The 6 Can't-Miss Opportunities for MSPs in 2021.

What you need to know to make 2021 a growth year

MSP Barracuda®
Your journey, secured.

BarracudaMSP.com

Table of Contents

Introduction

2021 is an exciting time to be in managed services. It's also a challenging time with the industry experiencing unprecedented change. However, MSPs that rise to the challenges and changes will be well-positioned to **find opportunities and new customers** as the world's connectivity undergoes a once-in-a-generation transformation. The transformations have already begun, but the widespread emergence of 5G, AI, blockchain, and IoT will continue their march, leaving almost no vertical untouched. While trends were already in the making, the COVID-19 pandemic has certainly acted as an accelerator in most cases.

Concurrently, legislative bodies across the globe are increasingly focused on **privacy and data protection.** As new laws come onto the books, MSPs will need to be familiar with the legal landscape to **maintain compliance** for themselves and their customers. As regulations become more complex, businesses will look for outside help to meet those regulations, which presents an opportunity for MSPs.

On the pages ahead, we'll touch upon some of the opportunities and issues that will be front-and-center for MSPs in 2021 and the future beyond.

Perhaps the biggest adjustment MSPs will have to make is the continued adaptation to the "new normal" both now and post-pandemic. Whether COVID disappears or rages, the landscape of 2021 is permanently altered in the wake of its impact. The difference is that, unlike 2020, when MSPs (and everyone else) had to cobble together improvised plans, 2021 allows for the creation of meaningful strategies, opportunities, and efficiencies that the new landscape yields.

On these pages, we've highlighted seven areas MSPs need to keep an eye on in 2021.

Chapter 1 -

Work From Home in 2021

Work from home saw huge increases everywhere in 2020. In the United States, Upwork released a report that states an estimated 26.7% of Americans will still be working from home through 2021[1]. And the trend isn't going anywhere.

The same report reveals that 36.2 million Americans (22% of the workforce) will still be working remotely by 2025. And it is not just in the United States. In South Africa, over a quarter of the workforce was still working entirely from home late in 2020. Figures were similar in the United Kingdom. Whether the pandemic fades or sticks around, there's no sign that work from home will be going anywhere. And that is perhaps the biggest challenge – and opportunity – for MSPs.

MSPs will need to navigate the new reality of work from home throughout 2021. The days of securing the network of a single corporate campus won't be as common. Instead, we have hundreds of employees fanned out, with each home-office becoming its own enterprise zone.

STARTLING STAT: 22 percent of the workforce will still be remote in 2025.»

1 Future Workforce Report, Upwork, December 2020

Hussain M. Al Jaroodi is an assistant professor in Saudi Arabia's School of Public Administration. He says that the work-from-home revolution has presented MSPs with many changes.

"It is very difficult to manage and protect remote employees, to ensure their safety while working on the company's network," admits Al Jaroodi. He advises MSPs to ensure that work-from-home employees utilize the following strategies:

VPN Usage

It's not enough to have employees use a VPN; the VPN itself must be adequately maintained as COVID continues to impose uncertainty on daily operations. Cybersecurity professionals must ensure that **remote employees require a VPN solution** to access the organization's network and, most importantly, keep the VPNs' software and network **up to date with the latest patches** recommended by the providers. Failing to do so is like putting a bright neon sign inviting hackers to find their way into a network.

Secure Access

VPN may not be applicable for all companies or their users. MSPs can still protect their customers' resources by **implementing zero-trust access (ZTA)** control to their resources on their network or in the cloud. Zero-trust access will validate that devices outside the perimeter trying to access the resources are authorized to do so, even if it is a BYOD. It ensures devices meet baseline security and compliance requirements before they can access resources.

Private Home Networks

As employees scatter, they need to resist the temptation to use the free Wi-Fi at the local fast food dine-in eatery.

"Remote employees should work on a **private home network,** instead of connecting to a public Wi-Fi while accessing the company's network," warns Al Jaroodi, and the home network needs to be secured using best practices.

"If an employee sends data through an unsecured public Wi-Fi connection, data might be compromised. This puts data privacy at risk, which in turn makes it possible for an attacker to capture the data," explains Al Jaroodi. Ideally, work-from-home employees should access the company's network via a **private, password-protected network.**

Secure Home Connections

MSPs and cybersecurity professionals should remind work-from-home employees to have their personal computers or work-issued workstations fully patched with the latest recommended updates and to keep their **antivirus and anti-malware software** up-to-date. Ideally, MSPs should take advantage of **automated deployment** of pre-tested software patches and updates to bolster their defenses.

As we settle into an era of employees working from home for the long-haul, MSPs' most effective weapons are entirely free of cost: effective communication and education. This is key to ensuring that employees are safe and aware of how to **identify, avoid, and report** cyber-attacks to their best ability.

Al-Jaroodi says that employing best practices is one of the most effective tools in protecting remote employees. These practices should be communicated regularly to them to ensure that they know the risks associated with risky behavior, such as using public WiFis, not updating the software, and not using a proper VPN.

Family Matters

The work-from-home transition has thrown employees into the home environment and what were once unimaginable shared-space situations. Accustomed to their own offices, supervisors are now sharing their home networks with teenagers on gaming consoles or school children attending their virtual classes.

Through it all, Al Jaroodi warns that remote employees should not allow members of their family to use their work laptops, mobiles, and other company-issued devices. It is also essential to remind remote employees to **protect their devices with a password** to prevent other people from accessing their sensitive or confidential files and information.

Over 36 million Americans are expected to be working remotely full time by 2025.»

Zooming in on Safety

Another home-threat could be virtual meetings. Public virtual meetings might be invaded. Sensitive data and information about the organization, clients, and employees may be leaked.

"Attackers may use leaked information to traumatize remote employees, clients/customers, and even blackmail the organization," notes Al Jaroodi. To avoid such an outcome, simple steps like requiring passwords for meeting entry can go a long way to keep proprietary work information private.

Zoom meetings could be invaded by hackers looking to leak sensitive information.»

Data Storage

Another step MSPs should consider is data storage. The decision as to whether to adopt cloud storage or store data locally on their remote employee's computer is an important one and will be different according to not just company policies and best practices, but laws.

Some data, like personal health information (PHI), could not be stored on someone's home computer legally. An audit of the types of data an MSP client is working should be conducted so that it can be routed to proper channels.

MSPs should conduct data audits of their clients to determine the best data storage plan.»

Chapter 2 -

Artificial Intelligence in 2021

As companies scrambled to adjust to the new reality in 2020, all the promise that AI seemed to offer in previous years took a backseat to merely surviving and adapting to the new work-from-home reality. Behind the scenes, AI played an active algorithmic role in transforming networks to adapt to the pandemic reality. But as we settle into post-pandemic life, AI and its untapped potential will once again steal the spotlight.

One of the conundrums of AI is that it can be used for good or ill. And the battle between the good guys and the bad guys and who can harness the power of AI for their ends will continue to play out in 2021 and beyond.

"AI is as disruptive as any new technology that has emerged," says Fahad AlGorain, a Ph.D. candidate in cybersecurity at the University of Sheffield in England. "For every new thing, there will always be a fight between good and bad actors."

He compares AI to technology like nuclear energy; it has very progressive, beneficial uses, but also nefarious applications.

76 percent of all enterprises will prioritize AI learning in 2021.[2]»

2 2021 enterprise trends in machine learning, Algorithmia, January 2021

But AlGorain advises that security specialists, MSPs, and other stakeholders need to **view AI as a tool and not a cure-all.** Trying to measure a winner or loser will be near impossible, because both sides have super-powerful AI in their arsenal. He notes that everyone is equally responsible for sharing the security of their systems as a bulwark against the threat AI can pose if it falls into the wrong hands.

Insider threats and employee and employer ignorance of compliance is also an issue. Employers are adopting the idea of "if it didn't happen to me, I am not vulnerable" and that is dangerous, warns AlGorain.

We will always have showdowns between the contrasting sides. AI can work to aid or hinder organizations, depending on its uses. The winner depends on the situation: are the good side **compliant and trained in AI and security** overall? AI is an incredibly useful tool in its own right for strengthening cybersecurity and fending off hackers, but needs to be **supported with the proper services and solutions to cover any additional holes** in a defense and by **educated individuals to monitor** the technology.

> AI needs to be supported with the proper services to cover any additional holes in a defense and by educated individuals to monitor the technology.»

Chapter 3 - Phishing in 2021

There's one reason why phishing remains the go-to-tool for hackers: it works. As long as it continues to work, hackers will phish. Jason Lowmiller is a cybersecurity professor at Anderson University in Indiana. He says that we are still not to the point where phishing can be neutralized as a weapon.

"Phishing will continue to work until 100 percent reliable tools that allow users to validate digital identities become readily available," predicts Lowmiller, going on to say that some of the clues as to what users can leverage to identify the legitimacy of websites or emails are not as intuitive as we would like to believe.

"What we are talking about are the different ways that our digital identities can be lost. These identities are easier to forge due to their highly distributed nature and their ubiquity," details Lowmiller.

Lowmiller adds that the state and the federal government has decades of experience in developing their control mechanisms for who has access to data and what parts of that data they can access, but a similar structure has not yet developed in the private cybersecurity space.

"Digital identities simply don't have this history, and they certainly don't have the central control of such a body to control the ways that they are used," notes Lowmiller.

This makes data security inherently difficult and diffused. Whereas the government has traditionally relied on a driver's license or a passport to verify identity, digital life is not the same.

"We now have identities at Facebook, our bank, and every other institution that we do business with. All of these are at the risk of being lost and stolen," warns Lowmiller. Stolen information turns into valuable information for hackers to weaponize.

"The distributed nature of our identities, who we share information with, the services that we take advantage of, and what information we choose to share are what keeps phishing an effective vector," says Lowmiller.

Until such a time comes that tools are available to verify senders and receivers' identities better, phishing will continue to wreak havoc. In the meantime, **MSPs' most potent weapon remains education,** reminds Lowmiller. Any additional technologies or services that an MSP offers, such as **AI for detection and defense**, should be **layered on top of the education**.

"The best that we can do is educate people on what information they should be sharing, what data organizations should and shouldn't be keeping, and to continually understand the ways threats can leverage things, like phishing or digital identities for fraud," advises Lowmiller.

Patterns of behavior (like password reuse) are difficult things to change. Unfortunately, the information that we value the least can sometimes lead to the most considerable risk.

"We don't treat all information with the same level of importance, and that also is a problem," admits Lowmiller.

MSPs will likely need to **automate most of their process**, especially regarding malware detection, phishing, and vulnerability testing. Since so much comes down to organization specifics, it's challenging to come up with a one-size-fits-all answer. Cyber talent is also an issue as the world faces a shortage. MSPs who have it should **use it as a selling point**.

"A decent approach would be to invest in local talents and try to keep them forever or at least until another talent can bridge the gap/ shortage of knowledge," details Lowmiller.

MSPs are well-positioned to fill local talent gaps. If maintaining a staffing pipeline of cybersecurity professionals proves too difficult or expensive, MSPs can always **turn to technology vendors** who offer services to supplement an MSP's internal cybersecurity talent with **external expertise from its own staff.**

Chapter 4 - Ransomware in 2021

In 2015, a tiny one-person Michigan radio station spinning oldies tunes out of a basement was hacked. The hackers demanded that Jim Higgs, the station's owner, cough up ransom money, or they'd destroy his files, which contained thousands of classic hits that played out across WAKV's airwaves.

> A new organization will fall victim to ransomware every 11 seconds by 2021.[4]»

4 Global Ransomware Damage Costs Predicted to Reach $20 Billion (USD) By 2021, Cybersecurity Ventures, October 2019

But Higgs wouldn't pay up, and the hackers made good on their promise, destroying all the music files the DJ had amassed over the years. However, Higgs would soon be back on the air after spending days rebuilding his music catalog from scratch. The amount the hackers were demanding? $500 (USD).

A $500 ransomware payment almost seems quaint by today's standards. Coalition's Cyber Insurance Claims Report released at the end of 2020 shows ransomware demands (the amount hackers demand from victims) has **increased 147 percent** just since 2019[5]. A $500 demand today would be unthinkable. Hackers are after increasingly bigger paydays, and when they don't get it, they exploit the data they do have.

5 Cyber Insurance Claims Report, Coalition, September 2020

Sodinokibi's files usually incur the lowest ransom demand at $73,920, while Maze's is just north of $420,000. One silver lining is that in the final quarter of 2020, average ransomware demands from hackers declined as more and more entities realized that paying the hackers doesn't always guarantee an end to their cybersecurity problems.

But ransomware is here to stay, especially as hackers become more creative in how they execute their plans. 2021 promises to be a turning point as ransomware morphs into outright extortion. Hackers are increasingly turning to "**double extortion**."

If a hacker can't get a victim to pay up, they threaten to release stolen data on the dark web. This can be devastating in many instances, so even if someone has sufficient back-up negating the need to pay a ransom, the data itself can then be used to coax an enterprise to pay. And if an enterprise still won't pay, the hackers have data that could perhaps be sold.

Ransomware purveyors generally don’t play nice, so once they have your data, the damage – whether the hackers get paid or not – is already done.

For years, the standard advice was "back-up, back-up, back-up." The reasoning was that if the hackers obtained your data, but you had update-to-date back-up, then the hackers are rendered toothless. This turns out not to be the case, so MSPs need to go beyond back-up and also invest in the best **anti-malware** technologies available.

No verticals are immune from ransomware, although MSPs who have clients in **healthcare, education, and the government** seem to be the most desirable targets for ransomware criminals. **Cities are attractive targets** because they usually don't have the budget for top of the line IT talent on staff, but typically have the means to pay if they are victimized.

And if the city opts not to pay, hackers have a lot of leverage, with access to critical services information and personal data. Being hit and succumbing to one ransomware attack is not always the end of the problems for organizations either. When the news breaks, it can bring about a **“circling sharks” scenario**, as other bad actors look to capitalize while the victims are trying to put the pieces back together.

The bottom line is that ransomware isn’t going anywhere anytime soon. If anything, **ransomware will become more pervasive** as hackers adopt and adapt. MSPs need to confront the threat with a **robust multi-pronged security approach**.

Chapter 5 -

Learning the Legal Landscape

If you started your MSP because you love IT, cybersecurity, and getting your hands dirty in the nitty-gritty of keeping a network running, chances are the law is a field you didn't study much. For better or worse, the law will continue to become ingrained in the MSP playbook.

Cybersecurity is not just about firewalls and patching. It is also about **education and legislation** — often, these two go hand in hand. The legislative landscape is continuously evolving as more rules and regulations attempt to add guardrails and protections to the increasingly massive amounts of data in the ecosystem.

Cybersecurity is no longer an amenity — it's the law. MSPs who once found themselves servicing networks and dispensing rudimentary cybersecurity services now find themselves on the front lines of building defenses against hackers. This role, though, **requires knowledge of the law**.

Over 280 different internet privacy laws were debated in statehouses across the USA in 2020. Expect that pace to continue in 2021.»

Lawmakers are often looking at MSPs to help implement and spread the word about new laws. The California Consumer Privacy Act, which went into effect in 2020, is just one example of landmark legislation that MSPs are expected to know.

MSPs need to continually produce **risk assessments of clients** and figure out what legislation applies to their clients. MSPs must help clients **be transparent** with how data is being **collected, stored, and used** as the CCPA mandates. Even if your MSP and your clients are not in California, beginning to comply with its provisions will have you prepared when new regulations come to your area.

MSPs need to know the law themselves and make sure their clients know it too. For that to happen, a new paradigm shift in company culture is necessary. Some steps to incorporate smart legislative know-how into your MSP include:

1. **Connect revenue and reputation with cybersecurity and regulation.** In other words, make sure clients and staff understand the importance of knowing the latest laws.
2. **Create a culture of consumer-protectionism** — Similar to the EU countries (as opposed to company-protectionism). This is a reverse from the traditional paradigm, where companies were worried about protecting their data first. This isn't to say your own client's data isn't essential, it is, but your clients must put their customer's privacy first. If they do that, customers will repay your loyalty with theirs. News reports and negative headlines have made data protection a top priority for consumers. The two need to work hand in hand.
3. **Prioritize consistent education and support of employees.** This can be done by connecting their professional success and growth with security and industry regulation, as opposed to just an annual to-do list. The connections are crucial for making the employees not just job-doers, but stakeholders.

Keeping in line with security and data regulations will not just keep your MSP on the right side of the law – it will open further opportunities to win new business with prospective and existing small and medium sized business clients.

Chapter 6 -

Partnerships to strengthen your MSP's own cybersecurity

MSPs not only have to keep their customers safe but they also now have to worry about keeping themselves safe. According to CSOnline, a growing number of managed services providers (MSPs) worldwide are being **targeted and compromised by hackers.** Such breaches can seriously impact their customers' business, as **compromised MSPs can serve as launchpads into their clients' corporate networks**.

Criminals who can't access their first network of choice can **probe for weak spots in an MSP's defenses**, gain access, and then move laterally into their quarry. In 2019 and 2020, there were several high-profile instances of **MSPs being breached**, including 22 municipal clients of a Texas MSP.

Threat intelligence firm Armor said it identified at least 13 of the MSPs hacked in 2019 had their infrastructure abused by cyberattackers to deploy ransomware on their customers' networks.[6] »

6 13 Service Providers Compromised by Ransomware in 2019, Armor, October 2019

The Secret Service sent out a security alert in June of 2020 warning of the dangers that inadequately protected MSPs can pose. Once inside, attackers can **leverage the MSP's systems to carry out attacks** against point-of-sale systems, perform business email compromise (BEC) scams, and deploy ransomware. The Secret Service advises MSPs to implement the following best practices for their managed services business:

- **Have a well-defined service agreement** with all of your customers so that all parties understand the business arrangement's parameters.
- Ensure remote administration tools are **patched and updated**.
- **Enforce least privileges** for access to resources
- Perform annual **data audits**
- Proactively conduct **cyber training and education** programs for employees

Hussain Aldawood, Director of Cybersecurity at GulfNet Solutions, cautions that a solid "self cyber strategy" requires time and investment on the part of an MSP.

One way that MSPs can protect themselves is to **partner with a company specializing in cybersecurity.** They can start building their cyber skills, but should leverage a partner until they get there, since not all MSPs consider themselves cybersecurity specialists.

"If MSPs can't pass a risk assessment themselves, they should not be offering security services," notes Aldawood. MSPs should also consider a multi-layered MFA when dealing with their customers.

"It is worth considering integrating a multi-layer, multi-factor authentication process with clients. Some clients are generally concerned about security. Some are not," offers Aldawood. Unfortunately, cybersecurity doesn't become a concern until something happens. By then, the mess can be very **time-consuming and expensive** to fix.

Aldawood's advice to MSPs is to treat themselves like they do their clients, which means leaning on the adage that it is **easier to protect than to fix**.

"Being vigilant to emerging threats means an MSP can be quick to implement new protection measures which can be used to thwart future attacks," states Aldawood.

MSPs need to **lead by example** and not get complacent when it comes to their own cybersecurity. Following best practices and **partnering with a well-equipped vendor** to cover any cybersecurity holes they can't cover alone will go a long way to keeping everyone safe.

Conclusion

MSPs that are proactive and forward-thinking in confronting constantly changing cybersecurity challenges, embracing emerging technological innovations, and learning the shifting legislative landscape will be well-positioned to emerge from 2021 successfully. There are plenty of software solutions that can serve as partners in the process. MSPs that are able to adapt to serving work-from-home clients and the security challenges they present will also find themselves rewarded with new opportunities and sources of revenue. Here's to an incredible 2021 ahead!

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.

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 the author: Kevin Williams

Kevin Williams is a journalist based in Ohio. Williams authors weekly articles on SmarterMSP.com, focused on cybersecurity and other MSP-centric topics. He has written for a variety of publications including the Washington Post, New York Times, USA Today, Wall Street Journal, National Geographic and others. He first wrote about the online world in its nascent stages for the now defunct “Online Access” Magazine in the mid-90s.

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