FOUR

Ways MSPs Can Fine-Tune Their Cybersecurity Go-To-Market Strategy

WRITTEN BY

Nick Cavalancia,
Technical Evangelist at Techvangelism

SPONSORED BY

CARBONITE® an opentext™ company | WEBROOT® an opentext™ company

If you're thinking about adding cybersecurity to your offering or want to change the way you offer your existing security services, now is the right time to stop and evaluate exactly how you should be taking it to market. SMBs today are operating in a very unique time where partially or completely remote workforces are the norm, cyberattacks are increasing in frequency and sophistication, and business owners are more focused than ever on remaining profitable.

Cybersecurity will be somewhat challenging for MSPs that traditionally focus solely on services with predictable service models, such as remote monitoring and management, cloud migration, and backup/disaster recovery. The reason? Cyberattacks are unpredictable in frequency, method, scope, and success rate, so delivering on the promise of working to keep a customer organization secure is tricky.

Therefore, it becomes really important to have a well-defined security offering with a solid go-to-market (GTM) strategy. Without one or the other, your success in marketing, selling, implementing, and delivering cybersecurity services will be less than desirable.

So, how should you go about building a modern-day cybersecurity GTM strategy?

You've already built at least one GTM strategy to bring your initial service to market, so you have some experience at this. But bringing cybersecurity to market requires some fine tuning of a traditional service GTM plan to support the current expectations of your customers—from the way you position the service to how you deliver it, and everything in between.

In this paper, we'll offer four ways to fine-tune your cybersecurity GTM strategy. We'll discuss why each is important and offer some guidance on how best to approach the way you bring your cybersecurity offering to market.

ONE

Build an Offering That Aligns with Your Customers' Level of Cyber Resilience

While cybersecurity in general aims to protect businesses from attacks, building a security offering and GTM strategy is not "one size fits all". None of your customers is exactly the same; some operate with a completely remote workforce, while others work with massive amounts of highly sensitive data, while still others wouldn't be able to survive the financial impact of a public data breach. So, you need to first understand the current state of your customer's ability to adequately protect against, prevent, detect, and respond to modern cyber threats and then focus on what about cybersecurity is important to them.

Cyber Resilience and the Small to Medium-sized Business

Traditionally, we've all encountered SMBs who believe cyberattacks are only a concern that impacts larger organizations. But that's just not the reality today; in fact, it's quite the opposite. Two-thirds (66%) of SMBs have experienced a cyberattack in the last 12 months[1] and 63% of have experienced a data breach in the same timeframe[1]. So, SMBs are keenly aware and have felt the impact of them actively being a target of cyberattack.

With such a material portion of SMBs experiencing attacks, it would be reasonable to assume they've taken steps to address this, right? Surprisingly, most SMBs not only *aren't* ready, but they *know* they're not ready; according to industry research, 73% of SMBs rate themselves as "cyber-novices"[2].

In essence, your customers have no idea what they're doing—and they *know it*.

The good news is the cyber pain felt by your customers is so impactful to them that they are also ready to spend money to address the issue. Nearly half of SMBs with less than 50 employees and nearly two-thirds of those SMBs with between 50 and 250 employees plan to increase cybersecurity spend in the coming 12 months[2]. In addition, nearly one-third of SMBs have allocated budget for consultants and third-party services and/or outsourced security[2].

Fine-Tuning your Cybersecurity

The opportunity here for you is to go beyond creating a security offering that just includes some common security solutions. SMBs are looking for a provider who is the cybersecurity expert that wants to implement an offering that truly makes their business resilient to cyber threats and minimizes the risk of a successful cyberattack. The offering also needs to be in line with the cyber-concerns of your demographic of customer, providing them with the confidence that their operations will be as secure as possible.

In other words, your GTM needs to be:

1. Holistic in approach
2. Customer-centric in nature
3. Dynamic in execution
4. Impactful in its protection

[1] Ponemon, State of Cybersecurity in SMBs Report (2019)
[2] Hiscox, Cyber Readiness Report (2019)

TWO

Use a Layered Security Strategy

It's no longer enough to just have antivirus installed on an endpoint and call it a security offering. Today's MSPs need a cybersecurity strategy that stands toe-to-toe with the bad guys' methods, frequency, and vectors of attack. Rather than starting with solutions and working backwards to a strategy, use something like the layered approach below and work towards solutions that fill the gaps.

Think of your customers' security needs as layers. Each layer should represent an aspect of a cyberattack that needs to be addressed differently than the others, as well be seen as an opportunity to secure that part of the environment. Take the example of such an approach below, which breaks a customer's environment into seven layers:

- **Perimeter** – Think of this as the logical "edge" of your customer's network, where potentially malicious data may enter or exit. Network appliances, network connectivity points, as well as email and web traffic all represent places that may need to be secured.
- **User** – The employee plays a role when they interact with potentially malicious content; either they are an unwitting victim or play a part in stopping attacks. This makes it necessary to pay attention to the user as part of your offering strategy.
- **Endpoint** – Think about both corporate and personal devices, laptops, tablets, servers, and mobile phones; every endpoint needs to be protected.
- **Identity** – Ensuring the person using a credential is the credential owner is another way to keep customer's secure.
- **Privilege** – Limiting elevated access to corporate resources helps reduce the threat surface.
- **Applications** – These are used to access information and valuable data, so monitoring their use by those with more sensitive access makes sense.
- **Data** – Inevitably, data is the target. Watching who accesses what provides additional visibility into whether an environment is secure.

For every one of these layers (shown below), there are specific methods and actions taken as part of a cyberattack, as well as types of solutions available to address cybersecurity concerns at that layer.

Attack Methods & Actions		Solution Types to Consider
Vulnerabilities, email, web, phone	Perimeter	Firewalls, email/Web scanning, DNS filtering
Phishing, scams, social engineering	User	Security Awareness Training
Malware, evasive techniques, fileless attack, RDG	Endpoint	Antivirus, Endpoint detection & response, application whitelisting, Ent. mobility mgmt.
Leveraging credentials, lateral movement	Identity	Multi-factor authorization, Identity & access mgmt
Elevation, permissions, persistence	Privilege	Privileged access/session mgmt
Recon, leverage, access	Apps	App-specific auditing, user activity monitoring, user behavior analytics
Exfiltration, encryption, fraud, esionage	Data	User activity monitoring, file auditing

Fine-Tuning your Cybersecurity GTM Strategy

Now, seven layers is a lot to take in as an MSP who's new to cybersecurity. Most MSPs start with the first three (perimeter, user, and endpoint) and evolve their offering over time. Additionally, many MSP-focused solutions offer a single product that addresses two or more of these layers at once, taking away the concern that you'll need to be a master of lots of different solutions just to get started.

When developing your GTM, consider the following:

1. **Determine what you're good at.**
   You won't have instant expertise in all things cybersecurity, but you do bring experience and skill set to the table. Figure out what your team is comfortable supporting and, perhaps, attempt to use the layers as a guide.

2. **Don't bite off more than you can chew at the start.**
   It's okay to start with an "essential" set of services. Just keep in mind that you need to differentiate yourself, so don't stay there too long.

3. **The solutions should help not hinder.**
   The solutions you choose should aid in delivering services by helping to lower the cost of delivery, assisting with gaps in expertise, and even automating some of the work that needs to be done.

THREE

Determine the Right Pricing Model

As you probably already know, pricing is the one factor that can make or break the success of an offered service. Too high and the customer is turned off; too low and there's not enough perceived value. Pricing in the MSP world requires the Goldilocks treatment: it needs to be "just right."

Unlike most of your other services, cybersecurity is a constantly moving target, which can make pricing it a challenge. After all, a predictable service offering equates to a profitable one. The unpredictability of trying to keep your customers secure can therefore impact profitability. So, it's imperative that you get pricing nailed down correctly.

Fine-Tuning your Cybersecurity GTM Strategy

Your pricing model needs to address a few things:

1. **It needs to be easy to understand.**
   Like every one of your other services, the pricing model should be simple to comprehend. Even with tiers of service, make it effortless enough for a customer to be able to understand scope and actual costs even, without you being present.

2. **It should demonstrate value.**
   The customer needs to see right away how the service justifies the expense. This can be a simple perceived cost/benefit ratio on the customer's part, or it can be based on how well your offering protects the customer against attacks. Offering tiers of service can also add value by giving the customer options and allowing them to choose the one in which they perceive the most value.

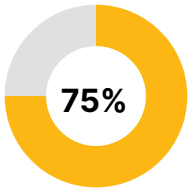
3. **It needs to focus on protection.**
   Because you can't predict the scope and frequency of attacks, it's important to keep the services centered on preventive measures. Threat detection should also be included, but steer clear of making remediation guarantees.

4. **Consider all your costs.**
   Cost is always a factor that impacts profitability. As you determine pricing, keep every cost factor in mind; these include labor and backend overhead, service delivery costs, and hidden costs (e.g., underutilization, ramp up time for new technicians, remediation costs, etc.).

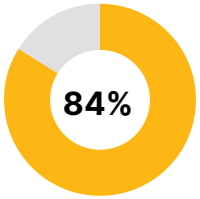
FOUR

Rethink How You Engage Prospects

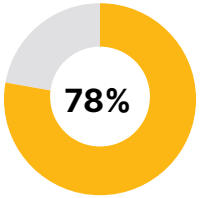
Assuming you're going to be looking for new customers with this service offering (in addition to selling it to existing customers), it's important for you to be thinking about how to engage prospects. The days of cold outreach are dead as 90% of buyers never respond to cold calls3. Instead, today's buyer is looking to establish connections with those they believe can assist their business. Business social media sites have become the primary vehicle for a number of aspects of the buyer's journey:



use social channels to inform themselves and evaluate vendors[3]



of CxOs/VPs use social to influence buy decisions[3]



of social sellers outsell those who do not use social media[4]

[3] IDC, Social Buying Study (2020)
[4] LinkedIn, Social Selling Index (2020)

Fine-Tuning your Cybersecurity GTM Strategy

Because the prospective customer is looking to social media, your goal is two-fold. First, you need to be wherever your prospect is online; second, you need to engage that prospect in a way that doesn't feel like an immediate pitch.

Consider the following engagement practices:

1. **Prioritize LinkedIn.**
According to the folks at LinkedIn, 80% or more of B2B social leads are generated on their platform each year. It makes sense, really. Where else in the world can you go to a single place and find multiple people in the right geography with the right title at the right kind of company that are the perfect contact to reach?

2. **Engage with Content.**
You only have a few minutes of a prospect's attention online, and a pitch as your initial contact is likely going to be met with a "no thanks." Why? Because there's no connection between the prospect and your business—yet. People today want to do business with an MSP that wants to invest in their success. So, consider using content that adds value for the prospect as a means of garnering their attention. Interacting with prospects via post comments, publishing relevant thought leadership, and interacting in groups are all ways for a prospect to "get to know" your business, creating a positive affinity and increasing the likelihood that they will be interested in the future.

3. **Be careful with prospecting emails.**
There's a very fine line between a wanted email and something that will come off spam-like, even when it's coming from a known entity. Create email messaging that is specific to your target and has a clear call to action (e.g., call, reply, or click a link). A personal tone tends to work better than one that's more sales-oriented. The personal tone creates authenticity and helps to foster a potential business relationship.

Building a Cybersecurity GTM Strategy that Works

The biggest challenge with bringing a cybersecurity offering to market is meeting the expectations of the prospective customer. From the very first touch, there's an expectation that you demonstrate value immediately through social media engagement and content. This is followed by an expectation that you can completely (100%) eradicate any and all security issues while meeting their specific security requirements. Then your pricing has to be simple, straightforward, and easy to understand. Lastly, you're expected to actually deliver a quality service.

It's an extremely tall order and you're going to need to make some changes to your GTM strategy to meet some of these expectations. Sure, making a customer 100% secure is never going to happen; but the marketing, selling, and delivering of your cybersecurity services will need to adjust to the current state of the market.

With some time focused on developing a GTM strategy that aligns with what your prospective customers are looking for—from end to end—you will find yourself delivering a security offering that gives your customer the ease and confidence they need, while being a profitable endeavor for you.

About the Author

Nick Cavalancia has over 25 years of enterprise IT experience, is an accomplished consultant, speaker, trainer, writer, and columnist, and has achieved industry certifications including MCSE, MCT, Master CNE and Master CNI. He has owned an MSP focused on the SMB, an enterprise IT consulting company, and today runs Techvangelism, where he serves the IT community as a technical evangelist, working with some of the most recognized tech companies today.

Nick has authored, co-authored and contributed to nearly two dozen books on Microsoft technologies, and regularly speaks, writes and blogs on a variety of topics including cybersecurity, cloud adoption, business continuity, and compliance.