Expert Guide

FOR INTEGRATORS AND SOLUTION PROVIDERS

WEBROOT®
an opentext™ company

PRESENTS

Tools and Tips for Adding Managed Security to Your Service Offering

Inside

Security is a hot market, with businesses of all sizes gaining ever-more understanding of the need to protect their IT infrastructure and digital assets. IT solution providers can capitalize on this trend by adding managed security services to their portfolio.

This Expert Guide explores how to launch a managed security practice and issues to consider when building out a security stack, as well as dealing with customer resistance and cybersecurity talent shortages, plus some in's and out's of cyber insurance.

POWERED BY ChannelPro
WWW.CHANNELPRONETWORK.COM

IoT playbook
WWW.IOTPLAYBOOK.COM

MASTERING MANAGED SECURITY

If you're like most channel pros, you're probably delivering at least some managed IT services to your customers, and almost certainly providing some assistance with security. You're probably not, however, offering a true managed security service that combines both disciplines. This white paper defines what managed security is, explains why you should be doing it, and explores the most critical issues to think about when launching a managed security practice.

WHAT IS MANAGED SECURITY?

Let's begin with what it's not. Just because you're an MSP who provides security essentials like anti-virus and firewall protection to your clients doesn't mean you're in the managed security business.

Though definitions vary, most experienced observers agree that a true managed security service 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. It's typically sold separately from an MSP's core managed IT service bundles, and often lets customers choose from a menu of basic, intermediate, and advanced tiers.

Here's something else experts agree on: Providing a managed security service is not the same as being a managed security service provider (MSSP). Unlike most MSPs with managed security offerings, MSSPs provide 24/7 log monitoring and analysis via a security operations center (SOC) stocked with powerful (and expensive) software and staffed by high-priced security analysts. Generally speaking, only very large MSPs and channel pros who do nothing but security can afford to make those kind of investments. As we'll see shortly, though, most MSPs with a managed security service can and should partner with an MSSP.

WHY SHOULD YOU OFFER MANAGED SECURITY?

The list of reasons for adding managed security to your service roster is a compelling one:

- **It's a red-hot market:** IDC expects sales of security hardware, software, and services to climb at a 9.4% compound annual growth rate through 2023 to $151.2 billion. Sales of managed security services specifically, by contrast, will grow at an even faster 13.9% CAGR during that period from a $21 billion base in 2019.
- **SMBs are increasingly eager to buy it:** They see the same headlines as you in the media about ransomware attacks on local governments and giant corporate data breaches, and aren't as confident as they used to be that their relative obscurity will spare them from being the next victim. In fact, many MSPs these days lead with managed security when selling to new clients and add managed network and endpoint services only after they've established a relationship.
- **The revenue is recurring and the margins are high:** The more monthly recurring revenue your company collects, the higher its potential sale price when the time comes to initiate your exit plan. Markups on managed security services can easily top 65%.

WHAT GOES INTO A GOOD MANAGED SECURITY PACKAGE?

There's no hard and fast rule, but most providers of managed security services eventually include a majority of the following in some or all of their tiered plans:

- Next-generation, behavior-based endpoint protection software that draws on artificial intelligence to block malicious activity in real time
- Next-generation firewall products that use AI the same way
- Spam and DNS filtering services
- Email security software
- Network security software
- Patch management
- Backup and disaster recovery
- Dark web monitoring, to know as quickly as possible when user credentials have been stolen
- Two-factor authentication, to make utilizing stolen credentials harder for the bad guys
- Endpoint detection and response software, to mitigate the effects of attacks that make it past the customer's first lines of defense
- SOC services, typically from a third-party MSSP, to identify, diagnose, and remediate security incidents quickly
- Vulnerability scanning services, to identify and mitigate gaps in a client's defenses
- Security awareness training, to prevent end users from falling for phishing scams
- Cyber insurance, to lessen the financial impact of a successful attack if all else fails

There are additional options as well, like mobile device management, data encryption, and secure remote access. Regardless of what your managed security packages include, though, be sure to price them at predictable, all-inclusive rates. To maximize their profitability, resist customizing them for customers on a one-off basis.

WHAT IF YOU'RE UNFAMILIAR WITH SOME OF THOSE TECHNOLOGIES?

Unless you're a full-blown MSSP, you'll probably end up delivering some managed security services yourself and outsourcing others. Figuring out what to outsource can be tricky, though. Here are a few do's and don'ts to keep in mind:

- ***Do* outsource critical items,** like SOC services, that are too expensive for you to offer yourself.
- ***Don't* outsource absolutely everything.** If all you're doing is passing along someone else's services, 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 more expertise or cheaper rates.
- ***Do* handle anything that involves site visits** (like firewall maintenance) and face-to-face meetings with customers yourself, to keep client relationships strong.
- ***Don't* perform tasks like penetration and vulnerability testing yourself.** No one can audit their own work fairly, so get an outsider's assistance when evaluating how well you've defended your clients.

Remember as well that what you need to outsource to others will change over time. The longer you're in the managed security business, the greater your ability to execute security tasks on your own will grow.

SHOULD YOU WHITE LABEL EVERYTHING OR BE TRANSPARENT ABOUT YOUR OUTSOURCING PARTNERS?

Honesty is usually the best policy on white labeling, unless you don't mind taking all the blame when one of your security outsourcers makes a mistake. Rather 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.

WHAT SKILLS DO YOU NEED IN-HOUSE?

Fewer than you might think if you're partnering with others. Experienced providers agree that everyone with a managed security offering should have

a basic understanding of threat vectors and stay up to date on the latest trends. Clearing those bars, though, could be as simple as taking some training courses through vendors or industry associations like CompTIA, and then reading a few good security blogs on a daily basis.

Harder to acquire if you don't already have it is the organizational and communication talent you'll need to collaborate with third-party partners effectively and execute incident response plans efficiently. Those skills aren't specific to security, though, and are mandatory in other areas of IT.

WHAT GUARANTEES SHOULD YOU MAKE?

Don't promise more than you can deliver. No one can deliver perfect protection, so no one should say they will. Tell your clients that you will reduce their exposure to threats and decrease the impact of any attacks that get through.

HOW SHOULD YOU DECIDE WHICH VENDORS TO PARTNER WITH?

Start by identifying all the security technologies you'll be delivering, and then look for the top names in each of those areas. Generally speaking, and despite the added vendor management complexity, you're better off working with multiple best-of-breed vendors than with one company that can do everything but has second-best solutions in some fields.

Test each vendor's products thoroughly and collect plenty of feedback from your peers in the industry before signing any agreements. Make sure the vendors you select share your values and treat customers the same way you do. If you don't want them talking to your clients, confirm that they won't do so without your permission.

Finally, try whenever possible to work with outsourced service providers that do more than just send you alerts. Some MSSPs will get on the phone with you to explain a potential threat and tell you how to address it. That's valuable training that will strengthen your firm's security IQ over time.

WHAT'S THE BEST WAY TO GET STARTED?

Eating your own dog food, as the saying goes. MSPs are under constant attack these days from cyberthieves hungry for the end-user credentials and other data stored 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.

Once your managed security practice is up and running, consider investing in the steps necessary to become SOC 2 certified. 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 give you a leg up over competitors when pursuing new ones. Better yet, SOC 2-compliant MSPs can charge more.

Last but not least, 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.

This white paper is based on input from:

- **SCOTT BECK,** President, BeckTek, **becktek.ca**
- **ROBERT BOLES,** President, BLOKWORX, **blokworx.com**
- **ANGELA HOGABOOM,** CEO, Ocular, **ocular.biz**
- **JOSHUA LIBERMAN,** President, Net Sciences Inc., **netsciences.com**
- **RORY SANCHEZ,** CEO, True Digital Security, **truedigitalsecurity.com**

BONUS ROUND!

Visit **channelpronetwork.com/managedsecurity2020** for more great content from *ChannelPro* on mastering managed security, including:

- A primer on cybersecurity A to (almost) Z
- How one MSP transitioned to MSSP
- *ChannelPro* Executive Editor Rich Freeman on the expanding attack surface
- MSP business coach and transformation specialist Erick Simpson on how to sell cybersecurity even if you're not an expert
- An article on how to leverage the cybersecurity difference for dollars
- An expert tour of the security threat landscape
- MSP Joshua Liberman on building the ideal security stack
- How to avoid the pitfalls of cyber insurance

Building the Ideal Security Stack

The specific services MSPs offer should depend on an analysis of the "threatscape," client needs, the security marketplace, and more. By Joshua Liberman

NEARLY ALL OF US have experienced the overwhelming weight of providing security for our clients. Of course, that pales before the amazing diversity of options we have to choose amongst for provisioning those security products and services. To make matters harder, this rich and expanding ecosystem is not only growing but also changing as vendors adjust offerings and pricing structures or get acquired. Plus, the "threatscape" evolves constantly, and different clients may require different levels of security. All of this makes building the ideal security stack a daunting proposition, a bit like hitting a moving target from a moving target. Read on to see how one intrepid MSP manages this morass.

Tiers or "All-In" Only?

Securing your networks is so important that many MSPs offer only the "all-in" option. They provide every service to every client without choices. While most of us would love to do this, there are mitigating concerns. A stack that includes everything from endpoint detection and response to device encryption imposes not just added costs, but complexity as well. And some of your clients may require (and put up with) a "stiffer security posture" than others. If you make things too hard to use, your clients will work around you.

That said, with all the hacks and breaches in the news, a lot of the groundwork for this selling has been laid for you already. And when you consider your potential legal exposure should your client get breached, the all-inclusive option looks even better. Another advantage of going all-in is that you don't have to worry about designing bundles or tiers of services, or grapple with what is safe to leave out of your bundles. Everybody gets everything in this one-size-fits-all world and there is a very good argument to be made for this.

In an ideal world, we'd all offer only these all-in plans. But the reality of cost/benefit and risk analysis means we cannot go all-in for every customer site and that some sites require different security postures. For that reason, Net Sciences offers three tiers of security services, each of which adds more services to the last one. The specific services you weave together to provide at each tier depends upon an analysis of the threatscape, your clients' needs, the security marketplace, and more. And, of course, it will change as these variables change.

Identify and Strategize

Whether your intention is to go with all-in, tiers, or a la carte, you've got to identify the risks you're mitigating and then find the appropriate tools and procedures to protect against them. There is no precise formula here. Your experience in the field, your exposure to vendors and technologies, and your interactions with peers are all important. Wearing both your security and business hats at once is important too. Approach securing your clients' networks as an exercise in risk management, as you

may find that selling mitigation is easier and more effective than simply selling security. After all, you don't sell gym memberships based on working out five days a week. You sell them based on results.

If you do decide to build security tiers, the natural question to follow is how many tiers to provide and how to build out those tiers. We limit our offerings to no more than three options. Beyond that, we tend to see confusion set in, and there is no such thing as a confused buyer. Keep it as simple as possible, and remember that the bundle is indivisible, as you don't want to have to manage a unique set of services for every site. We offer a Basic plan with six security services, an Advanced plan with three more security services, and a Comprehensive plan with another three security services. Over time, we'll migrate all of our customers to either the Advanced or Comprehensive plans, further simplifying offerings and fortifying sites.

Flexible and Extensible

Threats continue to develop and change, so security offerings continue to develop and change too. For example, nobody was defending against ransomware five years ago, or for that matter, against two-factor

ILLUSTRATIONS: ERHUI1979 / ISTOCK

authentication attacks based on SMS messaging last year. But now we have to consider both. That's you why you must design a flexible, extensible framework for your offerings. We provide a baseline security stack built on commoditized components, so if a product line changes suddenly, we can respond quickly and without great expense while we expand our stack.

Another issue you'll have to address is what happens when a vendor drops a product you are committed to or gets purchased by another player that doubles or triples your prices. Anyone paying attention in this industry has seen vendor acquisitions lead to wild product and pricing changes. You'll never be able to cover every eventuality, and you won't be able see every acquisition or strategic realignment coming. But with a sufficiently modular services design that allows you to snap new coverages and vendors in and out, you'll have at least a leg up on it.

There's Always More

Of course, there's always more to offer, like data loss prevention, email archiving, proximity logouts, and so on. We provide these advanced options on an a la carte basis. We also "downward propagate" our service stack. For example, at the beginning of the second year, we give customers on our Basic plan an offering from the next package up, covering its cost. A year later, we migrate all the remaining "second level" offerings to the first level, raise seat or site prices accordingly, and add a new suite of offerings at the higher tiers (raising those prices). This cadence allows us to keep adding new security and justify price increases every other year as well, a win-win situation.

Don't Forget Comprehensive Data Protection

You might be wondering what a discussion of backup and business continuity is doing here. That's easy; any security plan must include comprehensive data protection. No matter how well you secure your clients, eventually your protection will get beaten. And that is why having reliable backup and business continuity can save your skin. Be it ransomware, a bad patch, or anything that takes you down, the safety net of comprehensive data protection is unbeatable. That means file and folder backup, local failover, versioning for rollbacks of at least a year, and true disaster recovery with off-site imaging. This topic brooks its own discussion, but suffice it to say, without comprehensive data protection, you are not fully securing your networks.

JOSHUA LIBERMAN *is president of Net Sciences, founded in 1996. A 24-year ASCII Group member, former rock climber, martial artist, and lifelong photographer, Liberman speaks five languages and has visited five continents. He also writes frequently and raises Siberian Huskies with his wife Heidi, who calls him the Most Interesting Geek in the World.*

Securing the Security Resistant

SOME CUSTOMERS simply refuse to spend money on security no matter how clearly you convey the risks. Chances are good, of course, that these recalcitrant customers will eventually get breached and may blame you or even seek compensation for breach-related damages.

There are several strategies you can follow to try to prevent these situations from arising in the first place, and failing that, protect yourself from being on the losing end of a lawsuit.

For instance, at the beginning of every engagement, Mainstream Managed Services, a Merrimack, N.H.-based MSP, conducts a complete network security scan, followed up by a detailed statement of work that includes identified security vulnerabilities, the action plan proposed to address them, and a signature page where clients can accept or decline the plan in writing.

Reluctance to spend on security is a common scenario, though, "mainly because [customers] don't see it providing them with any competitive advantage," says Craig Peterson, Mainstream's president.

CRAIG PETERSON

For those that resist recommendations, "the first thing we try to do is work with the client to identify the issue," says Michael Schenck, director of security services for Kaytuso, a New York-based cybersecurity consultant. "If it's a price-point issue, we try to find another way to reach a security solution."

If this approach fails, Schenck tries to cover his firm legally with an approach similar to Peterson's. He prepares a "Risk Acceptance and Waiver of Liability" letter for signature by both parties documenting security solutions proposed, but declined by the client, with the client accepting all risks of this decision and agreeing not to hold the consultant liable. In many instances, he notes, this letter is enough to get clients to rethink their position.

While carefully crafted contract provisions that explicitly lay out who is and is not responsible for what happens if security recommendations are not followed are a must, they don't provide complete protection.

MICHAEL SCHENCK

"Even when a client doesn't take their advice, the MSP still has some responsibility to show that they are exercising their best efforts to provide security," says Rory Sanchez, CEO of True Digital Security, an IT services provider with offices in West Palm Beach, Fla.; Tulsa, Okla.; and New York.

MSPs can help protect themselves here by including more security controls as part of their basic services offering, "so that at a minimum, they can show that they are doing their best to safeguard things," Sanchez says.

Despite these best efforts, though, when a high-profile client breach gets publicized, "what's also going to hit the news is the fact that you are the MSP," Sanchez says, "not that you gave the client sound advice and they refused to follow it."—*Martin Sinderman*

AT-A-GLANCE

Good Security Help Is Hard to Find

WANTED: 4.07 MILLION cybersecurity professionals to join the current workforce of 2.8 million. That's a 145% increase of trained staff needed to close the global skills gap, according to the 2019 *(ISC)² Cybersecurity Workforce Study* from (ISC)², a nonprofit membership association and issuer of the Certified Information Systems Security Professional (CISSP) certification. In the U.S. specifically, the cybersecurity workforce needs to grow 62% to meet demand.

A shortage of cybersecurity professionals is a problem for companies in all industries and sizes globally, the research states. Among those with 3,000-plus employees, 65% report a shortage of cybersecurity staff, and 51% say their organization is at moderate or extreme risk because of it. In addition, 36% say the lack of skilled/experienced cybersecurity personnel is their top job concern.

Small companies (fewer than 100 employees) are staffing their cybersecurity teams with more general roles like security operations and security administration. Midsize companies (100 to 499 employees) have a slightly higher allocation for risk management and compliance, while large firm are more likely to have more specialized roles like penetration testing and forensics.

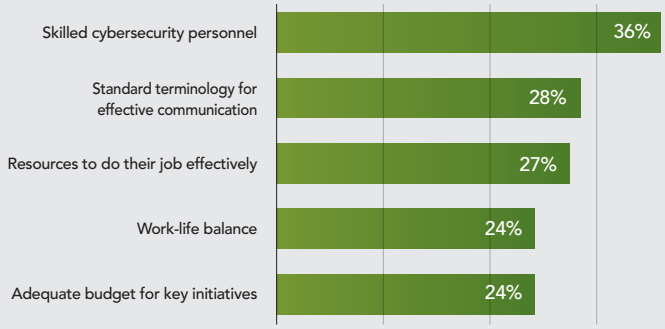
If you're an MSP looking to add to your cybersecurity staff, it may be difficult to poach from other companies, though, as these pros tend to be long-tenured, according to the research. Respondents have an average of nine years in an IT role, with six years at their current organization and five years in a cybersecurity role.

Beyond the current cybersecurity talent pool, respondents say they plan to recruit from these resources over the next year: new university graduates (28%), consultants/contractors (27%), other departments within an organization (26%), security/hardware vendors (25%), and career changers (24%).

The research also finds that women are an untapped resource; today cybersecurity professionals are more than twice as likely to be male.

If you can find the security staffing help for your MSP business, however, the (ISC)² research suggests potential customers of all sizes may be looking for a hand.—*Colleen Frye*

Cybersecurity Pros Believe They're Lacking in These Areas:



SOURCE: 2019 (ISC)² CYBERSECURITY WORKFORCE STUDY

PHOTO: ANDREYPOPOV ISTOCK

When Cyber Insurance Doesn't Pay

CYBER INSURANCE *should* protect SMBs (and the MSPs servicing them) from the financial effects of a data breach, but insurers can deny claims for a variety of reasons. That's why it's important to pay attention to the details.

Benjamin Dynkin, co-founder and co-CEO of Great Neck, N.Y.-based managed security provider Atlas Cybersecurity, says he is seeing "a lot more creative rejections on a large scale." Dynkin, who is also co-executive director of the American Cybersecurity Institute, encourages businesses to "work with a broker that understands these things."

Most commonly, insurance claims are denied due to inaccuracies in the policyholder's self-reporting surveys. "Whether through lack of knowledge or because they quickly filled out a form, it's easy for a company to overstate how they protect themselves," Dynkin says. "When the information on that form doesn't line up with what's really happening, that's grounds for rejection."

In addition to remaining compliant with the security terms of coverage, Dynkin says SMBs must understand exactly what's covered.

"Essentially what we've seen in the cyber-insurance security landscape is a tension between traditional notions of cyberattacks versus what [would] be a process failure," Dynkin explains, offering the example of a fraudulent email resulting in a compromise.

The insurance company will call this an internal process failure, he says. "They'll say, 'This has nothing to do with cyberattacks; they just tricked you.'"

"Make sure your broker won't just slap together something told to them by their underwriter," Dynkin advises. "Get walked through it."

Moreover, there are new questions of coverage arising all the time, Dynkin says. For example, the June 2017 cyberattack NotPetya caused damage globally, and in a Feb. 2018 assessment from the U.K.'s National Cyber Security Centre, Britain determined "the Russian military was almost certainly responsible for the 'NotPetya' cyber attack."

According to Dynkin, this declaration had an interesting policy implication: namely, the "act of war exception." Some insurers claimed "acts of war" were not covered under standing cyber-insurance policies.

"Nation states are getting more and more active in the space," Dynkin says, asking, "If that becomes a more common thing, does that get exempted?"

Aside from whether a claim will be covered is the question of how much a policyholder will get. Dynkin advises SMBs to plan for business interruption, the costs of which are easy to underestimate.

"There are very serious considerations around this," he warns. "If you sub-limit the wrong way, that may not be enough. Make sure you're adequately covered for your business."—*Geoffrey Oldmixon*