaders are always looking at innovative technologies to help them stay aligned with 21 CFR Part 11 and manage data in a GxP-compliant environment—without pulling their focus from the science of developing their life-changing therapies.

Egnyte for Life Sciences provides a compliant, unified data governance platform that boosts visibility and control over proprietary data—your most valuable asset. By providing a centralized environment for R&D, business, and regulated data, Egnyte for Life Sciences offers a GxP compliant environment to support regulatory requirements, like FDA 21 CFR Part 11 and GDPR.

Follow the steps included in this chapter, and the rest of our playbook to give your clients a leg up on understanding how best to take control of their cybersecurity challenges and regulatory compliance practices. Doing so can help build and maintain an enduring client relationship based on trust.

Action Step

Compile a list of resources for updates from relevant regulatory bodies for your clients' industries. The list should include federal agencies, such as the Federal Trade Commission (FTC), the Food & Drug Administration (FDA), or the Securities and Exchange Commission (SEC). It also should include state-level agencies, local agencies, and professional licensing agencies.

Chapter 2: Cloud Migration and Digital Transformation

Cloud migration—deploying an organization's digital assets to the cloud—is quickly becoming a core component of MSP services, especially as organizations move more of their infrastructure to cloud-based services. Managing these migrations is a complex process that requires buy-in from clients who are relying on your expertise to help them reach the other side of a technological upgrade.

That buy-in only comes with trust—which you can only build by providing consistent value as a partner to your clients. You'll have to understand their needs, while also being mindful of obstacles like cost as you provide guidance and implement new systems for each client.

Below, you'll find a set of tips and advice that will help you provide your clients with peace of mind—as well as set them on a course for a well-conceived, well-executed digital transformation.

Help Small Business Clients Navigate Budget Challenges

Companies and organizations with fewer than 1,000 employees are more likely to consider cost an obstacle to digital transformation.

Egnyte partner The Lewis Group—a real estate developer with 600 employees—provides an example of cost savings through cloud migration. The Lewis Group needed to implement remote access for its team members to see and use critical files such as project documents and architectural plans.

Egnyte implemented a cloud solution that reduced direct costs by 66%. It also saved an average of 30 minutes per day for each of the company's 600 employees—that's 300 hours of extra capacity per business day.

To truly understand how your services best benefit your client from a cost savings and efficiency perspective, you need to take a deeper dive into your client's goals, capabilities, and obstacles. That means expanding the relationship beyond IT partner—to business partner.

Action Step

Devote time to explaining the ROI of your services. Help your client understand how what you do supports specific business goals in a cost-effective way.

Offer Business Strategy Advice to Add Value

To remain competitive in the industry, many MSPs have found that they need to expand the list of services they offer to include cloud service management in order to meet a broader range of their clients' needs. This makes sense as more organizations are looking at ways to transition from on-premises solutions to the cloud. Around 60% of MSPs intended to expand their services even more in 2021.

Many of these new services focus on business operations and strategy. Companies still need help moving IT services, applications, data, and resources to the cloud, but 75% of MSPs added higher-level services to their offered solutions in 2020.

Here are just a few of the higher-level services you might consider offering to customers beyond IT migration and management:

- Tech roadmaps for core services and emerging technologies
- Needs assessments for specific user types and business units
- Consulting and training for C-suite stakeholders
- Compliance audits
- Consulting on architecture and design solutions
- Proof of concept and pilot project guidance

If a move toward business consulting is going to work, though, you will need to know how your core services align with the business goals of your clients—and you will need to determine how best to demonstrate that relationship.

Here are a few examples of how digital transformation and cloud migration might affect your client's current business strategy:

- Speeds up legacy processes, saving time
- Adds a layer of security and process control
- Improves customer experience
- Modernizes the company's toolset, creating a more attractive workplace for prospective employees

Business owners and managers speak the language of results. It helps to be able to show how your services can enable a company to perform well on its key performance indicators.

Your clients might also be persuaded by alleviating some of their fears about digital transformation or by giving them evidence they can use to achieve buy-in from leadership.

Action Step

Once you add business consulting to your suite of services, train your sales teams to recognize potential opportunities to offer those services early in the client relationship.

Provide Automated Data Security

Another way to help your clients is to introduce security automation. With the right tool, you can streamline time-consuming tasks such as cybersecurity threat detection, regulatory compliance maintenance, and ensuring secure external collaboration.

Egnyte customer Rockbridge, a private equity firm that makes investments for the hospitality industry, needed to secure its investors' private information companywide. The firm used labor-intensive internal algorithms to secure private data but sought a way to reduce the amount of manual work required.

The firm implemented Egnyte's AI-driven Protect data security and compliance solution and reduced the time to generate and review compliance reports from 40 hours to 10 hours per week. The benefits included a reduction in workload for the IT department, improved threat detection and response, and a decrease in the time it took to identify sensitive content.

The bottom line is this: Automated threat protection helps surface issues faster. It also identifies any potential stumbling blocks or friction in the transformation process.

Action Step

To learn more about how to guide your clients through the cloud migration and digital transformation journey, become an Egnyte MSP Partner. It's free to join and comes with a lot added benefits. Learn more at www.egnyte.com/msp.

Chapter 3: Adapting to a Remote Workforce

Remote and distributed workforces are commonplace today. Many businesses have opted to either take their teams fully remote or expand their work-from-home policies during COVID-19.

The pandemic only accelerated the shift to remote work. In a survey of 800 executives worldwide by McKinsey & Company, 85% of respondents said they increased the digitization of communication and interaction among employees because of COVID-19.

As a managed service provider, part of your role is to guide your clients through the transition from an office-focused workforce to a workforce that can function digitally and seamlessly in a remote setting.

With the knowledge that more employees will be working from anywhere after the pandemic, it's time to consider how a client's current infrastructure scales to meet these needs. The interim methods and frameworks put in place may not have been optimal, and as an MSP, you're in a position to help clients define how to move forward to optimize and secure those temporary-turned-permanent solutions.

Remote Work and Security

Research for the Egnyte Data Governance Trends Report revealed that 29% of employees use unsecured networks to access company data, and 47% of the files accessed contain sensitive information. The sensitive information on these files could be vulnerable to outside access.

The use of an unsecured or lightly secured network to access a company's digital data could create a pathway for cyberattacks or malware. Other potential issues include data sprawl and other problems related to content management, such as mismanaged permissions, file loss, and more.

Egnyte helped many companies transition to remote work during the pandemic. For example, IK Investment Partners in Europe and Brookfield Properties in the U.S. implemented cloud-based file sharing with Egnyte, allowing them both to adjust instantly to secure, reliable communication and collaboration when their employees were forced to work remotely during the pandemic lockdown.

London-based Egnyte client BW: Workplace Experts provided another recent example of how to overcome data throttling and other file-sharing problems in the face of a crisis. When the pandemic forced employees to stay home, BW implemented a single, cloud-based storage platform powered by Egnyte to speed data sharing and gain greater visibility and control of content.

Moving Forward: Remote Is Here to Stay

According to a 2020 survey of executives conducted by McKinsey & Company, more than 60% of employees in the United States are not able to work remotely because their jobs require their physical presence.

Still, that means about 40% of the U.S. workforce can potentially incorporate remote work at least part of the time. Industries that lend themselves well to remote work include information and technology, finance and insurance.

Of the 800 executives surveyed by McKinsey, 34% said they anticipated at least 10% of their employees to work a portion of the week remotely. Before the pandemic, only 22% of executives embraced remote work as an option.

And employees are keen to retain remote work as an option, even post-pandemic. According to a survey on remote work conducted by Owl Labs, half the respondents said they won't remain with companies that fail to offer remote work in the future, while 77% said they would be happier if they had the option to work at home after the pandemic.

The hybrid working model—where employees split their time between in-office and at-home workdays—allows flexibility for employees while also maintaining a pathway for the traditional on-site work environment.

Regardless of how the hybrid model works for your clients, the risks inherent to the remote model are still a concern. Traditional on-premises infrastructure won't provide the same security level when employees try to access information from home. In essence, the hybrid model requires the same fundamental changes.

Action Step

Hone your expertise in data governance, security, and compliance to create more opportunities for value-added services as you expand your role as a trusted advisor and partner for your clients.

Instill Governance Best Practices Throughout the Content Lifecycle

Remote work solutions are great for collaboration, but they can lead to regulatory and security nightmares if businesses don't instill good content governance practices. MSPs have always played a critical role in securing small and mid-sized businesses' IT infrastructure, but that role is even more critical in the emerging hybrid model.

Good governance requires you to understand the entire lifecycle of unstructured data, with a consistent view into your data and policies across all your data repositories. To establish strong content governance for your clients, you first need to ask them these questions:

- Where is your data?
- What kind of regulated data do you have?
- How is your data being shared?
- What is your content retention policy?

Get Visibility Into All the Data

Your clients can't truly get a handle on their governance strategy if they don't know what data end users are storing and where they're storing it. The first step is to compile a comprehensive list of content repositories, which can be expansive in a hybrid work environment.

Indeed, Egnyte's Data Governance Trends Report found that roughly half of the CIOs and IT leaders surveyed cited remote work and the use of multiple file-sharing applications as main drivers of content sprawl.

Once you get a handle on where the data is stored, you can then create a single source of truth for content policies. Egnyte supports an ever-growing set of repositories, including OneDrive, SharePoint, Azure, Teams (files and chat), Google Cloud Storage, Google Drive, Amazon S3, Box, Window Server, CIFS/SMB, connected folders, Exchange Online/Office 365, Gmail and Exchange.

Identify Sensitive Data

Data privacy regulations continue to proliferate, so this is an obvious area where MSPs can provide value to businesses that don't have the resources to keep up with the shifting legal landscape. Whether it's industry-specific regulations, or PII laws like GDPR or CCPA, or even governmental certifications like CMMC, businesses are on the hook for protecting and identifying sensitive data they store, whether it's their customers' data or their own.

And while it can be overwhelming for non-experts, Egnyte makes it easy to ensure compliance guardrails are properly enforced. As part of the onboarding process, you can select the relevant jurisdictions and regulatory compliance policies in less than five minutes.

Of course, the threat isn't just to companies in highly regulated industries. Many businesses mistakenly assume they're too small to be the target of ransomware. But their size and lack of IT resources is exactly why hackers go after them.

Take the example of Quanta Computer, which assembles products for Apple. Hackers stole Mac blueprints from Quanta in an attempt to extort $50 million from Apple. And since Apple has an army of security engineers to prevent these sorts of problems on its own systems, hackers opted to exploit a weakness in Apple's supply chain instead. If your clients are on the fence about the need for strong governance policies, remind them that if they're a supplier, they have to adhere to their customer's risks, too.

Enforce Rules Around Sharing

Help your clients put controls in place to enforce policies around least privilege when sharing data internally and externally. Is data shared through public links or in groups with large memberships? Do users have access to too many folders? The answers to these questions will determine the risks your client is facing, and you can then help implement rules like passwords and multi-factor authentication to mitigate those risks.

Egnyte uses machine learning to identify common access patterns and alert administrators when there is suspicious activity, such as the same login attempted from disparate regions in quick succession, or if a user suddenly increases its daily downloads tenfold. Egnyte also suggests potential remediation actions and creates reports that identify risk levels.

Set the Right Retention Policies

Data can quickly slide from being valuable to being a liability. One of the best ways to deal with content sprawl and security threats is by setting the right data retention policies.

For example, a client may need to hold on to files related to certain projects for many years for compliance reasons, but other data might only need to be saved for a much shorter time. And older data can be archived to save money and restrict access further. Getting rid of ROTS (redundant, obsolete, trivial, and stale) files means holding on to less data, and less data means less risk.

This will also be critical for auditors, who will have questions about deletion policies and why a business retains sensitive data such as PII, encryption keys, secrets, passwords and metadata.

Action Step

Talk to your clients about their governance strategies. If they can't adequately answer the questions raised in this chapter, explain the risks—both financial and legal—that need to be addressed.

Chapter 4: Building Trust in a Changing Landscape

As an MSP, you've built your business by providing value to your clients in areas where they lack expertise. Historically, that's involved back-office functionality that might fly under the radar, especially for senior leadership that just wants the technology to work so business can proceed as normal—but that dynamic is changing.

Technology is no longer an afterthought for most businesses. It's integral to what they do and front-of-mind for corporate executives who fear getting left behind or having to compete against the latest startup. New technologies are constantly emerging and your clients have questions about what they need to get an edge or how they can fend off the latest security threats they saw on the news. On top of that, remote work and a growing list of regulations has moved the IT landscape into uncharted territory.

So, with the spotlight on you, how do you remain their trusted technology advisor through all this uncertainty?

Identify Changes in the Market

Any MSP that wants to remain relevant today needs to identify changes in the market as they happen. This requires additional work on your part, but it's worth the effort in the long run.

For starters, monitor industry publications and forums. No one can be an expert on all the technologies coming out right now, but it's critical that you have a baseline knowledge of the latest trends in the industry. From there, you'll have a head start when, say, your client tells you they keep hearing about Kubernetes and you have to scramble to answer their questions about how it fits in their IT plans.

In many cases, the publications or forums will depend on your target audience or industry vertical, but there are solid places to get started, such as ChannelE2E, MSSP Security Alert or r/MSP. You can also follow industry experts on Twitter, Facebook and other social media and build a collection of trusted voices who can call out important trends and discussions.

Industry events are different amid the global pandemic, but they're still a vital part of staying informed. Attend local Meet Ups and other nearby gatherings that cater to your clients' needs, including MSP-centric shows like those hosted by The IT Nation or ASCII.

The virtual nature of many shows today makes networking harder, but look for social networking hashtags and interactive features on the conference platform. It can also be difficult to dedicate time to watching conference sessions while still working from home, so communicate with your coworkers so you can still find the time you need to learn. If conferences are in person, talk to people in the halls and ask what they're seeing.

If you need more help getting a plan in place to track changes, read "Seeing What's Next," by Clayton Christensen. His book is an excellent resource that lays out a three-part model any business can use to identify change, assess the impact and prepare for it.

Action Step

Set up Google Alerts for important terms you want to track. If you don't have time to read the stories every day, carve out a dedicated window every Friday to come back to flagged pieces at the end of the week. Resources like Egnyte's Partner Network also give you access to additional tools and relationships throughout the market.

Evaluate Innovative Tech Partners

As a reseller, the technology you choose is obviously central to your future success. If the underlying technology isn't cutting it, your client will never be happy.

And while the technology is rapidly evolving, many of the core principles of being a successful MSP remain. Your profit margin depends on your ability to deliver innovative tools and services efficiently. It also depends on your ability to scale through repeatable processes that reduce manual intervention.

When evaluating new tools, they should first and foremost solve a problem or fill a need for your clients. The next question is how can you package and price the offering that incorporates that tool in its cost. So long as the tool provides value to the client and can be priced to achieve your target profit margin, it should be a good fit.

Remember, your cost includes the effort to implement and support the technology. That means looking into how quickly you can get up and running and the degree of expertise your technicians will need. More skilled staff translates to bigger salaries, more training and positions that are harder to backfill.

Once you have these basic characteristics in place, layer on business metrics like their current pricing plan, how it impacts your monthly recurring revenue (MRR), and overall willingness to pay (WTP) for new/expanded services.

That knowledge is vital when you move on to competitor analysis. You'll have a concrete understanding of what kind of services people need, how they think about the value of those services, and where they stand on price. That helps you evaluate your competition, find gaps in their offerings, and position your business more effectively.

You also need to compare any new tool to your existing software stack. Assuming you're not looking to rip and replace the whole thing, you want to find tools that integrate nicely with your existing offerings. This is particularly true of anything you want to work with your automation and monitoring tools.

Look closely at how the vendor works with MSPs. Do they have a dedicated program and discounted rates? What does their licensing and SLAs look like? Do they promote the role of MSPs to layer on top of their product and add value for customers?

Utilize New Tools to Adjust to the Market

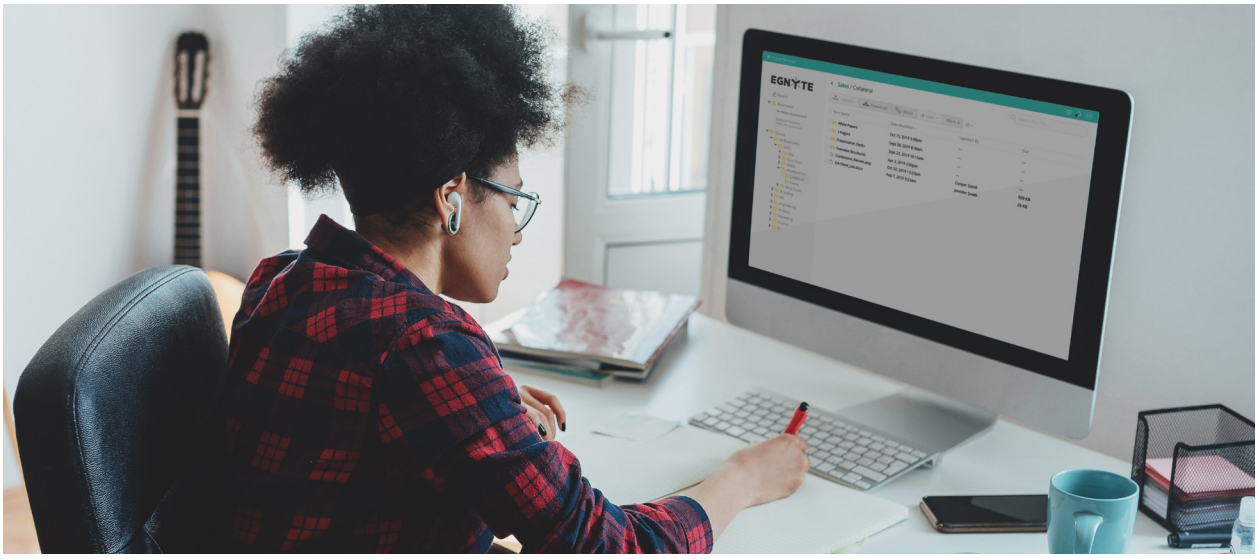
Evaluate how any new tool can help you adapt to market changes. For example, SMBs' data security requirements are accelerating. Data security is handled differently than endpoint security, and it requires new tools to meet those needs. Some MSPs are finding niche markets to serve like life sciences or construction. Some are evolving into managed security services (MSSPs) specializing in security practices.

MSPs should evaluate the need to secure data for every client, based on their industry and the data they hold. If it isn't legislation or compliance, market pressures like cybercrime and insurance requirements will push small and medium-sized businesses to increase the security around their data.

After you've determined the services you need to expand or create to stay competitive, pilot them with your existing customers. That strengthens the two-way relationship and boosts loyalty and engagement across the board.

Action Step

Make sure to utilize monitoring, reporting and analytics of platforms like Egnyte to expand your tool stack. That insight into the business mechanics of your work is the key to creating additional value for your clients.



Communicate your Expertise to your Clients

Once you've gotten a handle on the latest tools and determined which ones best fit in your catalog of services, you need to get the message out to current and prospective clients.

During quarterly business reviews (QBRs), sit down with customers. Talk about your client's current and future needs to see how you can best serve them. Highlight new services you've developed that can address those problems. Hopefully, if you've done your homework in tracking changes in the market and evaluating new tools, you'll be well positioned to meet their future needs, too.

These loyal and trusting relationships act as social proof—a crucial part of showcasing your value for other organizations through word-of-mouth marketing. Work with your current clients to create testimonials to support your marketing efforts. Not only does this showcase your value in someone else's words, it can also impact the perception of your brand.

And while word of mouth remains the most popular way for MSPs to expand their client base, it only goes so far. Eventually, you'll hit a wall and need to create marketing and social media campaigns to amplify your reach. Generate content that is relevant for your audience and provides practical advice that shows you are a trusted voice in their area of need. You can then pitch your content to trade publications that will help you target the right audience.

Action Step

Utilize QBRs as a means to evaluate clients' data security needs and risks. Talk to them about strategic and tactical goals, and use the discussion to advocate for new purchases that not only secure their content, but help them strengthen and grow their business too.

Takeaways

Throughout this playbook, we've outlined some of the key changes impacting the global managed services industry and provided recommendations to help MSPs confidently navigate the increasingly complex business landscape. Each chapter highlighted emerging trends you need to be aware of and their impact on your relationship with clients.

Great managed service providers build such strong relationships with their customers that, over time, they become trusted partners for their client's business. How you adapt to current customer expectations and provide proactive solutions to fit client's needs is a vital part of strengthening those relationships.

Understand the core drivers that impact your ability to gain revenue from customers. This will ensure you can grow your business as efficiently and effectively as possible.

Demonstrate Your Value Through Concrete Market Knowledge
Content and data governance are complex processes. When you have a clear understanding of how to implement security and privacy solutions for clients, it's much easier to provide the kind of support your clients need. And that support is what helps MSPs solidify their place as a vital part of their client's organizational infrastructure.

Keep Your Clients Data Safe
Cybersecurity threats are a persistant and potentially disastrous issue for all organizations, no matter their industry. Know how to keep clients data safe from breaches and malware attacks in order to position your services as a vital part of their company safety net.

Guide Organizations Through Difficult Change
The remote and hybrid team model will only continue to grow in the wake of the COVID-19 pandemic as people work from anywhere. Cement your place as a trusted resource for your client's business by helping them navigate these new structures.

Stay on Top of Trends and New Competitors
When you keep track of trends and new competitors in the market, it's easier to anticipate how you'll need to adjust your business strategy to decrease the impact on your customers and your bottom line.

Build Relationships Based on Trust
Relationships are at the core of your business. If those relationships aren't built on trust and a shared set of goals, it will be very difficult to scale your business and bring in additional customers from referrals.

Strengthen Service Offerings to Exceed Customer Needs
The managed services market evolves often—your service offerings need to match the requirements of both the market and your customers. That's a crucial part of how you provide consistent value as an MSP.

Understand How to Price Your Work Effectively
When you offer additional managed services for your clients, you need to understand how much they're willing to pay for them. This knowledge helps you price competitively without falling out of alignment with customer expectations of value.

Contact Us

+1-650-968-4018

1350 W. Middlefield Rd.
Mountain View, CA 94043, USA

www.egnyte.com/msp