ITGlue

The Ultimate MSP COVID-Era Recovery Guide

Introduction

The COVID-19 pandemic has brought about an unprecedented level of disruption to the business world. Priorities have changed and bottom lines have been impacted. Most organizations emerging from the crisis are realizing the significance of new technologies in reshaping the future of their business. There are three major technological trends accelerated by the onset of the pandemic – more reliance on remote work, increased use of e-commerce and greater adoption of automation. The one thing that these trends have in common is the need for IT in facilitating this change across the globe in a rapid yet secure manner. And this is where MSPs come in.

The pandemic has also taught us that the dynamics of an industry can change at any time. While MSPs had many great opportunities during the pandemic to facilitate a digital transformation, this also came with challenges like business uncertainty, downtime, client shutdown, slow growth, poor cash flow, higher costs due to technology investments, etc. When organizations return to their offices after the pandemic, it is likely to bring forth a new set of challenges as well. MSPs need to be prepared for this. This eBook will guide you with your COVID-era recovery plans and shed light on the different ways you can prepare for unforeseen circumstances.

Let's start with the proactive measures you must take to protect your business from the next pandemic.

Business Continuity Contingencies

Although the MSP industry fared better in comparison to other industries during the pandemic, not all MSPs performed equally well. MSPs that proactively offered innovative services and embraced new technologies managed to thrive while MSPs that continued to offer traditional IT services struggled to survive.

In this section, we'll discuss how a total business transformation can help you survive in the event of another global pandemic.

ITGlue

Business Continuity Testing

The top priority for any MSP is to maintain client uptime by incorporating proactive measures. Research suggests that **51% of enterprises across the world** witnessed IT downtime during the pandemic, which is a position your clients certainly wouldn't want to be in. You need to address business continuity for your business as well as your clients.

What you need is a solid business continuity plan that clearly outlines the priority of assets, the steps to be taken to maintain system uptime, the responsibilities of team members and the steps to be taken to protect client data in the event of a crisis. You need to review this plan at least once every six months and use simulations to identify any possible loopholes.

Exploring Growth Potential

Once you have established a way to ensure business continuity, you need to analyze different possibilities for growth. The pandemic has already shown that sticking to a single vertical and offering the same type of services is not a good idea. Before your clients venture out looking for new technologies, you need to reach out to them with your new service offerings.

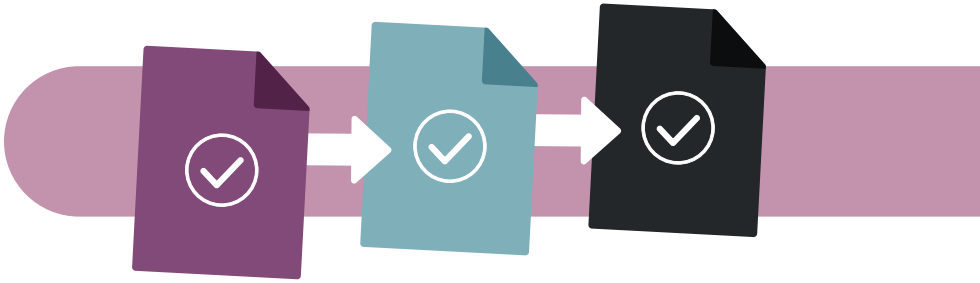
For instance, cybersecurity and vCIO have witnessed a significant rise in demand since the onset of the pandemic. Your new offerings should align with the evolving needs of your clients, which is something you need to keep in mind when expanding your services.

You also need to focus on how you can make life easier for your clients, especially during unforeseen events like a pandemic, during which your clients will need assistance transforming their workforce to operate remotely. Your sales and marketing efforts need to evolve as well. Since it would be almost impossible to meet prospects face to face, you need to enhance your virtual presence and make it simpler for current as well as potential clients to reach out to you.

Build External or Customer-Specific Documentation

The sudden transition to remote work brought new challenges to organizational network security in its wake. While it ensured operational continuity, it also made employees use their vulnerable home networks to access company data. Proactive MSPs tackled this challenge by taking care of VPN management, third-party patching, SaaS data protection, user privileges and more. In light of this, you need to follow all security protocols while helping your clients shift to a remote or hybrid work environment.

This is also a great time to explore your current technology stack and fill the gaps based on your clients' requirements. For instance, cloud technology is nothing new. However, there was and still is great demand for it during the pandemic since it facilitated digital transformation, easy data recovery, business agility and more. It is your job as an MSP to highlight the importance of new technologies to your clients and help them become more agile.



Integration of different tools is another key aspect you should consider when exploring your tech stack. The tools you have should function together seamlessly without any issue. For instance, your RMM, PSA and IT documentation tool should be well-integrated and must be accessed from the same platform. This can help boost efficiency by automating several steps in your workflow.

When you successfully implement all these business continuity contingencies, you can establish a resilient IT infrastructure that can overcome any crisis.

Summary:

- **Have a business continuity plan and test it periodically**
- **Explore new growth opportunities by offering new services**
- **Maximize device security by implementing the latest security protocols**
- **Integrate your tech stack to ensure seamless functioning**

Scaling a Remote Workforce

Remote work is not a new concept and neither are the related technologies that range from video conferencing to cloud data management. However, the pandemic accelerated the adoption of remote work at a remarkable rate. Going forward, it is almost impossible for any modern-day business to thrive in this digital world without a remote or hybrid workforce. MSPs are going to be at the forefront of facilitating this change and meeting the requirements of remote teams.

ITGlue

Refining Your Talent

The move to remote work comes with its own challenges for IT technicians as well as employees. From accessing data to ensuring optimal performance of devices, a lot of new information will have to be learned by existing and new team members.

Besides investing in new technologies and devices, you also need to train your technicians to handle remote IT infrastructure maintenance, VPN setup for employees, everyday operational issues and more. With the right training and education, you can overcome your technicians' knowledge gap and help them function effectively. You also need the right tools to facilitate knowledge sharing among technicians.

For instance, IT Glue's automated documentation ability helps seamless collection and sharing of critical information about your IT network. Similar tools can enhance the skills of your staff by facilitating knowledge sharing throughout the organization.

Expanding Offerings Through the Latest Technology

As more people start working from home, companies are likely to face new challenges in the form of security threats, documentation issues, compliance violations, etc. Your customers will be looking for ways to overcome these challenges, and you can fill in these gaps by offering these services. This requires you to look at your existing tech stack and update it as per your clients' needs.

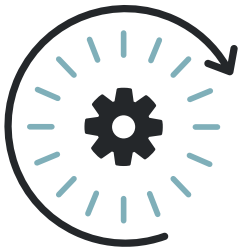
For instance, cybersecurity and data management are major offerings nowadays. A study has shown that **91% of organizations** would consider changing their IT service providers to get the right cybersecurity protection. If you are not offering this service to your customers, churn is inevitable. By equipping yourself with new antivirus solutions, remote monitoring tools, backup and disaster recovery tools, etc., you can create a solid offering to keep up with the evolving needs of your customers.

Boost Efficiency

Efficiency is a critical aspect when it comes to scaling any business. To serve more clients or help your clients expand their business, you need to identify ways of boosting your efficiency. This involves identifying your business priorities, the tasks where you use the most resources, the tools you use for various tasks, the people required for various tasks, the bottlenecks or pain points in your process, etc.

If you can automate various tasks, you can free up your technicians' time and make them more efficient. When investing in new software, look for automation capabilities. For instance, documenting everything manually is time-intensive, resource-intensive and error-prone. With an automated documentation tool, you can eliminate waste significantly and boost efficiency. Look for similar alternatives in various processes.

Remember, focusing on productivity is a good thing, but never compromise on quality for the sake of productivity.



Create a Sustainable Work Culture

Happy employees are the driving force behind the success of any organization. Before the pandemic hit, co-workers used to socialize while on the job and there was a sense of community while working with your peers. Among the major challenges the pandemic brought forth to the business world, the lack of team building is a key one.

Since face-to-face meetings are no longer feasible, it is time for MSPs to get creative with their team-building efforts. You can arrange a weekly coffee chat with your team members and discuss anything other than work. Make sure you keep the chat lively and instill a sense of belonging in each team member. By creating a strong and sustainable work culture among your employees, you can ensure solid business growth even during times of crisis.

Summary:

- **Refine your talent by enhancing knowledge sharing within your organization**
- **Fill the gaps in your services through new offerings and the latest technology**
- **Boost efficiency by automating redundant tasks**
- **Develop a strong and sustainable work culture for your team**

Cybersecurity Preparations

The evolution of technology has also given rise to a proportionate increase in security threats. Cyberthreats have been on the rise globally, with the pandemic making an already bad situation even worse. Even companies that had strong cybersecurity fortifications in their organizational networks couldn't adequately prepare for the sudden transition to the vulnerable home networks of their employees. As a result, there was a drastic spike in cyberattacks throughout 2020.

Cybercriminals have always been opportunistic and they just saw the pandemic as another way to deliver their phishing emails. COVID-themed emails carrying phishing URLs witnessed a high click rate and provide an easy opportunity for cybercriminals to infiltrate a network. In the United States, **one in three people clicked** a phishing link last year according to a study by Webroot. This should help you understand the gravity of the problem with cybersecurity in today's remote work environment.

In such a scenario, cybersecurity preparedness is non-negotiable for MSPs of all sizes. You need to incorporate the following measures to protect your organization as well as your clients from various cyberthreats.

Identify & Fill Technology Gaps

Keeping up to date with technology is the best way to combat all kinds of cybersecurity threats. This includes regularly reviewing your software tools, conducting security audits, incorporating new strategies, training your team, etc. If you are still providing IT services with legacy tools in this digital age, you and your clients are at a greater risk of being targeted by cybercriminals.

You need sophisticated tools that can automatically handle critical functions such as remote monitoring of assets, patching, multifactor authentication, etc. Tools that are designed specifically for remote infrastructure deserve special consideration when you are updating your tech stack.

Incorporate a Zero Trust Approach

Zero Trust refers to an approach wherein no person, device or application in a network should be trusted by default, even if it is part of an internal or external network. With remote working here to stay, this approach is critical to ensure only the right people have access to the right information within an organization.

To incorporate this correctly, organizations must first define what their critical data is. Then, it comes down to micro-segmenting users based on their location, access level, etc. Only when all parameters align correctly will a user gain access to critical info. This approach is a great way to prevent internal threats since it eliminates the age-old assumption that anything within the organization does not pose a threat to security.

Promote Resilience Through Security Processes

Not many businesses have the right infrastructure to support remote work. As a result, they are most likely to deal with a range of unexpected issues. The security issues arising here can be mitigated by incorporating various complementary security-control processes. Some of these processes include:

- **Boost incident response protocols** – When a major cybersecurity incident happens, there should be clear protocols on what needs to be done, who needs to be contacted, what the fail-safe options are, etc. There should also be clear escalation paths to provide alternatives if decision makers cannot be reached at the right time.

- **BCDR Testing** – In case of unavoidable data loss, a business must bounce back as quickly as possible with minimal downtime. This can be managed with a strong business continuity and disaster recovery solution. Testing it regularly will help you identify the vulnerabilities in your solution and rectify them before an actual data loss incident takes place.

- **Expand monitoring** – Remote working brings another vulnerability since some employees might access company resources with their personal devices. Are you prepared to monitor non-company assets accessing your network? You need to update your security information and event management (SIEM) system with new rules about expanded monitoring and novel threats.

Educate People About the Risks

The numerous cybersecurity measures you incorporate will not fetch you the results you desire unless you include the key stakeholders – the employees – in the security process. The employees of your clients are the first line of defense against any security threat and should be trained accordingly. With proper awareness, you can help your clients repel phishing and social engineering attacks.

To incorporate this, you must communicate with them regularly and warn them about any new security risks. Always make sure you provide clear instructions on what not to do when it comes to phishing and social engineering attacks. You can also simulate social engineering attacks to identify high-risk users. Special training must be provided to these users to further mitigate risks.

Tools like MyGlue can provide an additional layer of security by managing your client passwords and facilitating process documentation. Also, sharing documents like checklists and “How to” guides have never been easier. Take advantage of these tools to educate your staff about various security issues.

Summary:

- **Invest in sophisticated tools to combat the latest cyberthreats**
- **Incorporate a ‘Zero Trust’ approach that limits the access for all internal users**
- **Incorporate complementary security procedures to boost overall security**
- **Provide regular awareness training to employees to mitigate risks**

Returning to the Office

Although we still haven't fully overcome the pandemic yet, it would be prudent to plan your return to the office so that you have a framework in place when the time comes. The following tips could help you facilitate a safe return as part of your COVID-era recovery process.

ITGlue

Prepare to Manage the Chaos

Getting back to the office after over a year of remote working certainly won't be easy. The first few days will, in all likelihood, be chaotic and unpredictable. This is something you must be prepared to manage. It would be advisable to initially test the waters by asking only a few teams to visit the office. Once everything is settled, you can fully reopen with all your team members in place.

There is also the challenge of dealing with a hybrid workspace. Managers and supervisors should be trained to deal with a hybrid workforce and employers may also need to rethink their ways of working.

Put Safety First

The safety of your employees is of primary importance considering the pandemic still looms large. You need to lay down rules regarding vaccination policies, safety measures, sanitation habits, social distancing, etc. Also, you need to consider federal and state guidelines on what measures need to be taken while returning to work.

Some protocols may also call a change in the layout of employee workspaces, with workstations separated further apart to ensure proper distancing. You must also reduce the number of people gathering at one place. If any employee tests positive, there should be a separate protocol on what needs to be done regarding the quarantine of their co-workers.

New Services and Opportunities

MSPs also need to think about post-pandemic recovery in terms of new services for their clients. You need to consider the potential services your clients might be interested in when returning to office. Cloud, security and backup are here to stay even after the pandemic. What about the possibility of tailoring it to a hybrid workforce? Well, these are opportunities you will need to explore.

As your clients return to office, they might also need additional help from IT with regards to setting up servers, installing networks, etc. How are they going to be billed for these new services that may not be part of your SLAs? You can share the framework you have on employees' return to work. This will showcase your expertise to your clients and make them trust you even more. Make sure you consider different scenarios and come up with a plan that makes financial sense.

Summary:

- ✔ **Develop a plan to manage the initial chaos when employees return to work**
- ✔ **Ensure the safety of your employees and incorporate the right measures**
- ✔ **Explore the new opportunities your clients might be interested in when they return to work**
- ✔ **Think about how you are going to bill for the new services**

Marketing Your MSP & Exploring Opportunities

Your business growth can never stop, regardless of what crisis engulfs the world. This means that your need to figure out ways to appeal to your existing clients and generate leads from new clients. When the pandemic started, most MSPs witnessed a huge demand in IT-related services from their customers, and this is likely to continue when they return to office.

In times like these, you need to tailor your marketing and sales strategies to appeal to your target audience in the right way. You also need to explore new opportunities in the market and create new marketing initiatives based on that. Here's how you can do just that.

ITGlue

Define Your Value Proposition

When creating marketing and sales material, you need to focus on your value proposition. What differentiates you from your competitors? How do you plan on handling IT in the face of another crisis? Your customers are likely to expect answers to these kinds of questions before choosing or switching their service provider.

Educate your clients about the risks they are likely to face in the new hybrid work environment and how you can help overcome them. When targeting new customers, make sure that your messaging is structured and actionable. Don't focus too much on selling fear. Rather, focus on efficiency, cost-saving, security, etc. Your messages should also have the right call to action.

Identify Cross-Selling and Upselling Opportunities

It is much easier to sell to your existing customers than to new ones. This is why you must focus on various cross-selling and upselling initiatives. You need to explore what your customers require for their post-pandemic recovery. Rather than waiting on that next outreach from an existing customer, invite them to a meeting about the future of IT. Also, leverage your CRM and PSA to provide them with the right reports about various opportunities.

Your quarterly business reviews (QBRs) can help you demonstrate value to your clients and identify their pain points and IT requirements. You can leverage the feedback you receive here to boost your cross-selling and upselling opportunities.

Strengthen Partnerships

Use networking to your advantage and strengthen your business partnerships whenever possible. You can take part in various events and gain knowledge about how your customers operate. You also need to have strong relationships with your vendors since they can help you succeed in your marketing efforts. You can also provide vCIO services to explore your clients' actual requirements beyond the basic stack. This strategic approach can identify new opportunities and boost relationships in the long term.

Take time to review the requirements of your customers. Reach out to them every now and then and address any concerns they may have. Do not wait for them to reach out to you. Your customers should have confidence that you are here for them.

Be a Leader

During difficult times, people turn to their leaders for support. Be the leader your clients and peers need. Exhibit thought leadership by creating content on how best your customers can manage a crisis. While gaining more business opportunities should the goal of your marketing efforts, don't focus exclusively on that. Be at the forefront when your clients need assistance to get through challenging situations.

Summary:

- ✔ **Differentiate yourself from other players through unique offerings**
- ✔ **Upsell and cross-sell to your existing customers whenever possible**
- ✔ **Build strong relationships with your clients and vendors**
- ✔ **Take leadership and provide assistance to your clients during challenging situations**

Conclusion

The ongoing pandemic is arguably the worst health crisis faced by our generation. However, hard times rarely last. Even as the pandemic rages on, you need to contemplate the future of your business and how you are going to take it forward. Despite the unique challenges faced by the MSP industry, this pandemic has also given rise to multiple new opportunities.

By investing in the right tools, you can reduce waste, boost collaboration, increase visibility, secure client environments and enhance efficiency in your organization. IT documentation and password management tools can streamline your workflow effectively and boost your efficiency in ways you couldn't imagine.

Going forward, MSPs are going to play a critical role in facilitating new technology in organizations. Make sure you don't miss out on that. You can use this guide to gauge your preparedness and create a path to COVID-era recovery. With some proactive planning, you can make your recovery less exhausting and transform your organization for the better.

ITGlue

To know more, sign up for a free demo.

Check out our case studies to find out how over 6,000 MSPs around the world have fallen in love with IT Glue.

Keep track of all updates from IT Glue by subscribing to our blogs.

GET A DEMO TODAY!