Marketing & Selling to Cybersecurity Leaders

5 WAYS TO FAIL | 5 WAYS TO SUCCEED

magnetude

OPPORTUNITY AWAITS...

There's tremendous opportunity for cybersecurity vendors who can help chief information security officers (CISOs) and their teams thwart attacks and reduce risk for the business. The cybersecurity market is now valued at over $215 billion[1] and grew by 70% just between 2019 and 2023,[2] but estimates suggest that true demand for products and services could be as large as $2 trillion.[3]

However, it's not easy money—it needs to be earned.

Gaining trust remains one of the top barriers to sales—and the key and critical factor that CISOs and other security leaders value the most. The only way that cybersecurity vendors are going to be heard and noticed is by taking deliberate steps to establish trust with the audience.

New vendors bearing new products and services flood the market every day. With them come the attendant marketing messages, some more sensationalistic than others. It's adding up to a noisy market, especially with the advent of AI, where it's increasingly difficult for cybersecurity marketers to differentiate their brand and offerings.

Unfortunately, amid all the noise there are also some poor choices on the marketing front—in the form of buzzwords, inflated capabilities, lofty claims, and in the most extreme cases a fundamental lack of awareness of the role of the CISO in modern business. Sad, but true, key decision-makers in security tend to tune out marketers by default. The good news?

WITH A CONCERTED EFFORT, IT'S POSSIBLE TO TURN THE TIDE AND BREAK THROUGH.

CROWDED MARKET LANDSCAPE, LOTS OF NOISE

LESSONS FROM THE CYBERSECURITY TRENCHES

CISOs and security leaders are facing a harsh reality. A few lessons on what CISOs want us to know about them.

LESSON 1

THE CISO IS A BUSINESS EXECUTIVE.

CISOs don't have unlimited budgets, and they're not seeking to eliminate every risk. They're tasked with minimizing the risks that could hurt the business the most without hindering business stakeholder colleagues from generating revenue.

LESSON 2

SECURITY LEADERS ARE FIGHTING VENDOR FATIGUE.

The average security team manages 75 security products at once, and they're hounded by hundreds of different companies to add to that footprint. They loathe adding any more unnecessary complexity to their technical stack.

LESSON 3

MOST SECURITY TEAMS ARE OVERWORKED AND UNDERSTAFFED.

More than 9 in 10 CISOs will tell you that they and their employees are under moderate to high stress levels. They're balancing pressure from the board, escalating threat vectors, and a firehose of security alerts and false positives.

LESSON 4

SECURITY VETERANS ALWAYS TRUST BUT VERIFY.

Security professionals are inherently wary—they battle criminals for a living, after all. They'll want statistics, data, and customer stories to prove out vendor claims.

When cybersecurity vendors bring these truths to bear in product marketing, go-to-market strategies, and marketing campaign development, they start creating the kinds of nuanced marketing that engenders trust.

5 WAYS TO FAIL | 5 WAYS TO SUCCEED

Getting the message to CISOs and security leaders right means communicating in a way that positions vendors as trusted advisors. We've outlined five critical areas where you may be failing to communicate correctly–and provided some tips on how to change in order to succeed.

FAILURE #1

LEADING WITH FUD

CISOs are fed up with FUD. There's no quicker way to lose credibility with security leaders than to base marketing and sales campaigns primarily upon fear, uncertainty, and doubt (FUD).

Why? Security veterans live and breathe cybersecurity and know full well that breaches are an ever-present problem. They know the cost of a breach and are well aware of the risk of getting fired or even prosecuted. They're building out complex security practices that address dozens of different risk areas and racing to stay in front of threats like ransomware. CISOs feel first-hand the pressure of establishing a complete defense strategy and the frustration of tools that only add more alerts and complexity rather than adding more protection.

> ***If your content and pitch decks focus their messages on breach statistics and CISO anxieties, it's time to rethink that strategy.***

SUCCESS STRATEGY #1

FLIP FUD. FOCUS ON THE POSITIVES.

Security leaders want vendors to get to the point right away, explaining clearly how they help security teams solve a specific business risk or technical problem. Moreover, they mistrust any vendor who promises a silver bullet that's going to slay all their cybersecurity monsters at once.

Often, your internal technical resources or your company's CISO can be an excellent source for guidance on how to clearly communicate the problems you are solving—or the specific challenges the CISO is facing. Show you are on the same side—there to support them with your in-depth knowledge and solutions.

FAILURE #2

NOT KNOWING THE CISO'S M.O.

A big reason that many cybersecurity marketers resort to FUD is because they haven't done enough homework to truly understand their buyers. Sure, they may have identified the personas they want to target—be they CISOs, directors of security, boots-on-the-ground security analysts, or general IT managers at smaller organizations. But they may not go much deeper than that.

SUCCESS STRATEGY #2

GET CONNECTED AND THEN LISTEN!

The best cybersecurity marketers spend the time talking to real prospects and customers who fall within these persona categories. They strive to truly understand the realities of security professionals' daily work, and the fundamental business or technical problems they face.

KNOW THE AUDIENCE: HITTING THE MARK WITH MESSAGING

Trusted marketers not only promote products and services but seek to educate and inform around topics that really resonate with CISOs:

- REDUCING risk in meaningful ways, without being breathless or vague
- SHARING security research and technical knowledge
- MAKING security simpler
- MEASURING risk and bringing accountability and discipline to the security program
- COMMUNICATING risk to the board and business stakeholders
- REDUCING security friction

These are a few key examples, but there's obviously no set formula for which messages will work—the point is to start listening to the real business problems of CISOs and start structuring the solution and messaging backward from there.

One final thing to note is that the key persona may not necessarily be the CISO. But the mantra of 'know your audience' holds true regardless. Seek to understand their pain points and their level of technical expertise and adjust accordingly.

According to a survey of cybersecurity professional, almost half (45%) of companies still don't employ a CISO or equivalent[7].

FAILURE #3

A C+ IN BUILDING RELATIONSHIPS

Marketers can't force CISO trust. Establishing a relationship with the CISO community takes time, persistence, and some really good pull marketing tactics.

As we've mentioned, most CISOs default to ignoring vendors. That means they're sending email blasts directly to their spam filter and they're screening sales calls mercilessly. Rarely do CISOs say their preferred method of learning about vendors is through marketing collateral. Instead, they find products by:

- Identifying a business or technical problem
- Doing lots of independent research online and at industry events
- Getting a sanity check on the options through social media, industry groups and colleagues at other organizations
- Reaching out to the vendors who seem credible and worth a further exploration

That doesn't mean CISOs aren't ever open to sales pitches. In fact, they expect to see some kind of call-to-action on all of this content so they know where to go or who to talk to if they want more information about your product. And your team should always be ready to provide more—more technical details to back up generalized information, more case studies to show how products are implemented in the real world, and more customer references so that CISOs can verify your claims themselves.

SUCCESS STRATEGY #3

TIME AND TACTICS REAP BIG DIVIDENDS

So take heart, it's not impossible to get on a CISO's radar without relying too heavily on push marketing. It's just a matter of getting creative to create a volume and variety of content to establish passive touch points for the brand where CISOs are most likely to look. This can include offering up easy-to-find educational content, on-demand webinars, and contributing valuable thought leadership to industry publications or landing speaking engagements.

In another vein, marketers can establish trust by doing no-strings-attached community outreach and road shows around topics that matter. Similarly, they bolster credibility by regularly sharing research and security knowledge held by their in-house experts without necessarily pushing a product-driven agenda.

These kinds of pull tactics reap big dividends in trust and credibility—but they require investment and persistence to pay off. Just as there's no silver bullet product that will solve a CISO's security problems, there's also no magic wand to wave in cybersecurity marketing. It takes time and consistency to build momentum.

FAILURE #4

CHOOSING THE WRONG SPOKESPERSON

Finally, it's crucial that cybersecurity marketers deliver their messages through people that CISOs find credible. Spokespeople and internal thought leaders can make or break trust, and so organizations need to choose them wisely and train them well.

Many security vendors make the mistake of simply pushing forward a company executive or a technical leader as spokesperson because they're in charge or they have a great technical vision. But they may not be the right fit if they lack communication skills, if they're so focused on technology that they can't broaden out to talk about business context, or they're simply a technically brilliant but abrasive person who won't be relatable. On the flip side of the coin, another common mistake vendors make is letting the marketing people who are professional communicators do all the talking even though they don't have the kind of security pedigree a CISO can respect.

SUCCESS STRATEGY #4

FINDING THE RIGHT THOUGHT LEADER

A great spokesperson offers a balance of technical expertise, business know-how, and communication skills. Even if you don't have someone with the total package at the moment, it is possible to train in weak areas—particularly when it comes to communication. Being an effective influencer requires practice to stay on script, to stay pithy, to get a point across, and to still sound human in the process. The more the marketing team can do to develop those skills in their people, the better chance they have at building trust in the marketplace.

FAILURE #5

ALIENATING WITH AI

Artificial intelligence is everywhere right now, and that's not doing it any favors. CISOs are being bombarded by claims that AI can solve every cybersecurity pain point under the sun. And so many vendors say they have innovated breakthrough AI and successfully integrated it with their product line. These messages are so ubiquitous and hyperbolic that CISOs can't help feeling like the hype around AI is overinflated.

This rings especially true given the sometimes low quality of AI-generated content, from eBooks to emails, being served up to CISOs. Content produced primarily with AI and without the human touch can be bland and basic at best and completely irrelevant and erroneous at worst. In both cases, though, it sets a low bar for what AI can do and raises doubts about AI's capabilities—not just for content generation, but for cybersecurity.

Vendors are understandably leaning hard on AI right now, both as a product and as a solution, and while there are absolutely use cases where AI gives a big boost to efforts, a heavy-handed approach to AI may be having an unintended effect. Instead of driving interest, marketing that relies heavily on AI may be alienating target customers, depressing adoption rates, and damaging brand reputation.

SUCCESS STRATEGY #5

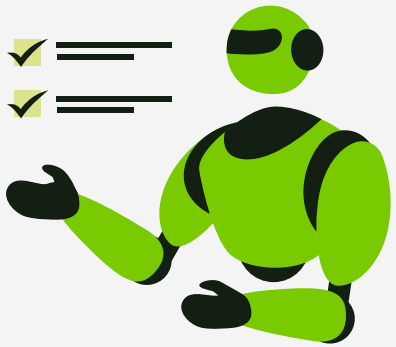
DULL THE CUTTING EDGE

Some CISOs feel dubious about what AI can do, but others are intimidated by this advanced technology or hesitant to grow the security stack. Overcoming all these objections takes a counter-intuitive approach: make AI seem less impressive.

Focus above all on the business case for AI, connecting the practical capabilities of the technology to the pain points that CISOs are suffering with. Security leaders aren't interested in staying on the technical vanguard, but they do have real (and worsening) problems that AI can solve. Highlight how to make AI seem like a valuable and viable addition rather than a flashy new feature—it's no longer new news.

Focus also on the simplicity of the AI, explaining how quickly and easily users can get fluent with the feature and how seamlessly it fits into existing workflows. CISOs who are weary of adding cost and complexity need to feel confident that AI will supply ample ROI with minimal disruption.

Rather than trying to impress them with AI, work to build their confidence with the technology as it pertains to your offering.



FINAL THOUGHTS

Just as there is no silver bullet to solve all the security challenges in the market, there is no single method to effectively gain and keep a CISO's trust and no single marketing message or program that guarantees success.

Building relationships with security leaders to truly understand their pain points and what does (and doesn't) resonate, how they seek and consume information and the best ways to 'speak' to them is an on-going process. CISOs want to be heard—and we should be listening.

THE MAGNETUDE DIFFERENCE

ABOUT MAGNETUDE CONSULTING

Magnetude is a B2B marketing firm that pioneered the fractional marketing approach for small to medium tech-related businesses. The firm offers a wide range of strategic and execution-focused marketing services to seamlessly dovetail into client growth goals. The company specializes in growth strategy consulting and fractional marketing department services including marketing strategy, messaging, branding, websites, content development, digital marketing, demand generation, sales and channel enablement, and brand visibility.

Magnetude services clients across the globe and brings specialized expertise in areas including cybersecurity, big data/ AI, SaaS products, B2B professional services, and emerging and established technology related products and services.is a B2B marketing firm that specializes in working with entrepreneurial companies looking to market the right way in today's increasingly complex environment by providing full-service, fractional marketing department services.

magnetude

Needham Heights, MA 02494
866.620.6629 | info@magnetudeconsulting.com
magnetude-consulting | @_Magnetude
www.magnetudeconsulting.com

Interested in hearing more about our capabilities?

CONTACT US