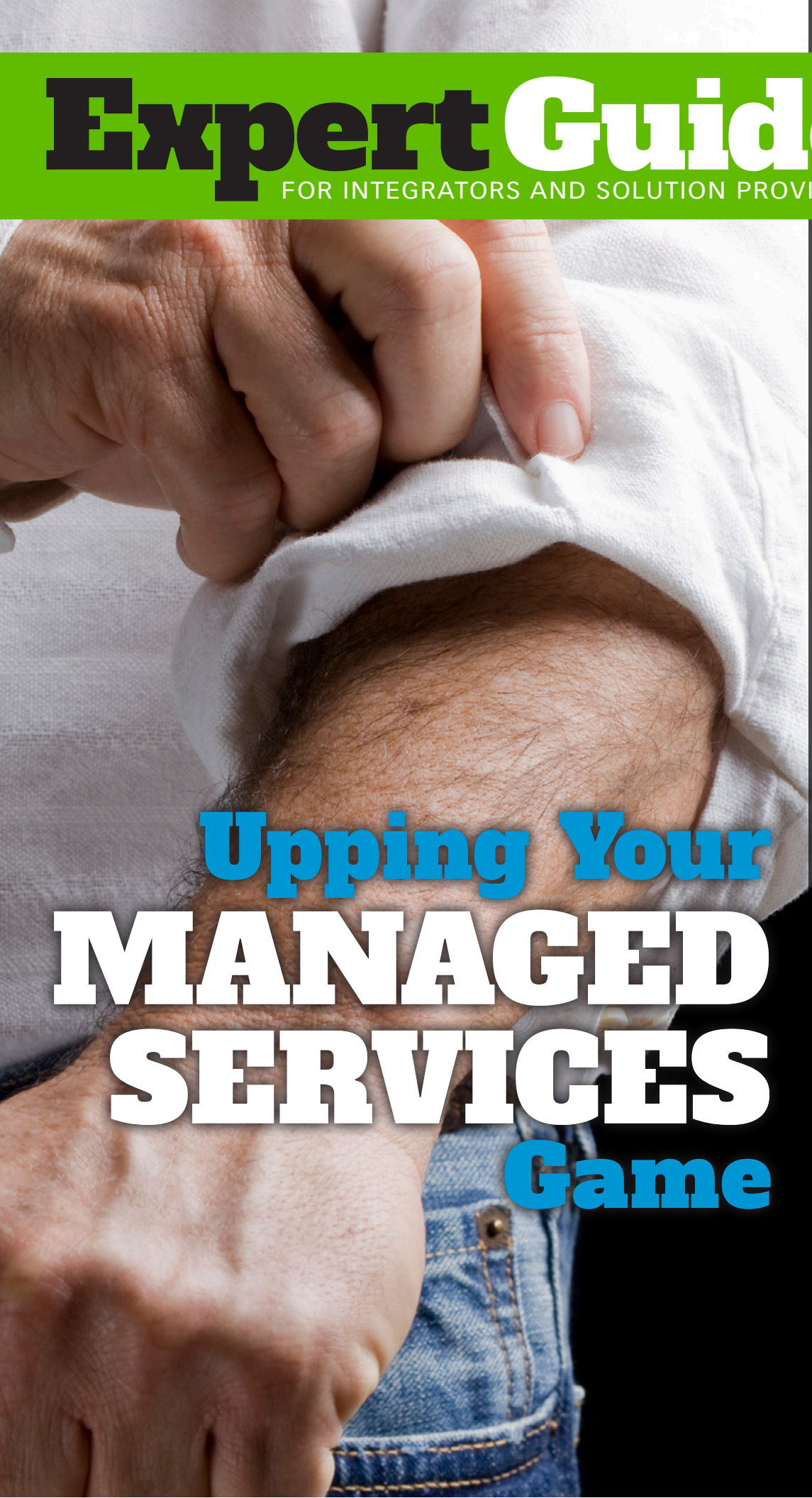
Expert Guide

FOR INTEGRATORS AND SOLUTION PROVIDERS



Upping Your MANAGED SERVICES Game

Inside

2020 has been a year of unique challenges for small and medium businesses and the IT solution providers who have helped them pivot to a remote work model during the pandemic. While it remains to be seen what the "new normal" workplace will look like, it's clear that cloud, cybersecurity, and the Internet of Things will be key factors enabling the new environment.

This Expert Guide from *ChannelPro* will walk you through what you need to up your managed services game heading into 2021, such as developing cloud solutions, offering managed security and managed IoT services, plus why you should standardize to increase efficiency. In addition, one of your peers, BeckTek's Scott Beck, shares how he helps customers understand that cybersecurity is business-critical.

MAKING A CASE FOR MANAGED SERVICES STANDARDIZATION
By Colleen Frye

THE CLOUD SOLUTION RECIPE FOR CYBERSPACE SUCCESS
By Rich Freeman

WHEN SECURITY AND MANAGED SERVICES MEET
By Rich Freeman

MANAGED IoT SERVICES—THE NEXT FRONTIER
By James E. Gaskin

PEER TO PEER: TURNING YOUR MIC ON
By Scott Beck

POWERED BY ChannelPro
WWW.CHANNELPRONETWORK.COM

IoT playbook
WWW.IOTPLAYBOOK.COM

MANAGED SERVICES STANDARDIZATION

MAKING A CASE FOR

Embracing standard processes, tools, and solutions is the foundation for scaling your business. By Colleen Frye

TALK TO PROFITABLE, fast-growing MSPs and you're likely to find that they're serious about employing standard processes, using standard tools, and selling standard solutions. Why? It increases efficiency, deepens expertise, and makes scaling the business easier.

"Whenever you can standardize, you simplify the business," says Daniel Wang, chief automation officer at Intelligent Technical Solutions, a managed service provider serving the Las Vegas, Phoenix, Los Angeles, and Chicago areas. "You make it easier for employees to follow, and you have that [economy] of scale."

Lack of standardization is why so many MSPs struggle to grow, says Wang, who is also CEO of startup MSPbots, a Chicago-based robotic process automation (RPA) company. "They just keep fixing the same problem over and over," he says.

They also make that process harder than it needs to be. Consider a flow chart for solving firewall problems, says Paul Dippell, CEO of Service Leadership, a consulting and benchmarking firm serving IT solution providers. "If all your customers have Cisco firewalls, that flow chart and everything downstream in your operation from that flow chart is all the same." Add a second firewall, and your flowchart doubles in complexity.

In addition, MSPs that support a hodgepodge of hardware and software often need more staff, and higher-skilled, higher-paid ones at that, to meet SLAs, Dippell says. "They do solve more of the huge number of problems coming in because they get smarter people. So customers are happier, the employees are happier … but they go broke." This usually leads them to standardization, he says.

There are hurdles to embracing standardization. "It's hard because you have to find what really works," says Michael Kahn, founder and executive partner at PCDataNet, a managed service provider in Elgin, Ill.

The IT industry's speed of change is a hurdle too, Wang says. After you've defined a process, made sure it works, and trained employees to follow it, your RMM or PSA vendor may release a new version and you have to start over, he explains.

Enforcing the Rules

According to Dippell, MSPs are often hesitant to dictate to clients what tools to use or force them to change out equipment. Overcoming that reticence is essential, though.

"Imagine you allow the customer any brand of laptop, any brand of desktop, any brand of server, any brand of firewall, any brand of router," he says. "The number of different processes you'd have to write is effectively infinite. The best practice is rabid, disciplined, exceptionless standardization of the hardware and software the customer runs."

ILLUSTRATION: AMITITUS / ISTOCK

This can be a difficult conversation for MSPs, Dippell says, but the key is helping customers understand the value to their business as well as the risk the MSP is assuming in providing service for one flat fee—whether an issue takes 20 minutes to resolve with a low-cost employee or many hours with a highly skilled technician. "[The MSP is] taking all of this operating risk off of you. The quid pro quo is you run the equipment I tell you to run."

Wang doesn't hesitate to deliver that message. He's signed up clients who literally just bought a Cisco switch or $2,000 firewall not included among his standard solutions. He'll support that equipment in the short term, or help the customer sell it on eBay, but is willing to walk away if the customer will not move to the standard stack. "We're not 100% everything standardized, but that's what we strive for," Wang says. "We don't want the technician to learn five different kinds of firewall."

PCDataNet, for its part, moved to standardized offerings as part of its relaunch last August to a managed services model, Kahn says. "Our clients had everything and anything. People were picking and choosing what services they wanted, and that ended up over the years causing a lot of frustration," he says, adding that managing a variety of technology "prolongs the time that it takes us to help them."

Now Kahn offers customers two options for each offering, and although he won't refuse to support an alternative if the client insists, he does try to sway them toward the standard stack. "We let them know we've taken a … deep dive as to which of these vendors are truly the best, and that's why these are the ones that we put in our offerings."

Standardizing Your Own Tools

MSPs need to standardize their own internal tools as well, particularly if they have acquired companies that may be using a different RMM or PSA, for instance. With one set of applications, "they can move employees from function to function without having to train them on a different set of tools," Dippell says.

He recommends a quick, though painful, surgical approach to standardizing disparate tools rather than drawing the process out. "It's not hard to find an MSP that's four or five years into standardizing their tools and not done," Dippell notes.

> "The best practice is rabid, disciplined, exceptionless standardization of the hardware and software the customer runs."

PAUL DIPPELL
CEO, Service Leadership

Importance of Documentation

A critical aspect to standardization is documentation. "If there is no documentation, it did not happen," quips Kahn, who was responsible for over 400,000 desktops and 22,000 servers when he worked at a telecommunications company. He applied the lessons he learned about processes there to PCDataNet and worked with his team to refine them. "We document everything."

He uses both IT Glue and Liongard to do so, and refers to them as "living documents." He explains, "Technology's constantly changing and we need to make sure that we also are changing as things progress."

Even with documentation, sticking to a standardized process depends on top-down buy-in and vigilance, Wang says. Whenever there's an issue, first determine if it's a standard operating procedure (SOP) problem or a people problem, he adds. If it's an SOP problem, the process may need to be updated or simplified. If it's a people problem, management needs to educate staff on the importance of following process.

Humans are humans, though, so Wang recommends identifying and automating repetitive processes through scripting. "Because once you automate it, it's almost 100% accuracy."

Kahn, a longtime scripter himself, agrees. "I have found that usually if you can fix one machine, you can fix many. And if you were to write your scripts in such a way that you can correct the issues, you're saving your company a lot of money by not having to rely on one of your engineers or a network technician to manually run through the steps."

Wang's startup firm MSPbots is creating bots using RPA to automate rules-based processes in the ConnectWise Manage PSA platform initially, with plans to add more bots over time. For example, a bot would do things like prompt an employee to enter their time immediately, attach an agreement to a ticket, or search an internal wiki for more information.

While bots may be the future, MSPs who want to simplify business processes and boost efficiency and profits can—and should—get started with standardization now.

READER ROI

MSPs WHO EMBRACE STANDARDIZATION increase efficiency, deepen expertise, and scale their business more easily.

START BY STANDARDIZING the hardware and software your customers run plus the tools you use yourself, and try to minimize exceptions.

DOCUMENT EVERTHING and maintain vigilance in continually evolving documentation as processes change and ensuring that employees are following processes.

THE CLOUD SOLUTION RECIPE FOR CYBERSPACE SUCCESS

Want to make money in the cloud? Think solutions, not products. By Rich Freeman

CHRIS PLOESSEL is a big-time Amazon Web Services partner who generates a lot of revenue reselling that vendor's applications and infrastructure.

Profit? Not so much.

"It's almost more of a burden than it is a benefit," says Ploessel of selling AWS licensing. "We make very low margin on it."

That hasn't stopped RedNight Consulting, the Aliso Viejo, Calif.-based cloud service provider he heads, from making plenty of money, though. To the contrary, the company has been growing steadily since its founding in 2015 and routinely clears 30% to 40% margins on its offerings. The key is that those offerings are cloud *solutions* built on top of AWS products rather than cloud products alone.

Indeed, as many channel pros know all too well, simply selling Office 365 licenses and maybe a little Microsoft Azure capacity is a dead-end street financially. Blending several such products and adding services to the mix, by contrast, is a recipe for durable cloud success. And you don't have to reinvent your business overnight to get started.

Cookie-Cutter Profits

Almost any kind of software product an SMB might require is available in the cloud these days. A cloud solution combines one of them with complementary systems and proprietary expertise. The simplest examples bundle an

anchor product, like Microsoft's Windows Virtual Desktop (WVD) offering, with Azure Active Directory services, security, backup, and ongoing remote management. Ploessel, who sells Amazon Workspaces to clients rather than WVD, has found a virtual desktop deal to be a good source of follow-on projects too. "Everything else just rides on its coattails," he says.

Providing SaaS migration services is another easy starter solution. Every first-time Office 365 adopter needs help configuring applications, moving data into the solution, and getting user accounts established. Vendors like BitTitan and SkyKick make affordable tools that automate much of that effort, so the work is generally very simple. At $100 a seat or so, it's also very profitable, and you can supplement it with end-user training.

Migrating on-site server workloads onto infrastructure-as-a-service platforms can be even more lucrative. So-called "lift and shift" projects require a great deal of assistance with tasks like needs analysis, asset inventorying, cost planning, and security. "Every customer we talk to is interested in getting out of their on-premises stuff," Ploessel says. "The migrations themselves, if you have the right toolsets, are pretty simple."

Business process optimization (BPO) solutions are generally more demanding and therefore more profitable still. Such engagements typically address a business (as opposed to IT) problem, require knowledge of a customer's strategic goals and pain points, and involve expertise that goes well beyond installation and migration.

Kicking them off, however, can be as easy as asking clients which of their workflows cause the most headaches, according to Ro Kolakowski, founder of 6th Street Consulting, a Microsoft SharePoint Online specialist based in Redondo Beach, Calif. More often than not, the answer is an approval process of some kind involving a paper form that makes its way from one employee's desk to several others.

"Nobody knows where the piece of paper is," Kolakowski says, adding that digitizing that process in SharePoint often takes just a few hours. "It's a cookie-cutter solution for us, and that's why we end up with a very high margin." Not to mention a procession of further, potentially even more revenue-rich, workflow solutions.

"We're able to put this together in one to two hours, and they're very happy," Kolakowski says of that first effort. "They start showing the other departments, and the other departments come to us, and sometimes their needs are much more complex than one or two hours."

RO KOLAKOWSKI

Eric Long, president of TeraCloud, a Dallas-based provider of managed online solutions, has had similar success with BPO projects, despite the extra effort they typically require up front. "Those are very, very long sales cycles, but we're immediately talking to the C-level people," he says.

New Skills, Different People

Knowing how to talk to C-level executives is a critical part of delivering cloud solutions effectively. Selling cloud solutions is a consultative process best performed by people who are comfortable communicating with business leaders in nontechnical terms and good at translating business needs into language that engineers and developers understand. You'll also require engineers and developers with the know-how to build solutions that meet those needs.

"It's a totally different skillset," Long notes.

Acquiring all those people isn't easy. The quickest, but also costliest, answer is simply hiring people with an established cloud computing resume. Alternatively, you can recruit people with basic technical know-how, good customer service habits, and an eagerness to learn, and then turn them into cloud solution specialists over time. That's a longer undertaking, but also less expensive and more likely to produce employees who consistently follow your firm's preferred way of doing things, versus whatever they learned elsewhere.

"We're trying to train from within and find the right type of person [who] has that understanding of business automation," Long says.

A third option is to partner with companies that already have the skills you need rather than cultivate talent internally. So long as you work with trustworthy firms and establish clear rules about revenue sharing, client poaching, and other issues in writing, this can be the fastest and most cost-effective strategy of all.

"A lot of times, VARs or MSPs are afraid to get into this," Ploessel notes. "We've had great luck partnering with folks."

Still, offering cloud solutions isn't without risk. If your team continually has projects to work on and customers to support, you can make a lot of money. If they don't, you can lose a lot of money. Moreover, cloud billing schemes are consumption-based, which means the amount your clients end up paying each month can be hard to predict. Some customers can handle that lack of predictability, but others can't. Some may even refuse to pay bills that come in significantly higher than anticipated.

"If you're doing $20, $30, $40, $50,000 with a client and they default, you're on the hook, and that's a big deal," Long warns.

That hasn't stopped him from betting his entire business on cloud solutions, though. "It's highly profitable," he says.

READER ROI

- **CREATING CLOUD SOLUTIONS** that combine multiple products with proprietary services is far more profitable than reselling cloud products.
- **SAAS MIGRATIONS**, server workload "lift and shift" projects, and business process optimization are three of many cloud solution examples.
- **SUCCESS IN CLOUD SOLUTIONS** requires salespeople who understand business needs and technologists who can translate those needs into finished deliverables.
- **CULTIVATING SUCH PEOPLE** from within is often more cost-effective than hiring outside experts.
- **PARTNERING WITH OTHER CHANNEL PROS** is also an option, provided you define clear guidelines in writing.

WHEN SECURITY AND MANAGED SERVICES MEET

Managed security is a high-margin opportunity for those with the skills and tools to provide it. By Rich Freeman

COULD THERE BE A BETTER PLACE to be in IT right now than the intersection of managed services and security?

Indeed, while sales of security hardware, software, and services will climb at a 9.4% compound annual growth rate through 2023 to $151.2 billion, according to IDC, sales of managed security services will grow at an even better 13.9% CAGR during that same period from a base of $21 billion last year.

The margins on managed security, which can easily top 65%, are pretty good too. "It's incredibly lucrative," says Angela Hogaboom, CEO of Ocular, a solution provider with specialized security and compliance expertise in Denver.

Ready to get in on that? Be prepared, experts say. You may be an MSP and you may offer security services, but that doesn't necessarily mean you're in the managed security business.

Providing Confidence

Definitions vary, but most channel pros with experience in the field agree that a true managed security offering is a multilayered package of sophisticated, subscription-priced services that combine to help clients assess their needs, protect their data, detect attacks, and respond to breaches. Steep profits aren't the only payoff, either.

"Even more important to me, coming from the MSP space, is the stickiness that you get with your clients," says Scott Beck, CEO of BeckTek, an MSP and advanced security provider in Riverview, New Brunswick (see page 22 for more on how Beck established himself as a security expert). "When you get those solutions in, and they get used to it and you get their staff trained around it, you become almost irreplaceable."

SCOTT BECK

Most providers sell managed security plans separately from their core managed IT service bundles. Many let customers choose from a menu of basic, intermediate, and advanced tiers.

Included in those options, typically, is a mix of behavior-based endpoint protection software, next-generation firewalls, spam and DNS filtering solutions, email and network security protection, an endpoint detection and response system, two-factor authentication, BDR, and a dark web monitoring service that alerts you when a client's credentials have been stolen. Vulnerability assessments that identify gaps in a customer's defenses, security awareness training that teaches end users to recognize phishing scams, and cyber-insurance policies that lessen the financial impact of successful attacks usually factor into the package as well.

So do remote monitoring and support from a professionally staffed security operations center (SOC). Building a SOC can cost million however, and staffing one with experienced a alysts is expensive. As a result, most manage security providers partner with an outsource SOC vendor. That's something Joshua Libe man, president of Albuquerque, N.M.-base MSP and system builder Net Sciences, wou do even if it wasn't more cost-effective.

"I just don't see, even if the money wa there to do it, that it provides me significa benefits over dealing with people who a truly expert [and] who can analyze millions data points when we can only analyze tho sands," he says of operating his own SOC.

Successful managed security provide apply that thinking beyond just the SOC. " you need to Google how to do somethin a pretty good general rule of thumb is th maybe you should consider outsourcing it Hogaboom says. Your margins will dip som but your clients will be safer, and therefo happier with you.

"Having trusted partners who can provic those services, with you acting as an inte mediary, actually is very helpful with provi ing that sort of confidence to your clien that you have people who are being proa tive," Hogaboom notes.

Playing Quarterback

Hogaboom and others, however, cautic against outsourcing absolutely every sec rity function you perform. If all you're doir is passing along someone else's service

"IF YOU NEED TO GOOGLE HOW TO DO SOMETHING, A PRETTY GOOD GENERAL RULE OF THUMB IS THAT **MAYBE YOU SHOULD CONSIDER OUTSOURCING IT.**"

ANGELA HOGABOOM
CEO, Ocular

you're not adding much value of your own, and if you're not adding value of your own, you're vulnerable to losing customers to competitors with greater skills or cheaper rates. Any task that involves face-to-face contact in particular, Hogaboom advises, should come straight from you.

Another word of advice from managed security veterans: Don't promise more than you can deliver. No one can provide perfect protection. Tell your clients that you will reduce their exposure to threats and decrease the impact of any attacks that get through.

"You just have to be aware that you're playing a higher-stakes game," notes Liberman.

To further protect your hand in that game, many managed security pros counsel, resist the temptation to white-label your security bundles. Honesty is usually the best policy when it comes to crediting your technology partners, unless you don't mind taking all the blame when one of those vendors makes a mistake. Rather

"YOU JUST HAVE TO BE AWARE THAT YOU'RE PLAYING A **HIGHER-STAKES GAME.**"

JOSHUA LIBERMAN
President, Net Sciences

than exaggerate your capabilities, tell your customers that you're the quarterback of a carefully assembled team of the industry's most elite cybersecurity service providers.

Eating your own dogfood, as the saying goes, is a good first step in launching a managed security practice. MSPs are under constant attack these days from cyberthieves hungry for end-user credentials and other data in RMM and PSA systems. You can simultaneously protect yourself from that threat and familiarize yourself with the security products you'll be selling by deploying them at your own company first.

Consider becoming SOC 2 certified as well. Complying with the SOC 2 data management standard, and completing a third-party SOC 2 audit, will not only help you serve customers better but also give you a leg up over competitors when pursuing new clients. Better yet, SOC 2-compliant MSPs can charge more.

Finally, do exactly what you should be telling your customers to do, and for the same reason: Buy a good cyber-insurance policy to shield yourself from potentially devastating expenses should your systems be compromised. The return on that and other investments will be worth it, according to Hogaboom.

"No two clients are the same and no product set is the same, and the solution is customized every time," she says of managed security. "There's always something to offer."

WHAT'S IN A NAME? MSP VS. MSSP

IN THEORY, a managed service provider (MSP) that offers security services can rightfully call itself a managed security service provider (MSSP). Though opinions vary, however, many experts agree that providing a managed security service is not the same as being an MSSP. Unlike most channel pros, MSSPs provide 24/7 log monitoring and analysis via an in-house SOC. Only large MSPs and IT providers that do nothing but security, generally speaking, can afford a SOC of their own. For that very reason, partnering with an MSSP makes good sense for most managed security providers.

READER ROI

- **MANAGED SECURITY** is a rapidly growing, high-margin opportunity for MSPs, but entails more than just anti-virus and firewall services.
- **A TYPICAL MANAGED SECURITY OFFERING** includes a mix of subscription-priced services for assessing needs, protecting data, detecting attacks, and responding to breaches.
- **MOST MANAGED SECURITY PROVIDERS** outsource especially sophisticated and expensive functions like maintaining a SOC.
- **AVOID WHITE-LABELING** outsourced services, though, unless you're prepared to take the blame for a vendor's mistakes.

Managed IoT Services—the Next Frontier

Now may be a good time to get in on the ground floor of building a managed services business around IoT solutions. **By James E. Gaskin**

DESIGNING AND DELIVERING IoT solutions can be a lucrative source of project revenue. Managing IoT solutions, or operating them on an outsourced basis, can be a rich source of *recurring* revenue. It's a business model MSPs are already familiar with, but managing the billions of IoT devices currently installed and planned is an even bigger job than managing a traditional IT network. Does it make sense to start your IoT MSP practice?

For MSP Mike Bloomfield, it does. The president geek of Tekie Geek, based in Staten Island, N.Y., is offering both business and residential IoT management services. For his business clients, he says, there is some overlap with the types of services MSPs typically offer, such as managing Wi-Fi access points. (For more on Tekie Geek, see page 22.)

Jack Knocke agrees. "In many cases, IoT management means working with the same types of devices [MSPs] typically work with," say Knocke, president of IoT Advisor Group in Jacksonville, Fla., which helps IoT vendors take their products to market.

One big difference, though, is IoT projects often fall into the operations technology basket, not IT, which requires a different approach than selling a PC, according to Knocke. "Integrators are comfortable justifying new PCs for customers. IoT projects get into business questions and the operations side, and those talks make some integrators uncomfortable."

A good way to get started with IoT management is to work with existing customers as they start doing IoT projects, Knocke suggests. For example, the plumbing company with your VoIP system is a good candidate for fleet management to track its trucks.

> "Owners of 5,000 to 6,000 square foot homes are more likely to pay for everything to be done for them. They want to know the TV will work."

MIKE BLOOMFIELD
President Geek, Tekie Geek

Be aware, though, that additional management tools and training will be required, Bloomfield says. "Go through whatever training your vendor offers. I take the training myself and train my nine employees."

Tekie Geek uses an RMM tool from Kaseya for his managed services customers, and he's testing the Domotz RMM for IoT devices. "Domotz made IoT monitoring very easy," Bloomfield says. He has also used OvrC RMM on-premise hubs, which are a one-time cost vs. a monthly fee for Domotz, "but don't give you the same amount of power."

Is the profit potential worth the extra tools and training? Yes, says Bloomfield.

"IoT is still new, but we're making money, backing IoT support into the cost," he explains. "We sell some equipment but at a lower margin level like for Sonos [home sound systems]. Hardware automation controllers are better, with enough margin on the back end. For businesses, IoT monito ing becomes part of the workstation cost fo other devices."

For residential clients, Bloomfield rec ommends sticking to high-end homes. Whil some competitors might service homes fo $10 a device per month, "they lose mone with one service call." In contrast, he says "Owners of 5,000 to 6,000 square foo homes are more likely to pay for everythin to be done for them. They want to know th TV will work."

Pricing your services correctly is key t profitability, Knocke says. "If you price it ap propriately and support it the right way, Io monitoring can be extremely profitable. A $5 per month you'll have to sell thousand to make it work, but if you look at your cost and service time you put into it, it's simila to your MSP model."

He adds that once you have an IoT gate way in place, you can do all sorts of IoT pro ects. "Your car, your forklift, and your HVA systems are now IoT management ready."

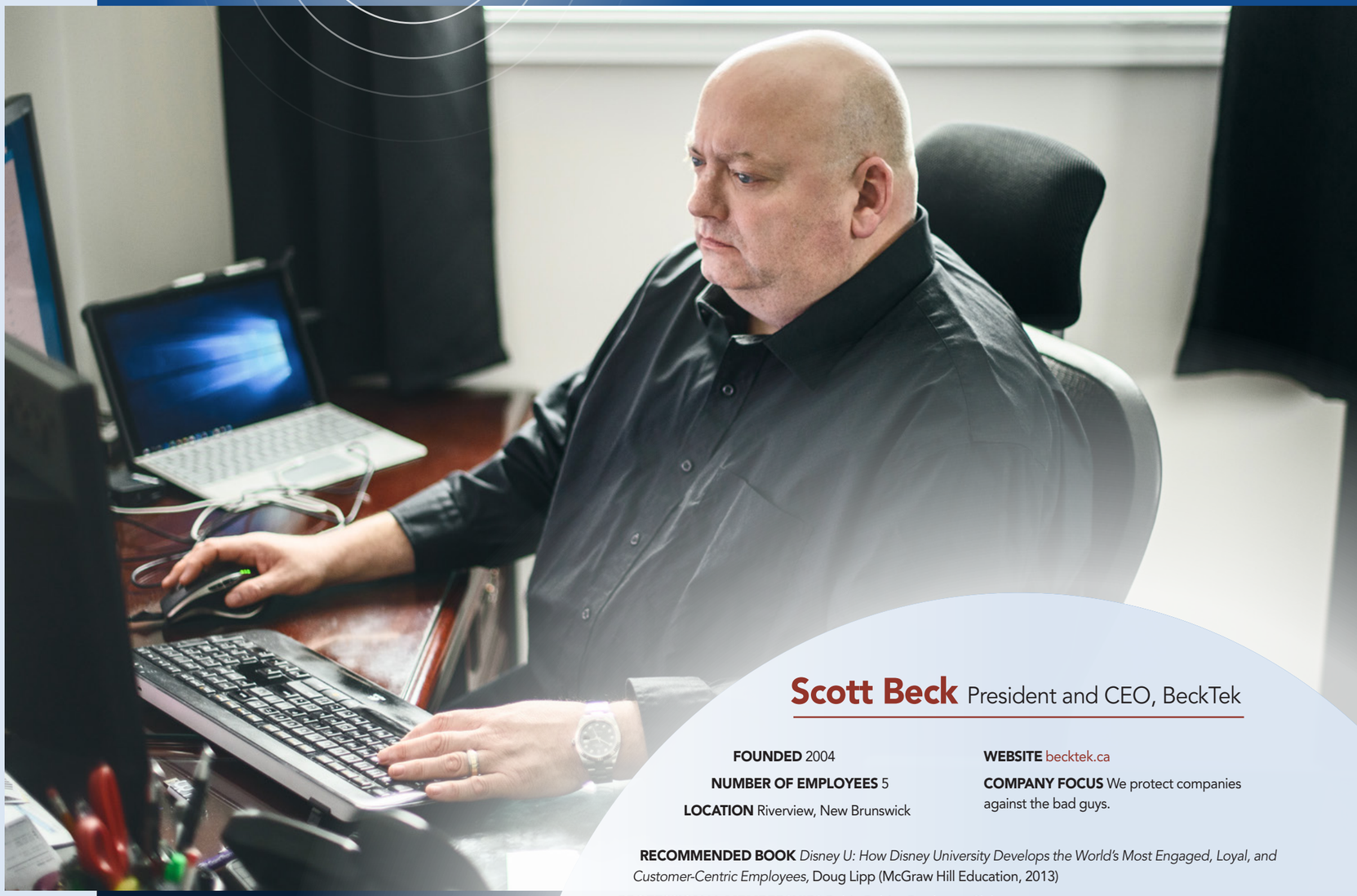
Another angle, he says, is monitoring Io sensors for water or fire damage, and othe business losses, which can lower insuranc costs for your customers.

Perhaps the more pertinent questio now is whether an MSP can afford to ignor IoT management projects. "'The sky is fal ing' message is always around, and IT-onl MSPs will be fine for five to 10 years," say Knocke, who adds that it is "better to b forward thinking. Businesses prefer to bu from full-service management providers."

JAMES E. GASKIN *is a* ChannelPro *contributing editor and former reseller in the Dallas area.*

TURNING YOUR MIC ON

BeckTek established itself as a security authority by telling stories that help clients and prospects understand that cyberdefense is a business solution. By Scott Beck • Photography by Denis Duquette



SELLING SECURITY is about storytelling. Whether I'm sitting with a client one-on-one or standing on the stage in front of hundreds, telling a story from the front lines of cybercrime that has been in the media or shared by my vendor partners makes security more relatable to businesspeople. When you can help customers make that connection between what the risks are and what that means to their business, you can see the light bulbs go off. That's when they start paying attention and want to know how to protect themselves.

My own ah-ha moment occurred in the early days of ransomware when my peer group encountered CryptoLocker. Since then, BeckTek has done two things: We transformed to a security-centric MSP, and I transformed myself into a sought-after public speaker on the topic. That combination has changed our business over the last six years and accelerated our growth.

MSP vs. MSSP

BeckTek purposefully chose to be a security-centric MSP versus a managed security services provider (MSSP). Rather than build out a security operations center (SOC) and put a team in place to support it, we evaluated and tested existing solutions to determine what would make sense for our clients' price points and required security levels to give them peace of mind.

We built out a stack of solutions and, like an orchestra conductor, we ensure they all play well together. We are also the "one throat" for our clients to choke if there is a problem.

Our security offering includes three main platforms: SOC-monitored advanced endpoint protection, breach detection and response software, and a universal threat management firewall featuring intrusion detection/prevention services. We also use a third-party email security solution to clean email before it hits the client's email servers, and offer employee education and training along with dark web scans. All these different layers go into making our security "cake."

Not everybody requires a seven-layer cake, so we customize the stack to a client's needs and acceptable levels of risk. At a minimum, we require clients to have our RMM, advanced endpoint protection, and breach detection and response solutions.

Clients really don't care about *which* tech solutions you're using, but they *do* want to hear that they're protected. So over the years I've worked very hard at becoming a public speaker and telling stories that help people understand why security is a business solution. Stories are powerful tools, and if you offer free, valuable information and establish yourself as an authority, people will want to engage with you.

Becoming a Storyteller

You can become a security storyteller even if it doesn't come naturally to you. Back before BeckTek, when I was a radio DJ, I found it quite scary just turning on the mic and knowing there were people listening, despite being in a room by myself.

But about seven years ago, I heard a speaker at an industry event talking about security, and my wheels started turning. I thought, "Yeah, I can talk for an hour on security." So I approached my local chamber about doing a free seminar. It went well, and I branched out through other local service organizations. Once I got the first couple under my belt I got more comfortable. Then other organzations started approaching me. My first local radio spot led to a TV spot, which put me on the radar for speaking engagements, and inclusion in the movie *Cyber Crime*, a documentary (available on Amazon) featuring me and other security experts.

To go down this road, you must get uncomfortable in front of an audience before you get comfortable. Also, recognize that everybody makes mistakes and something always goes wrong. I've learned that if you can joke about yourself, you put people at ease and they'll forgive any little mistakes.

Once you turn your own mic on, prospects who reach out because they've heard you speak are already prequalified and pre-sold on the concept that they've got a security problem. That has opened a lot of doors for me.

Scott Beck President and CEO, BeckTek

FOUNDED 2004

NUMBER OF EMPLOYEES 5

LOCATION Riverview, New Brunswick

WEBSITE becktek.ca

COMPANY FOCUS We protect companies against the bad guys.

RECOMMENDED BOOK *Disney U: How Disney University Develops the World's Most Engaged, Loyal, and Customer-Centric Employees,* Doug Lipp (McGraw Hill Education, 2013)

PROFESSIONAL MEMBERSHIPS Robin Robins Producers Club

FAVORITE PART OF MY JOB If most technicians were honest, we love throwing on our Superman cape and solving problems and helping people; that's really the fun part to me.

LEAST FAVORITE PART Delivering the bad news when things go really wrong

WHAT PEOPLE WOULD BE SURPRISED TO KNOW ABOUT ME As a younger person, I was actually very shy and insecure.