MSP Barracuda

Mastering the Art of Selling Security-as-a-Service

CONTENTS

Introduction

For the longest of time, demand for managed security services has been stubbornly limited. The primary reason for this is that security and compliance are all too often viewed as a tactical investment limited to deploying a firewall and installing anti-virus software on a desktop or notebook PC running Windows.

But the way organizations approach security is changing. Not only is the volume of attacks they must defend against increasing, so too is the sophistication of those attacks. Organizations of all sizes find themselves under siege from everything from zero-day attacks that appear with little to no warning to ransomware schemes that trick gullible end users into encrypting large amounts of data the organization can't do without. More challenging still, the attack surface that needs to be defended keeps expanding thanks to the rise of both mobile and cloud computing.

The security and compliance opportunity for MSPs falls into four broad categories. Almost every MSP is expected to be able to provide firewalls, spam and content filtering, intrusion detection, and antivirus services. While demand for those services is high, competition at the level of security services is increasing. **MSPs that want to ensure higher profit margins need to focus on providing additional security services**, including vulnerability assessments, encryption management, two-factor authentication, and training programs to further end-user security education. At the highest end of the security services space there are emerging opportunities ranging from analytics for identifying anomalies in real time to outsourced security operations centers. In the latter case, the MSP manages everything from detection to response on a 24/7, end-to-end basis. Finally, organizations of all sizes need to make sure compliance mandates are not being violated. Rather than treating compliance as an event, compliance today needs to be managed as a continuous process.

IT security and compliance are always going to be a means to a larger end. These days, however, managed service providers that want to stay relevant to their customers in the age of digital business will need to provide access to extensive IT security and compliance expertise one way or another.

Sizing the Security Opportunity

The global cybersecurity market is currently worth $173B in 2020, and is expected to grow to $270B by 2026. Obviously, that creates a massive opportunity for IT service providers that have the security expertise needed to succeed. Allied Market Research estimates that **by 2022 demand for managed security services will grow at a compound annual rate of 16.6 percent to become a $40.1 billion market.**

At a time when the volume of attacks is increasing exponentially, the attack surface inside most organizations continues to expand. In fact, a recent survey of 555 MSPs conducted by Barracuda MSP finds that more than two-thirds of respondents are already being asked by customers to protect instances of Microsoft Office 365 in the cloud. More than a third have also already extended their reach into other public cloud services.

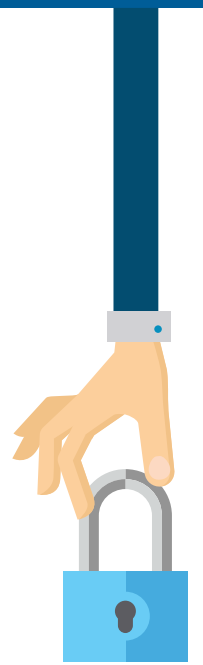
More organizations than ever have embraced mobile computing as well. The challenge they face, however, is not just securing the devices and the applications that run on them, but also making sure the wireless networks being used to access corporate resources are not distributing malware.

As organizations continue to invest in Internet of Things (IoT) projects, the opportunity to deliver managed security services will increase accordingly.

Today the cybersecurity market is valued at

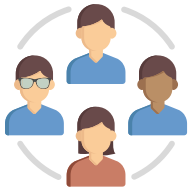
$173 billion.

Advantages of Selling Security as an MSP



Just as IT security services are becoming a prerequisite for any IT solution, the cost of delivering security-as-a-service is dropping. Thanks to the rise of cloud computing, most security technologies are now being offered as a service. IT organizations and small businesses are still looking to MSPs to configure and manage the delivery of those services, but acquiring and setting up dedicated infrastructure for IT security products is no longer a requirement. Some organizations may still prefer to deploy IT security technologies on premise to meet performance and compliance requirements. But, just as many now prefer to treat security alongside the rest of their IT investments as an operating expense.

1. Staffing advantages



It's no secret there's a massive shortage when it comes to IT security expertise, though. Estimates say that a "talent crunch" will create 3.5 million unfilled cybersecurity jobs globally by 2021. While that shortage creates some challenges of managed service providers and internal IT organizations alike, MSPs have a strategic advantage in that they can resolve security issues faster because the odds are good they've seen the problem before.

A modern IT security strategy requires mastering a whole range of security technologies, including everything from new classes of anti-malware software for securing endpoints to Big Data analytics applications. At a bare minimum, a layered approach to security needs to span email security, next-generation firewalls, anti-persistent threat software on the endpoint, as well as monitoring tools. The fundamental advantage a managed security service provider (MSSP) has is that it can leverage investments in those technologies across multiple customers.

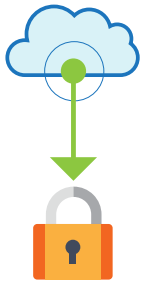
Even if an internal IT organization could attract the security talent they need to implement a specific class of technologies, their odds of being able to hold on to that talent are limited at best. In fact, because an MSP bases its business on providing security-as-a-service, they generally can pay IT security professionals better.

In addition, the best IT security talent is usually attracted to organizations that present them with the most interesting set of challenges. **MSPs tend to have much more robust training programs in place to attract IT security professionals** that need to continue to expand their skill sets and, by extension, market value.

By
2021
there will be
3.5 million
unfulfilled IT
security jobs
worldwide

Finally, most MSPs are in a much better position to be able to take advantage of advances in IT automation to lower the cost of delivering IT security. Whether it involves automating tasks such device management, monitoring, helpdesk ticket monitoring, or leveraging investment in security information and event management (SIEM) software across multiple customers, an MSP can always aggregate the costs of delivering those services across multiple customers. In contrast, an internal IT organization needs to absorb the cost of delivering similar capabilities entirely on their own limited budget in a way that most internal security staffs are not likely to embrace.

2. Cloud advantages



Many vendors are now offering a raft of security services that are delivered via the cloud. **The days when MSPs needed to build security operations centers on their own from scratch are over.** Security services in the future will be a mix of cloud services provided by vendors that will be augmented by higher-value services offered by the MSP. Collectively, that approach enables the MSP to reduce its total cost of delivering managed security services.

In effect, the MSP quickly evolves into becoming a broker for delivering multiple IT security services; some that are home-grown and others provided via vendor partners with expertise in a specific area.

The centralization of security in the cloud provides the added benefit of making it easier to apply analytics and other forms of threat intelligence against data now that it is centrally located. In time, MSPs will be a primary source of data for artificial intelligence (AI) services that will automate most lower-level IT security functions. Whether an MSP decides to partner with a vendor to gain those capabilities or build it themselves, security services based on machine and deep learning algorithms are only as good as the amount of data that can be correlated. Most internal IT organizations simply won't have enough data to effectively take on the challenge of implementing the next generation of advanced AI security services on their own.

Challenges with Selling Security-as-a-Service

No matter how hungry an MSP is to make a sale, they would be well-advised to be selective when it comes to onboarding a new client. In fact, the single biggest challenge that MSPs offering security services will face isn't finding enough customers, but rather resisting the temptation to engage a customer that they know will be more trouble than they're worth.

The first thing every MSP should do when approaching a customer about managed security services is make sure that all the parties involved in the initial conversation understand the true scope of the challenges associated with securing the IT environment. MSPs need to ascertain how much legacy software and infrastructure makes up the customer IT environment. Generally, the older the applications and systems in place, the more vulnerabilities there are. If the customer doesn't have the resources required to modernize the IT environment, the risk the MSP takes on to secure it rises exponentially.

The next major issue MSPs need to tackle is how much money the customer is willing to allocate to IT security. In fact, how quickly pricing comes up in a conversation with a prospective customer is an early indicator that customer may not appreciate the true value of IT security to their business. **If a customer is only willing to fund a bare minimum level of IT security, that almost always spells future trouble for the MSP.** Once that inevitable IT security incident occurs, the terms and conditions of a service contract won't provide customers with any comfort in their hour of need. All it really does is provide them with an incentive to take their business elsewhere because they'll be looking for someone to blame for their plight other than, of course, themselves. MSPs, deservedly or not, are easy targets for customer ire, so they need to be smart about which security customers they take on.

Next Steps: Download The SMB's Guide to Cyber Security and use it as a tool to help educate customers and start conversations about security.

> "When clients come to us after an attack or incident, it basically comes down to what can they afford and how much risk can they tolerate going forward."
>
> –Chris Johnson, longtime MSP; member of Executive Council for CompTIA's IT Security Community

Building Tiers of Service

Given the fact that security is now core to every IT process, all MSPs need to be able to provide some level of foundational security. They may not always be able to charge separately for it, but it's hard to imagine any managed service today that doesn't include some aspect of IT security.

Foundational IT security services should include endpoint protection, server lockdown, and network perimeter security, as well as some form of backup and recovery. In some instances, a customer may prefer to contract for each service à la carte. But as more customers come to recognize that IT security is a core function of doing business, they are increasingly expecting IT security to be bundled with other managed IT services. For example, a managed print service should now include the services needed to secure those printers on an end-to-end basis.

The challenge that presents MSPs is making sure they don't find themselves giving away the IT security service just to gain the business. IT security can be costly to deliver in terms of both products and the people required to

master them. So, **MSP profitability can suffer considerably when IT security services simply become another cost of doing business, instead of remaining a stream of revenue.**

MSPs need to carefully weigh what other IT security services to provide. Database security, for example, requires more expensive technologies and expertise. Rather than building out that capability themselves, MSPs should consider partnering with another service provider that has already established a specialty around that specific capability. Naturally, many MSPs get uncomfortable bringing additional service providers into their accounts for fear of losing business. Any third-party service provider that an MSP partners with should have a demonstrable history of delivering unbranded white-glove services. Otherwise, the potential for confusion over who owns the relationship with the customer becomes too great.

Next Steps: To learn more about creating service tiers as an MSP, download our step-by-step how-to guide: How to Create MSP Service Tiers

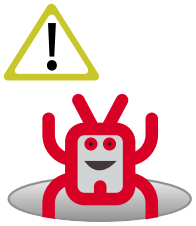
How Risk Management Equates to Pricing

MSPs need to understand the various levels of risk associated with any activity. It's one thing, for example, to secure an email system. It's quite another to secure mobile computing applications or a digital business process involving financial transactions across multiple borders. **MSPs need to make sure the customer understands that not all data inside their organization is of equal value.** Credit card numbers, healthcare records, or any other form of personally identifiable information (PII) represent primary targets. The amount of time and effort associated with protecting that data should be much higher than, for example, protecting product information the company routinely shares anyway.

Prioritizing what data needs to be secured comes down to how much financial exposure would result from losing control of that data. On the one hand, loss of PII data affects everything from how the company might be fined to damage to the corporate brand that results from having to disclose those breaches. As painful as those costs might be, however, they could be trivial compared to the loss of intellectual property that a company has spent years investing in.

MSPs need to tier their security services based on the level of risk being assumed. Business leaders that think in terms of risk management will immediately understand there is a correlation between the cost of the services being provided and the value of the data that needs to be protected.

Security Pitfalls to Avoid



There's no such thing as perfect IT security. Despite the best efforts of the best MSPs, there's a strong probability that at some point every organization is going to be breached, likely multiple times. The role of the MSP is to minimize the number of breaches, while also putting in place a means of quarantining and remediating any breach that occurs. It's critical that MSPs do not overpromise what they can deliver only to be accused by the client of underdelivering.

MSPs are especially vulnerable to IT security fatigue. Most of the alerts being generated in an IT environment wind up being false positives. Before too long, even the most dedicated IT security personnel becomes inured to them. Of course, it's only a matter of time before an alert that gets ignored signals a major security incident.

MSPs also need to pay close attention to how they engage with their customers. One of the primary reasons many organizations continue to hire internal IT staff is the sense of personal service being provided by someone who intimately knows their business and people. MSPs need to replicate that experience by dedicating customer service personnel to specific customer accounts. That way the customer doesn't feel they need to re-educate the technician about their issues every time they engage with them. No matter how good an IT security service is, most MSPs wind up losing customers due to customer service issues more than anything else.

Next Steps: Read this blog post on how to build customer trust.

Becoming an MSSP

There is a world of difference between being an MSP that includes security as part of their overall services portfolio and becoming a managed security service provider (MSSP). **An MSSP needs to specialize in a much broader suite of security technologies to secure specific types of applications or deployment scenarios.** Most MSPs, for example, are not up to the task of securing a global Internet of Things (IoT) deployment on their own.

MSPs that have made the leap to becoming an MSSP strongly advise that any MSP considering making a similar jump set up a separate business unit to address the opportunity. The costs of becoming an MSSP are so great that the rest of the MSP business can easily find itself starved of resources.

MSSPs usually take on much higher levels of risk as well. The liability attached to a single bad customer experience could drag the entire MSP under. Isolating that risk within the context of a separate business unit or company creates the opportunity to pursue new revenue opportunities in a way that doesn't imperil the rest of the business in the wake of catastrophic customer event.

Next Steps: Watch our webinar "What Cyber Liability Errors & Omissions Coverages You REALLY Need" to learn about liability requirements for MSPs

> "Constantly review the different offerings and enhancements that you can provide. There is no 'set it and forget it' approach to security."
>
> -Christopher Cable, project manager & system engineer at Techworks Consulting

Marketing Security the Right Way

Given the growing demand for managed security services in the market, the level of competition across the category is increasing. The challenge is that the volume of fearmongering that currently surrounds IT security winds up making potential customers less inclined to listen to fevered marketing pitches. **Messages involving doom and gloom should be avoided at all costs.**

MSPs would be well-advised to use vehicles such as blogs, podcasts, infographics, videos, and newsletters to provide potential customers with forthright advice on how to deal with specific classes of threats. Rather than reminding prospective customers that the IT security sky is falling, MSPs should provide suggestions that identify concrete steps a customer can put in place to either mitigate a threat or remediate a specific type of problem with an eye toward getting customers to trust in the expertise of the MSP.

Almost all of that content needs to be authored by someone with technical expertise. IT security content developed by marketers simply doesn't resonate with the same level of authenticity as content developed by IT security experts. If an MSP's internal IT security staff doesn't have the time or ability to develop that content, than an MSP should tap into a wealth of third-party content that most IT security vendors now routinely make available.

Nothing engenders trust in an MSP as much as a customer testimonial. **It's a critical for an MSP to have clients that are willing to validate their efforts in front of other potential customers.** Whether it's a simple case study or a roundtable that the MSP sets up for customers to share expertise and insights about their common cybersecurity

enemies, it's critical for an MSP to be viewed as the trusted conduit through which IT security knowledge is shared and augmented. As part of that effort, MSPs should also make external IT security expertise available to their customers whenever possible. There's nothing like a renowned IT security expert even indirectly being seen to validate the expertise of an MSP.

As a rule, MSPs should pay close attention to the fundamentals of content marketing; the core principle of which is to package up relevant content in a way that educates and informs new and existing clients without promoting products or services directly.

Next Steps: See how your marketing stacks up. Take our interactive marketing assessment.

Conclusion

IT security and associated compliance requirements represent a major opportunity for MSPs. While there may be initial resistance from some potential customers, a description of how distributed denial of service (DDoS) attacks are increasing in volume or an example of how cybercriminals are employing social engineering techniques to trick even the most sophisticated end-users into downloading ransomware is enough to convince everyone involved that IT security is best left to the professionals.

The conversation then quickly moves into the nature of the IT environment that needs to be protected and at what level. IT service providers can either develop that expertise themselves or partner with an IT security specialist to meet that requirement. In most instances, IT service providers will find themselves relying on a mix of internal and external security specialists to get the job done.

Regardless of how security services are delivered, every MSP needs to provide some level of managed security services. While that clearly creates new opportunities for MSPs, **the most important thing for any MSP to remember is the need to overcommunicate the value of their services.** After all, it's easy to find fault when something goes wrong. But far too often, MSPs don't get the credit they deserve for the millions of attacks they do thwart. So providing customers with regular updates about security activities is a key part of maintaining successful—and profitable— security engagements.

Kick start customer conversations with our step-by-step guide, **How to Get SMB Customers to Understand the Value of an IT Investment**.