Expert Guide

FOR INTEGRATORS AND SOLUTION PROVIDERS

PRESENTED BY Dropsuite

Safeguarding Business-Critical Data

Inside

IDC expects data creation and replication to grow at a 23% CAGR through 2025. Therefore, it's critical for businesses to have the right stategy for protecting, backing up, and storing all that data.

This Expert Guide from *ChannelPro* includes tips for protecting the newest endpoint, Microsoft 365; a report on the rise of alternative backup strategies; a breakdown of the Internet of Things storage issues; and some predictions on storage, cloud, and other markets.

PROTECTING THE NEWEST ENDPOINT: M365

With Microsoft 365 becoming cybercriminals' latest target of choice, you must protect it just like you protect your clients' desktops and laptops.

WELCOME TO THE YEAR OF THE PREDICTABLE

After two strange, surprising years, 2022 is shaping up to be refreshingly easier to handicap in markets ranging from cloud computing and security to storage and beyond.

THE RISE OF 3-2-1 BACKUP ALTERNATIVES

In response to the increased prevalence of ransomware and other trends, alternative strategies to the bedrock principle of back-up are emerging.

SOLVING THE IoT STORAGE CONUNDRUM

Developing a secure storage architecture requires an understanding of how IoT devices work, as well as business requirements, workflow, and data retention needs.

DOCUMENTATION PRO TIPS

Clear, thorough, and well-maintained client documentation leads to repeatable and profitable results.

POWERED BY ChannelPro
WWW.CHANNELPRONETWORK.COM

IoT playbook
WWW.IOTPLAYBOOK.COM

Protecting the Newest Endpoint: M365

With Microsoft 365 becoming cybercriminals' latest target of choice, you must protect it just like you protect your clients' desktops and laptops. By Joshua Liberman

THE GREEK PHILOSOPHER Heraclitus said, "The only constant in life is change."

Flying to my first ASCII event of 2021, I am considering much of what has changed this past year. Writing this on an airline tray feels like a slow return to normal. Wearing my KN95 mask feels a bit less so. In many ways, what has changed the most is the ubiquity of our new Microsoft 365-centric workforce and the high-profile target it has become. This has been the biggest impact we have felt from the plague year, which many of us will look back upon with "2020 vision."

Now in 2021, with its new reality of distributed work, even our most premise-centric clients are really engaging with M365, including OneDrive, SharePoint, Teams, and more. This reality has brought a great shift in focus by miscreants of the web, especially the "more professional" bad actors. M365 has become the target of choice, with impersonation, admin hijacks, and other compromises the wave of the future. M365 has effectively become a new "endpoint" and must be protected just as you protect your desktops and laptops.

While calling M365 an endpoint may sound like a stretch, it is susceptible to compromise, hijack, and data loss—just like a traditional endpoint. That means we must armor M365 as we would any endpoint. Even though nearly every mailbox today is protected by anti-spam software, whether M365 native or third-party products like Mailprotector, Proofpoint, or others, most of those products fall short when it comes to targeted attacks like spear phishing. That's why so many of us also layer anti-phishing products such as those from Avanan or others and engage a security operations center (SOC) to monitor M365 logs. We bundle complete, frequent backups with every M365 seat as well, as so much data lives there now.

Mail Filtering and Anti-Phishing

Until just last year, I was convinced that mail filtering alone was sufficient to stop both "traditional" spam and email-borne malware attempts, including just about any sort of phishing attempt. And then I came a few keystrokes away from falling for a particularly well-crafted spear-phishing attempt that employed impersonation and some data that had most likely been culled from a colleague's social media posting(s). I realized that dedicated anti-phishing was the only answer. To be effective, an anti-phishing solution must do more than scan mail headers; it must deal effectively with impersonation, verify links are safe, and more. That is quite a tall order and one that we have now filled with Avanan, provided through Solutions Granted.

M365 SOC Services

The next step is to attach active monitoring and alerting to your M365 endpoints, much like the endpoint detection and response

ILLUSTRATIONS: BAGIRA22 / ISTOCK

(EDR) protection for your traditional endpoints. There are many clearly malicious actions that can easily be flagged here. For example, logins to the same mailbox from geographically disparate locations close in time (aka "impossible logins") are a red flag. But the creation of global admins, rules that copy or redirect messages to outside addresses, and lateral movement within M365 (to SharePoint, for example), should be noted and alerted as well. And of course, any actions that clear logs are also highly suspect. Having a live set of eyes on your M365 endpoints is critical, and here again, we chose to work with Solutions Granted.

M365 Backup

As we began our transition from premise to hosted solutions such as M365, one of my first concerns was how we were going to back up all this newly "clouded" data. As a traditional MSP, we had developed significant expertise with managing Exchange servers but had always struggled with SharePoint backup, not to mention identifying and securing remote storage. The good news here is that this is far easier in M365, as all this data is effectively in one place. We shopped the market across several vendors and ended up working with Vault America to deploy Dropsuite. It provides frequent data snapshots that cover all the backup bases (OneDrive, Outlook, SharePoint, and Teams), and allows for genuinely easy, highly granular restores.

Vendor Sprawl

Some of you may note that we are weaving together offerings from several different vendors and adding significant costs to our M365 delivery. You might also argue that you can replicate a lot of this by delivering more advanced versions of M365 with advanced threat protection and email archiving, for example. Those are valid points and worth considering. But I would point out that our stack is just three vendors (Microsoft, Solutions Granted, and Vault America) and costs me under $6 per M365 "endpoint" in total, far less than moving "up stack" in M365. This means you can deliver all of this with M365 Business Standard at $20 or so per mailbox or price the bundle at $10 and attach it to any version of M365. While you do have more to manage, I have found the functionality of third-party options to be superior.

Monetizing It

This leads to perhaps the biggest question. How do we sell these services to our clients and make good money doing so? As with all that we do, we sell the cake, not the recipe, and we make sure that we keep the bundle intact both to ensure its efficacy and to maximize the economy of scale we achieve by bundling. We approach M365 as the broad, capable, and complex solution it is, not as a "$5 mailbox in the cloud." We explain what M365 can do for our clients, and stress how important it is to secure and protect that infrastructure. Educating our clients in all that they can do in M365 and its criticality to their operations has made placing this suite for every M365 endpoint we sell much easier. Being able to attach this bundle to any version of M365, even nonprofit, helps too.

Beyond M365

We always strive to address security in a holistic fashion, and the rather sudden shift from premise to cloud and then to work from anywhere (WFA) has only reinforced this. We continue to secure traditional endpoints, the network core, and the newly porous perimeter. But even as we protect against today's threats, we must try to anticipate those that are still below the horizon. The shift to WFA changed our concept of the perimeter, just as cloud has shifted our idea of the network core. As we move forward, new security challenges around desktop as a service, distributed cloud services, and more continue to develop. Protecting the M365 endpoint is critical, but it is only the first step in this journey.

JOSHUA LIBERMAN *is president of Net Sciences, founded in 1995. A 27-year ASCII Group member, former rock climber and martial artist, and a lifelong photographer, Liberman has visited five continents and speaks as many languages. He also writes and speaks in the IT field and raises Siberian Huskies with his wife Heidi, who calls him the Most Interesting Geek in the World.*

WELCOME TO THE YEAR OF THE PREDICTABLE

AFTER TWO STRANGE, SURPRISING YEARS, 2022 IS SHAPING UP TO BE REFRESHINGLY EASIER TO HANDICAP IN MARKETS RANGING FROM CLOUD COMPUTING AND SECURITY TO STORAGE AND BEYOND. BY RICH FREEMAN

LAST JANUARY, forecasting the year ahead in IT seemed like a fool's errand. With a pandemic still raging, vaccines just arriving, and deep economic uncertainty persisting, all anyone could say for sure about 2021 was that it was bound to be better than 2020.

Twelve months later things are different. COVID-19 remains an issue and no one knows quite when inflation and supply chain bottlenecks will ease, but the future looks significantly more predictable than it did the last time *ChannelPro* gazed into its tech industry crystal ball.

In fact, the future looks *so* predictable these days that in fields ranging from cloud computing and security to storage and PCs, our go-to panel of industry experts advised us to expect a lot of what you might predict yourself, with a few new wrinkles mixed in.

ILLUSTRATION: DILOK KLAISATAPORN / ISTOCK

MANAGED SERVICES

Despite—or perhaps because—of the pandemic, 2020 and 2021 were good years for managed services. Gary Pica, president of MSP advisory firm TruMethods, believes 2022 will be even better.

"We're at a point now where almost anyone with less than 250 employees is going to outsource some or all of their services, because they have so much more technology," he says. "There's no going back at this point in the digital revolution."

That bounty isn't flowing equally to everyone, however. MSPs with fine-tuned business processes and proven competitive strategies in the sector's top 25%, Pica reports, are outperforming peers in the bottom 50% by a wider margin than ever before.

"They're adding a bunch of recurring revenue. They've matured their security posture. They're getting $160 to $250 a seat," he says, adding that less advanced peers will have a hard time keeping up this year.

"I'm not suggesting that those small or less mature MSPs are going to go away," Pica says, "but they're going to have to decide more specifically, what is my niche?"

This is especially true because 2022 will be a year of continued M&A activity funded in part by the $2.3 trillion worth of uninvested capital currently held by private equity investors, according to S&P Global Market Intelligence. "Being run by businesspeople, they have dedicated sales and marketing focus," Pica notes of PE firms, which means the big MSPs they're building will be directly targeting customers of smaller MSPs this year.

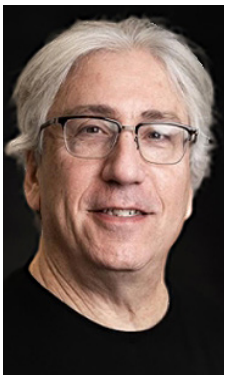
In case that's not pressure enough, MSPs of every size will continue to face tight hiring conditions in 2022, according to Pica. Finding good people was difficult before the pandemic, he notes, but in the work-from-home era technicians can potentially sign on with any MSP anywhere.

"Now you've got to compete with the whole world basically, and definitely the whole country," Pica says.

CLOUD COMPUTING

On the other hand, at least you don't have to compete with Amazon and Microsoft. Google does, which is why Forrester believes the company will fall short of a milestone it once said it would achieve by 2022.

"They expected to be either first or second in the cloud services provider world, and we don't think they're going to make it," says Lee Sustar, a principal analyst at Forrester. The industry heavyweight is adding plenty of users, he observes, but isn't gaining significant share thanks to multicloud procurement strategies—leading companies that buy from Google to buy from AWS and Microsoft as well.



"I THINK WE'LL SEE AT LEAST ONE MORE, OR PROBABLY SEVERAL MORE, SOFTWARE SUPPLY CHAIN TYPE OF ATTACKS."

JON OLTSIK
PRINCIPAL ANALYST, ENTERPRISE STRATEGY GROUP

That's OK, though. There will be more than enough spending to go around, according to Gartner, which sees outlays on cloud services rising close to 22% this year to more than $482 billion worldwide. That's down from the 27% growth recorded in 2021 but still four times the 5.5% uptick that Gartner projects for IT revenue overall this year.

Forrester expects a growing portion of that cloud spending to flow into industry-specific solutions like the Microsoft Cloud for Healthcare and IBM Cloud for Financial Services. "In a heavily regulated industry where a lot of compliance issues come to the fore, the ability to get a set of cloud services with those considerations already in mind can be very beneficial," Sustar notes.

SECURITY

Anticipating what 2022 holds for the security market may be even easier than forecasting the year ahead in cloud.

"I think it will be an active year," says Jon Oltsik, senior principal analyst at Enterprise Strategy Group, dryly. "I see no letup in the threat landscape."

That applies to more than just ransomware too, he adds. "I think we'll see at least one more, or probably several more, software supply chain type of attacks," like the kind that struck SolarWinds a year ago.

The challenges of securing a hybrid workforce in which employees split time between home and office will make matters even worse. "We've already seen increases in the amount of attacks," Oltsik says, adding that a lot of the ensuing breaches result from negligence among remote workers who can be difficult to monitor. Indeed, 84% of organizations surveyed by security vendor Egress last summer had experienced at least one incident caused by human error in the prior 12 months.

On the plus side, Oltsik sees 2022 as the year that channel pros move past desperately patching work-from-home holes. "I think we'll go from a defensive posture to a more offensive posture," he says, in which the goal is to build a hybrid security foundation scalable and manageable enough to endure the next five years.

"It gives creative and aggressive channel partners a great opportunity," he observes.

VENDORS

So, according to Dell at least, does APEX, the as-a-service cloud infrastructure platform the company officially launched last May. "I think you're going to see them push very hard on that," says Bob O'Donnell, president and chief analyst at TECHnalysis Research. "They see the channel as, obviously, an important mechanism for them to get these as-a-service offerings out there."

Microsoft, for its part, will have more than just Azure and Microsoft 365 going for it in the cloud this year, O'Donnell predicts. Though it may not be a breakout hit, Windows 365, the "cloud PC" platform that Microsoft rolled out in 2021, will soon begin transitioning from test deployments to full-scale production.

"It's not for everybody, but there are certain applications, certain environments, where it makes a ton of sense," says O'Donnell, citing call centers and temporary workers as examples.

HARDWARE

Hardware makers reaped even greater dividends in 2021 from continued demand for office and work-from-home PCs. Global endpoint spending (excluding data center gear) was on track to rise 15.1% to nearly $802 billion last year, in fact, according to recent projections from Gartner.

Credit a small part of that sum to Roger Kay, president of analyst firm Endpoint Technologies Associates. He bought a sleek and speedy new notebook late last year. When he's in his home office, he connects it to his 43-inch monitor, mouse, and external keyboard. When he's on the road, he stashes it in his computer bag.

"That, I think, is sort of the ideal rig you want," Kay says. "Big, comfortable, high-performance, and not too expensive when you're in your own environment, and then you want some ability to go to other places."

It's a perfect formula, in fact, for hybrid workers who want to use one current-generation PC both at home and in the office, which is why laptop sales should remain strong well into 2022, Kay adds. In fact, non-data-center endpoint shipments will climb 2.3% this year, according to Gartner.

"NOBODY IN THEIR RIGHT MIND WOULD WANT TO BUY SOMETHING THAT LIMITS THEM TO A SINGLE PLATFORM."

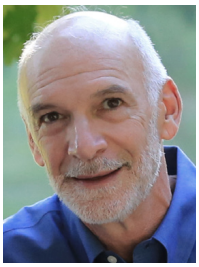
BOB O'DONNELL PRESIDENT AND CHIEF ANALYST, TECHNALYSIS RESEARCH

With employees spending more time in the office but still collaborating with people at home, cloud-connected meeting room devices like Microsoft's Surface Hub should have a strong year too. To realize their promise, O'Donnell notes, digital whiteboards must be capable of running the multiple videoconferencing solutions that most businesses use.

"Nobody in their right mind would want to buy something that limits them to a single platform," O'Donnell says, "and yet you've still got some of these vendors, Microsoft and Zoom in particular, trying to push a single-platform hardware solution for a conference room." Cisco, by contrast, announced plans to add cross-platform compatibility to its Webex hardware last October, and O'Donnell expects that move to yield dividends for the Silicon Valley giant this year.

That's a significant slowdown from last year but a welcome change from the streak of annual sales declines that preceded the pandemic.

Unless, of course, continued chip shortages mar that upbeat picture. "The chip supply is going to be a bit unpredictable," says Kay, who sees something akin to normalcy returning sometime this spring or summer.



ROGER KAY

Assuming chips are available, Kay expects a crop of faster, more power-efficient Windows PCs, inspired in part by the impressive combination of speed and battery life in laptops bearing Apple's M1 processor, to start showing up this year, along with videoconference-optimized desktop monitors that are even "bigger and denser and brighter and more beautiful" than predecessors from 2021.

The only downside to the endpoint picture, in fact, is that once the current purchasing wave is over go out to five to seven for most people because their devices still work," Kay says.

DIGITAL SIGNAGE

There's plenty of hardware involved in digital signage, of course, which means the same product shortages impacting the PC and peripheral markets are impacting purchases of displays and media players as well.

"In conversations with the big distributors and several of the large integrators around the country, they're having to adjust their businesses to the flow of goods coming and the availability," says Alan Brawn, principal of advisory firm Brawn Consulting. "The economic momentum, aka demand, is there and growing but the supply will take some time to catch up."

When it does, he continues, look for pent-up demand to drive brisk sales momentum—or rather, brisk*er*.

"There was still growth of 6% to 8% in 2020 and into the first half of 2021," Brawn says, stemming from pandemic-related sales of health monitoring solutions, traffic control systems, and touchless displays. 2022's even higher spending, he believes, will be spurred by organizations in education, healthcare, and other verticals buying into the digital signage value proposition the way retailers did long ago.

Bigger displays, including dvLED panels, will account for only some of that higher spending, according to Brawn. "It's the behind the scenes—pun intended—things that will drive the opportunities," he says, including analytics and artificial intelligence software that mines digital signage usage records for trends and market opportunities.

STORAGE/BDR

Signage solutions are but one contributor to what will be predictably strong demand for storage in 2022, according to Greg Schulz, founder and senior adviser at analyst firm and consultancy StorageIO. "More data continues to be generated," he notes.

IDC, in fact, expects data creation and replication to grow at a 23% CAGR through 2025. As a result, the analyst predicts, the 6.7 zettabytes of storage capacity in use as of 2020, the last full year for which figures are currently available, will climb at a 19.2% CAGR over the same period. To put that number in context, each zettabyte is a billion terabytes.

> [WITH BDR], "IT'S NOT JUST HAVING MORE COPIES OF YOUR DATA. IT'S ALSO HAVING MORE VERSIONS OF THOSE COPIES AS WELL AS VERSIONS THAT ARE KEPT IN DIFFERENT LOCATIONS."
>
> GREG SCHULZ
> FOUNDER AND SR. ADVISER, STORAGEIO

Despite exploding use of cloud solutions, a lot of that data will reside on premises, and not just in corporate data centers. "We're seeing more storage actually being deployed out at the edge," Schulz says. Research from Gartner confirms that trend. While just 10% of business data was created and processed outside a traditional data center or cloud last year, the analyst says, 75% will be by 2025.

Much of that data will reside on good old-fashioned hard drives, according to Schulz. Though adoption of flash storage, which is faster than disks, continues to soar, HDDs remain a more affordable option for data that isn't used heavily.

"They're better together," says Schulz of flash and disks.

They're also equally vulnerable to attackers and corruption, which is why companies will take BDR even more seriously in 2022, according to Schulz. "It's not just having more copies of your data," he says. "It's also having more versions of those copies as well as copies of those versions that are kept in different locations."

It's a harbinger too—and a predictable one at that—of fresh sales ahead for the SMB channel.

The Rise of 3-2-1 Backup Alternatives

THE 3-2-1 BACKUP PROCESS became the standard decades ago, when companies kept their Novell NetWare server under a table in the break room. The long-standing recommended strategy was to have three copies of everything on two different media, with one copy stored off-site. Lately, however, in response to the rising prevalence of ransomware and other trends, experts are increasingly gravitating toward alternate schemes.

The 4-3-2 strategy (four copies of your data, in three locations, with two of those locations off-site) is what Greg Schulz, founder and senior analyst at the Storage I/O Group, calls "the new school data protection and backup process." The 3-2-1-1-0 scheme (three copies of your data on two different media, with one copy off-site and one copy offline or air gapped, and zero-error recoverability solutions) is another option.

> It may be time to "rethink what, why, where, when, and how data is being protected and for what reason."

GREG SCHULZ
Founder & Senior Analyst, Storage I/O Group

These strategies provide more versions to line up with recovery point objectives, according to Schulz, who suggests it may be time to "rethink what, why, where, when, and how data is being protected and for what reason." The tools available today make it much easier to configure the number and location of copies and vary where they're stored off-site and online, he notes.

"The biggest difference today is your ability to increase the number of versions and retention and adjust the number of copies and where they're located," he adds.

CRS Technology Consultants, an MSP in Cape Coral, Fla., follows the 3-2-1-1-0 strategy most closely, according to owner John Joyce. CRS handles clients with between two to 200 employees. "We're happy the same base technology is now available to all the clients we serve," says Joyce, thanks to the investments cloud backup providers have made.

The ease and affordability of cloud backups give him the flexibility to handle any size customer and let them choose the amount of warm or hot standby infrastructure they prefer. "Our CPA with an assistant can afford a half-day to recover, but the larger clients downtown can't," Joyce notes.

For CRS' clients, backup and a business continuity plan are nonnegotiable. "After Hurricane Irma in 2017," he adds, "no company in Florida argues about backups." He does still have one client, a two-person accounting firm, which demands a tape be stored in a safety deposit box.

Now with the hurricane of malware and ransomware, clients need the best backup and business continuity system possible, says Joyce. "Copies on-site, to the cloud hourly, isolated and replicated, and test, test, test."—*James E. Gaskin*

Solving the IoT Storage Conundrum

Developing a secure storage architecture requires an understanding of how IoT devices work, as well as business requirements, workflow, and data retention needs. **By Samuel Greengard**

THE INTERNET OF THINGS requires significantly different hardware and infrastructure than conventional IT, and nowhere is this more apparent than for storage. "The IoT spreads computing across the network and it often includes large and widely distributed datasets," states George Crump, president and founder of analyst firm Storage Switzerland.

Organizations that gloss over IoT storage may find themselves dealing with latency issues and other performance problems. They may also find themselves swimming in useless data and unable to pinpoint the data they require when and where they need it. Finally, they could face new security challenges and higher overall costs.

Yet, for channel pros and others engineering and configuring IoT systems, it's not as simple as tossing cloud storage and edge networks at the IoT data challenge. "There are important issues that an organization must address in order to get the most out of the IoT," says Greg Schulz, founder and senior analyst at The Storage I/O Group.

Connections Count

A starting point for navigating IoT storage is to recognize that IoT solutions generate vast volumes of data. However, not all data is created equal and not all data storage requirements are the same. IoT data often resides outside a traditional data center and includes many file types and sizes. "The IoT is a multi-dimensional environment," Schulz explains.

It's important, then, to understand how smart connected devices change storage requirements. In some cases, it's necessary to store data on a device such as a vehicle or industrial machine, utilizing onboard flash storage and transferring the data periodically through batch uploads. In other cases, it's better to process and store data on an edge server. In still other scenarios, data must reside in the cloud or on a conventional data center server. Sometimes it's a combination of all these approaches and more. "You really have to understand the way IoT devices work, business requirements, where applications exist, and how data needs to flow," Schulz says.

> "IoT storage is a more complex framework than traditional IT."
>
> **GEORGE CRUMP**
> President and Founder, Storage Switzerland

Moreover, as 5G streams into the picture, new and different IoT frameworks will take shape. "Connections impact IoT data storage significantly," Crump says. For instance, he says, 5G "is likely to reduce capacity requirements at the extreme edge and move the storage upstream to an edge data center."

A Better Way

Every IoT storage framework must ultimately address the *volume, variety*, and *velocity* of data (how much data is generated and used, the types of data that exist, and how fast those different types move about). A focus on the data lifecycle—how it is used from creation to deletion—is also paramount. "Storage cannot be architected in isolation [from data requirements]," Crump explains.

For instance, data retention policies must be taken into account. And it's especially important to consider how different configurations and storage frameworks impact security and data privacy issues.

It's also essential to build an affordable storage framework that can adapt and scale without disrupting business processes. In order to do this, an organization must understand how, when, and where data is needed to handle various tasks. Schulz suggests working with clients to identify business needs. This helps define how best to map applications and workflows to appropriate storage tiers—and determine where processing and storage should take place.

Finally, make sure to address key security issues, including whether data should reside on a sensor, device, system, or hard drive; whether it should be encrypted; and whether a storage device is exposed to physical theft or intrusion. The task is complicated by the distributed nature of the IoT. "You have to understand how many copies of the data exist, how data travels across a network, and what regulatory standards might apply," Schulz explains.

To be sure, the storage challenges related to the IoT translate into an opportunity for channel pros. Concludes Crump: "IoT storage is a more complex framework than traditional IT. A flexible, agile, and secure IoT storage framework can ultimately generate value for clients and unlock new business opportunities."

SAMUEL GREENGARD, *a business and technology writer in West Linn, Ore., is the author of* The Internet of Things *(MIT Press, 2015) and* Virtual Reality *(MIT Press, 2019).*

PRO DOCUMENTATION TIPS

Clear, thorough, and well-maintained client documentation leads to repeatable and profitable results.

BY JAMES E. GASKIN

WHETHER YOU CALL IT documentation, standard operating procedure notes, or How To Do X, written guidelines that direct employees on proper processes are the mark of an MSP on the way up. "Good documentation is the foundation of success, increased productivity, and profitability," declares Adam Bielanski, former MSP and CEO of the Sierra Pacific Group, a managed services and IT consultancy.

Yet Todd Kane, president of Evolved Management Consulting, says many MSPs he works with are lacking in this area. "Eighty percent may have something they call a documentation system, but it's unstructured, noisy, and not used much, except maybe for passwords," he says. "Maybe only 20% have good documentation practices."

If your business falls into that category, consider the following best practices for maintaining complete and useful documentation.

Why Do It?

Creating solid, well-maintained documentation is the only way to scale an MSP business, because it reduces the number of hats the owner must wear. And if you're interested in one day selling or merging your MSP company, the better your documentation is, the easier the process.

"A good documentation platform reduces the use of tribal knowledge in your organization," says Kane. "Project documents lower your cost of labor for the same amount of work, reduce complexity, and increase productivity."

It's also the easiest way to hold people accountable. If your core values and/or processes are written down, it's clear when they are violated, adds Allen Edwards, founder and president of Eureka Process, an MSP coaching and consulting company.

Edwards calls documentation a "recording of decisions made" on processes to follow in every part of an MSP's business, including time tracking, client tickets, onboarding, and more. For MSPs looking to get to the next level, and for each step up thereafter, the first hurdles are process and documentation. A well-defined process must be documented to create a consistently positive result.

The idea of defining and documenting ev-

ILLUSTRATION: MYKYTA DOLMATOV / ISTOCK

ery process is akin to eating better and exercising more—everyone knows they should do it, but life often gets in the way. For channel pros, days are hectic and full already. Does documentation really make a difference?

It does for Craig Pollack, founder and CEO of FPA Technology Services in the greater Los Angeles area, now in its 31st year. His boutique MSP focuses on long-term relationships by doing more things for fewer clients, and his staff of 22 supports 65 or so clients. "Documentation is so big for us, it's one of our core values," he says.

FPA documents anything and everything, from presales conversations through every user and network device. "Clients have said they hired us because they knew we had lots of documentation, so if their account manager left, it would be only a blip to them," and not an exercise in reeducation, says Pollack. "New engineers praise our docs and pick up our processes quickly."

When creating documentation, try to hit the sweet spot between too little and so much that employees won't read it, Bielanski advises. "Focus on the action that needs to happen, and why the process is important." Drill down to specifics where necessary for techs, he adds, but not for managers and executives who don't need that level of detail.

For Edwards, less is more, but you must know your audience and what they're doing. If your techs have been trained on a tool, the docs don't require step-by-step instructions with screenshots. "Firewalls, for instance, need 10 to 20 serious details out of the thousands available," he notes. Provide information that's necessary and sufficient, he adds, and edit each document until you get that result.

Bielanski prefers documentation that includes written and video instructions where possible. "Some people are readers, some prefer videos." He also recommends revising documentation when needed.

How to Get Started

Beginning a documentation project can be daunting for everyone involved. For starters, finding time is always a problem, even when you have great intentions, because documentation often falls into the "important but not urgent" category.

Another hurdle is letting perfect be the enemy of good, adds Kane. People have an idea of awesome documentation, so it holds them back. "Even a bullet list with basic information is a perfectly good place to start," he says.

Assign the subject matter experts in each department to craft the documents for their core area, suggests Bielanski. "Find a documentation champion in each area, like sales, service, and finance."

Give employees time to plan and write documentation too, adds Kane. "If you say, 'Hey, can you guys please document the client environment,' managers will get frustrated quickly with the lack of response," he says.

> "Good documentation is the foundation of success, increased productivity, and profitability."

ADAM BIELANSKI
CEO, Sierra Pacific Group

Changing company culture to one that values excellent documentation requires getting techs on board. Try providing some group training for your managers, and even offer bonuses to techs who spend time on documentation.

Unfortunately, some employees will still balk. Edwards describes it as an 80/20 issue but breaks it down to 80/10/10. "About 10% will hate it, period, and won't work with the program. The other 10% will come around when they see the others leave," by choice or not.

Whether their issue is creating the documentation, filling out action reports, or refusing to follow the written directions, Edwards says, "you can't let them wear you down. Managers have to actually manage."

Kane suggests you treat documentation like a project, train employees on why it's a good idea, and show how it benefits them directly as well as how it helps others. "Communicate how you'll measure them, then measure them against that level of behavior," he adds. "If one hasn't logged into the document system at all, that's a problem. Be clear that if they're not using documentation, they aren't doing their job."

What you use for a "documentation system" can vary. Kane prefers IT Glue because he was one of the original testers when he worked at the company that created it. "Hudu is another player, and we also use PowerShell scripts, shared utilities and scripts, and supplemental tools like Network Glue."

Pollack uses IT Glue too, along with Teams and SharePoint. His system gives every customer their own folder with defined docs in the same order across all clients.

Bielanski combines IT Glue with a recorded video version, usually created in Loom.

Mistakes to Avoid

Even though Pollack keeps documentation front and center, he still experiences mistakes due to failure to update documents in a timely manner. "Most of the time, they're just inaccuracies, like a network diagram from 18 months ago," he says. He makes sure techs have time during a project to update client documents or gives them time after the ticket closes. "You have to build in time for documentation, and not just push more tickets."

Another mistake, according to Bielanski, is creating documents but not testing the processes described. "A service manager will assign the project to a tech but doesn't take the time to think things out or outline the goals before the writing starts," he explains. His clients find it wrenching when they come to grips with the fact that they have no good documentation because they have no clear definition of each process and the best way to perform the task.

The worst mistake, though, is not doing anything, says Edwards. "Get started and keep going, no matter how slow. At least it's better than doing nothing."

READER ROI

- **THOROUGH, UP-TO-DATE DOCUMENTATION** is key to a channel pro's scalability, productivity, and profitability.
- **START WITH** a well-defined process, then put it in writing or video, finding the right balance between too much and too little detail.
- **TREAT DOCUMENTATION** like a project, train employees on why it's important, and monitor and measure their use of it.

PRESENTED BY

Dropsuite

Dropsuite is a cloud software platform enabling businesses and organizations globally to easily backup, recover and protect their important business information. Dropsuite's commitment to advanced, secure, and scalable cloud technologies keeps them at the forefront of the industry and makes them the preferred choice of leading IT Administrators and Service Providers globally.

Find out more at dropsuite.com.