Insight Revenue

Selling Cyber 2026

Moving from Technical Validation to Organizational Readiness

Insight Revenue: Buyer Intelligence Series

Contents

Introduction

Cybersecurity is an unusually dynamic field. It also presents corporate buyers and the sellers of cybersecurity with some unique challenges:

1. On one hand, cyber companies do not have to work hard to create a need. Every day the headlines remind us, the threats keep coming. Some of these damaging attacks, such as the ransomware attack on Change Healthcare that disrupted healthcare services across the US, turn out to have been organized by sophisticated groups. Others, such as an attack on Transport for London turns out to have been perpetrated by a lone teenager, just because.

2. The exponential increase in threats, enhanced by AI and other technological advances, have meant an expansion in corporate budgets devoted to battling cyber attacks. However, even increased budgets are proving to be insufficient, with buyers increasingly trying to make the least bad purchasing decisions, working to identify the degree of risk they are happy to assume.

3. These forces: the large number of threats and the availability of budget, has meant a large influx of suppliers into the market. By one count, there are over 6,000 cybersecurity companies, each proposing different methods: everything from adopting a zero trust model to taking an adversarial approach. Underpinning these methods is a bewildering variety of technologies with AI being used to perfect social engineering as well as finding previously unknown software vulnerabilities to expose.

> "We can no longer ´do more with less.´ We must do different."
>
> – CISO, Global Financial Services Company

All of this is overwhelming to buyers who remain as worried about overspending as they are worried about potential breaches. This makes it very hard to prove value when leaders can see the cost and complexity of the stack without fully appreciating the risks being mitigated. As one client put it "if we do well, clients ask if they're spending too much but they fire us if we miss anything".

Understanding cyber buyers

The titles alone are bewildering. One prominent vendor's website lists 24 possible roles/departments who might be involved in making cyber security decisions, everybody from the Chief Information Security Office to Cloud Architect.

Reality is even more complicated with many others having a stake in cybersecurity purchases: the finance team will want to know about the ROI, legal will have questions around liability, the infrastructure teams will want to ensure that any new tools fit into their existing architecture, and important users will complain if too much friction is introduced into their day-to-day. While cyber companies know that the buying group is complex, we find that they often fail to provide their sellers with guidance that would allow them to more efficiently navigate and broker consensus within the buying group. Over time, high performers figure out a motion that works for them while others struggle to make sense of the buyer's world. While each company will want to craft its own set of personas, we find that the sellers benefit from being able to look beyond simple firmographics and start to classify their buyers:

1. Perhaps easiest to identify, how mature is the company? A small organization might still be grappling with the basics, needing to deploy a password management tool. More mature organizations will be keen to stay ahead of the curve, optimizing architecture and resilience, especially if they are in an industry that is perceived to be a good target.

2. Less obviously, does the company subscribe to one of the foundational cybersecurity theories or frameworks? A company deploying a more traditional castle-and-moat architecture might, for example, resist more Zero Trust-aligned solutions. And it's worth noting that even a small, new company might subscribe to an operating philosophy while a larger company, perhaps grown through acquisitions, will be struggling to make sense of a hodge-podge of systems and processes.

3. Somewhat simplified, does the company take a risk-based approach or a compliance-centered approach to cybersecurity decision-making? A company that takes more of a compliance-centric approach will be looking to "check the box" while a risk-led company will be looking for prioritized exposure reduction.

4. More difficult to identify, does the company see cyber as a cost or a source of business advantage? While most companies are looking to minimize downside risks, others are willing to invest in solutions that make them more productive and that deepen customer trust. Realistically, this is a smaller set of companies.

Sellers need this information to match their motion to the type of company and buyer they're dealing with. Some companies, given their solution set, will want to focus on a particular segment, focusing on best-fit companies.

Buyer Type	What They Care About	How to Sell
Immature + Compliance-led	Passing audits, minimal disruption	Lead with speed, simplicity, and "good enough" coverage
Mature + Risk-led	Reducing real exposure	Lead with architecture fit, measurable risk reduction
Hybrid / Fragmented	Integration, tool sprawl	Lead with consolidation, simplification, interoperability
Business-led	Growth, trust, uptime	Lead with revenue protection, customer trust, operational continuity

Irrespective of buyer type, we find that sellers need to be realistic about the amount of change that their customers are willing to make. Most companies will be working on evolving their cyber capabilities and so will need to understand how a new solution fits their existing ecosystem.

Demonstrating value

Cybersecurity value can be very difficult to prove. Buyers are often asked to justify spending that results in nothing happening. We find that sellers succeed when they are able to match the argument to the buyer, emphasizing different aspects of risk reduction, the operational impact and then business enablement. The table below, for example, is a snapshot of where different types of value arguments might be expected to resonate.

Persona	Most Resonant Value Arguments
CISO	Risk reduction, operational resilience, automation
CFO	Financial impact, ROI, insurability, fine avoidance
CIO	Resilience, integration, productivity
COO	Business continuity, process uptime
CHRO	Streamlining protocols, reducing staff complaints
Compliance / Legal	Regulatory alignment, audit readiness
CMO / Sales	Competitive differentiation, trust
Board / CEO	Strategic enablement, reputational protection
Business Executives	Growth enablement, trust, business uptime

What further complicates this is that these preferences are not fixed. It might also not be obvious where the power lies within a particular company. For example, at some companies CFOs are actively involved in all growth decisions, at others, the CFO might be most focused on budget. This means that sellers need to identify buyers as well as their relationship with each other. Who is likely to be a mobilizer? And who will they need to work with to obtain a budget?

Leaning into the change

In working with cyber companies, Insight Revenue has observed a persistent tendency to downplay the amount of change that more sophisticated and novel solutions may impose on the buyer. This is especially true if an organization is moving from a 'point-in-time security' to a more mature, continuously evaluated cyber stack. While nobody has ever thought that a check-list approach to cyber is the best, the reality is that a more sophisticated posture will demand a large upfront investment in terms of time and resources.

This is partly an issue of volume: continuous data requires different working practices. Rather than managing discreet projects, teams find themselves managing a flow. The goal becomes making sure that scarce resources are deployed to the highest-risk/greatest opportunity items instead of reacting to the last thing. Suppliers, we find, win once they show an appreciation for the dynamic and openly explore whether or not a potential client is ready for their solution.

It is also a part of needing to constantly negotiate solutions with different groups who may or may not report to the security team. A misconfigured cloud resource might belong to the DevOps team while an identity issue might sit with IT. More challenging yet, it might be that the issue sits with HR who is receiving complaints about employee time spent on protocol management.

The solution, Insight Revenue finds, is to lead with the implementation. The goal is to see if the client is ready to imagine a different way of working. If they're not willing, then the prospect is less qualified even if their need might be obvious.

Beyond direct sales

As with any other technology sale, the channel is of crucial importance, especially when it comes to accessing the midmarket and SMB segments. There are multiple players who handle everything from distribution to systems integrators who handle more complex projects. Depending on the product, Managed Security Service Providers might be of great importance as they will end up owning the customer relationship. Consultants and Advisory firms often perform an important gatekeeping role.

Tactically speaking, however, we find that it's relatively easy to form a partnership but that it is more difficult than anticipated to drive real business through the channel. For one thing, too many companies do not spend enough time on articulating a very crisp value proposition: something the partner can run with without having to spend too much time internalizing it.

Win-win relationships, we find, are based on having a jointly agreed plan. Both parties need to come together to identify where they might be able to drive the most business. They come together to identify the metrics that will allow both parties to evaluate each other. It's not enough to simply stand-up large goals. The evaluation process helps direct things like co-marketing resources and helps both parties hold each other accountable.

Being able to put together a joint plan demands a particular set of channel sales rep competencies. Channel sales reps typically need to be better at influencing and motivating than their peers. They will also find themselves needing to do more planning and project management. All of this is made easier if they are armed with insights and a budget they can use to help the partners improve their business.

Leading sales organizations, Insight Revenue finds, ultimately end up managing partners as an extension of their own sales force. They spend considerable resources enabling partners and on managing channel conflict. They are acutely aware that some conflict makes for healthy competition but that too much conflict can prove destructive.

Conclusions

Cyber sales often appear uniquely complicated. It is frequently a technical maze that requires broad organizational participation. Since the ultimate goal is prevention, identifying exactly how and where value is created remains a challenge.

However, complexity cannot be an excuse for vagueness. Insight Revenue finds that the most successful sellers do not simply present a better solution. They bring a clear hypothesis addressing three fundamental questions:

1) What does this reduce?
   This may be expressed in terms of risk, exposure, or incidents.

2) What does this replace or simplify?
   Too often we see sellers failing to put their solution into context. Ideally, you can identify what tools, processes or effort the solution replaces otherwise you are potentially just creating more noise.

3) What happens if the buyer doesn't change? Beyond identifying the nature of the risk, sellers should try to quantify what this might mean. For example, if an order processing system is offline what will that mean in terms of lost revenue? If there is a data breach, what will that do to customer confidence? Will your insurance company continue to provide coverage if you can't identify your exposure levels?

Perhaps the most significant shift for 2026 is the realization that the implementation conversation can no longer be deferred. When buyers are overwhelmed with options, head-nods regarding a problem or a solution are no longer reliable buying signals. There is a necessity to slow down the process in order to eventually speed it up. Engaging the buying group early around the friction of the fix has become a critical tool for qualifying readiness and establishing genuine trust.

We find that the teams experiencing the most success are those that collaborate during the proposal phase on a '**Joint Plan for Success**'. By mapping a path that accounts for both the objectives and the likely obstacles, these teams prove they are not just selling a solution. They are taking ownership of the outcome.

How Insight Revenue can help

Insight Revenue connects decades of frontline experience with a research-led approach to closing the gap between boardroom strategy and sales execution. Our **Insight to Value** methodology is an evolution of our work at CEB, Gartner, and Challenger, refined through hundreds of global sales transformations and continuous research into the modern buying environment. By operating as a strategic extension of your team, we move beyond the event-based nature of traditional sales training and focus on the sustainable behavior change required to drive predictable, high-quality revenue.

The Insight to Value model is built on three pillars:

1. Shaping Demand through Insight In a market saturated with over 6,000 providers, traditional feature first selling only adds to the noise. Most methods assume a buyer's self-diagnosis is complete, leading to reactive sales cycles that fail to gain executive traction. We focus on sparking deeper conversations that challenge the status quo and surface the technical and organizational obstacles the buyer may have overlooked. This approach earns the right to lead high level discussions that move beyond point solutions toward resilience.

2. Building a Collaborative Value Case Cyber buyers are increasingly skeptical of ROI claims that ignore the complexity of their existing stack and the trade off decisions they make daily. Meaningful alignment requires more than a technical bake-off. It requires a rigorous exploration of the barriers to change. Our approach quantifies the Cost of Inaction for all stakeholders, from the CISO to the Board. We help teams identify whether true organizational readiness exists before they commit significant resources to a deal, ensuring a focus on high fit, high probability opportunities.

3. Executing a Joint Plan for Success In the current buying landscape, finding a champion and having a strong product is no longer enough to win a deal. Success requires a shared roadmap. Our B.R.I.D.G.E.™ roadmap provides a modern approach to joint opportunity management, facilitating a process where both sides align on priorities and deployment realities long before the contract is signed. By coaching the buying group through the decision-making process, we earn the business by ensuring more effective adoption and a faster path to risk reduction.

Thank You

Insight Revenue would like to thank past and current clients for their help in writing this. Cyber is uniquely complicated and we have been honored to be allowed to help. A special thank you goes to Michael O'Neil of the Uptime Institute for all his time.

Insight Revenue
The Science of Growth

W insightrevenue.com
E info@insightrevenue.com

EMEA

Calle Sant Elies 34
Piso Atico P1
Barcelona, 08006,
Catalunya, Spain

M +34 678 536 345

AMERICAS

407 Ayre Street
Suite #1114
Wilmington, DE 19804
United States

M +1 202 744 2239