2025

Cybersecurity Buyers Report

ActualTech
BY FUTURE B2B

CYBERSECURITY MARKETING SOCIETY

New Threats, New Budgets, Same Old Humans

When we first released this guide in December 2024, the world was already sprinting into what we lovingly refer to as "Peak Cybersecurity Paranoia." Six months later? Turns out paranoia pays. We've seen funding flow faster than a zero-day exploit through unpatched firmware—and buyers are still very much in the mood to secure the bag... and the network... and the fridge, apparently.

The original report warned us that 2025 would bring increased attention to cybersecurity—and *spoiler alert*—it was right. Midway through the year, security is no longer just a line item on the budget; it's *the* line item. Budgets are still growing, but now they're backed by more urgency and shorter buying cycles. Marketers, if you're still waiting for "the right time" to launch that campaign—congratulations, it was four months ago.

WHAT'S CHANGED SINCE DECEMBER?

1. **AI's Hype Curve Has Entered Phase 2: Consequences**
   While generative AI helped your marketing team scale webinars and crank out content at breakneck speed, CISOs now face an inbox full of AI-generated phishing attempts that read like they were written by Hemingway. The market has matured, and buyers are now demanding AI-driven *defenses*, not just AI-fueled hype.
2. **The Rise of "Compliance-as-a-Conversion-Tactic"**
   Marketers, rejoice: The alphabet soup of cybersecurity compliance (NIS2, DORA, CCPA++, etc.) is now your top-of-funnel weapon. Buyers aren't just investigating vendors because of shiny features—they're looking for partners who make the pain of compliance go away faster than their auditors can say "gap assessment."
3. **Webinars Remain Supreme—With an Asterisk**
   Webinars still beat trade shows and podcasts, but buyer fatigue is real. Those 47-minute product walkthroughs with 39 slides? Yeah, no. The winners now are those offering snackable insights, immediate takeaways, and a live chat box that *isn't* monitored by a bot named Greg.
4. **Self-Service Grows, But So Does Confusion**
   The report correctly predicted the slow-but-sure shift toward direct-buying preferences. Mid-year? That's holding steady—but here's the twist: More vendors have slapped on a "Start Free Trial" button without adjusting for SMB onboarding complexity. The result? A surge in abandoned trials and follow-up support tickets that would make your customer success team cry.

5. **PoC Anxiety Is Spiking**
   Buyers now walk into every proof of concept like it's a hostage negotiation. Integration anxiety is real, data privacy scrutiny is up, and everyone's asking the same thing: "Will this thing *actually* work with our mess of a stack… and not get us on the front page of Reddit?" Vendors who lead with clear integration messaging are winning.
6. **The Human Problem Just Got… More Human**
   We used to say humans were the weakest link. Now, they're also the biggest wildcard. Social engineering has gotten creepier, deepfakes are in play, and your average employee's password is still Spring2025!. Messaging that tackles real-world human behavior—not theoretical security architecture—is what's cutting through.

WHAT TO DO NOW

If you're a security marketer:

- Lead with clarity, not cleverness.
- Build nurturing cadences that align with 3-to-6-month budgeting cycles (we still don't impulse-buy EDR platforms like we do socks).
- Show how your product integrates without requiring a blood pact and three weeks of professional services.
- And for the love of all things SOC 2, stop treating SMBs like enterprise-light. They're different animals—and they know it.

If you're in product or customer success:

- Circle back to your PoC onboarding. Streamline, simplify, secure.
- Get ahead of post-sale deployment delays by aligning expectations up front.
- And seriously, revisit your documentation. Some of it reads like it was written in Klingon.

We'll be back with the full 2026 update soon—but for now, take this data, sharpen your pitch decks, and keep fighting the good (cyber) fight. Just make sure your Zoom background isn't revealing your post-it note of admin passwords.

Executive Summary

Authors: Scott Lowe & Dr. John Honchell

Welcome to the 2nd annual cybersecurity buyer's report from Future B2B and ActualTech Media!

Our 2024 cybersecurity solutions buyer's report yields some evolutionary changes over our 2023 findings, but, more importantly, uncovers critical guidance for marketers, sales teams, and even product and customer success teams at cybersecurity vendors. Our report this year is an abbreviated, more consumable version of our 2023 report, but includes rich information for those at cybersecurity vendors that wonder what lies inside the minds of the buyers they're trying to reach. Some key themes emerged in this year's report, some surprising and some expected:

- **Theme 1.** As expected, smaller companies, which we define as those with 1 to 99 employees, act quite differently than their medium (100 to 999 employees) and large (1000+) counterparts. The results shared throughout this report reinforce this finding. While not necessarily surprising, making sure to remember this fact is important to marketers trying to break through barriers to entry across the spectrum.
- **Theme 2.** Cybersecurity gets increasing mindshare year over year, and 2024 going into 2025 is no exception. In all of our results, it was clear that this is a topic getting consistent attention from end users in 2024, who also indicated that it will be even bigger in 2025.
- **Theme 3.** The people problem is still the biggest challenge. For years, eternally fallible humans have been identified as the weakest link in the information security apparatus. Our findings this year do nothing to change this and, in fact, they just reinforce this issue. Solve the people problem and most of the security problems are also solved, it seems.
- **Theme 4.** Budgets are there and buyers are eager to spend. Respondents indicate that they have money to spend in 2025 and they will spend it faster than they were in 2024 with shortened budgeting cycles for cybersecurity solutions.
- **Theme 5.** Companies that can position their product as scalable, and target smaller companies with a direct buying option—with the ability to scale into larger companies—may have a winning strategy, especially if marketing can effectively communicate that.

Throughout this report, we've provided direct guidance on how to put into action activities that support the findings presented. We hope that this makes it easier for readers to see themselves in a solution rather than just be inundated with random data points.

Of course, there's a lot more detail as you read further. We look forward to your feedback and suggestions as we start work on the 2025 version of this research!

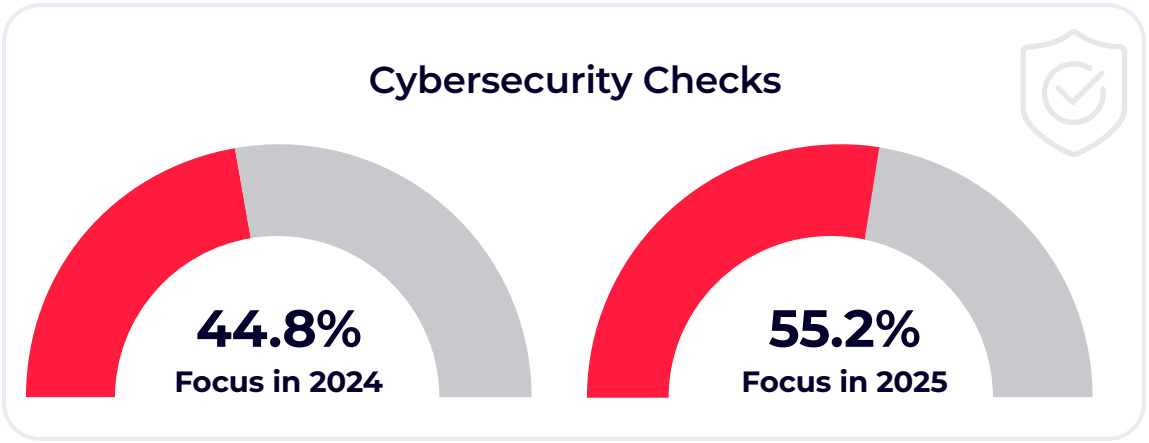
Cybersecurity Remains a Core Focus

KEY FINDING: CYBERSECURITY WILL SEE INCREASED ATTENTION IN 2025

Cybersecurity's heyday is far from over, as respondents indicate critical security services will remain a key focus in 2025 compared to 2024. For 2024, 44.8% of respondents indicated that cybersecurity received significant attention for their organization. For a 2025 projection, 55.2% of respondents say the same.

That's a massive 23% jump in anticipated focus in 2025, signaling that information security will remain a key priority for the coming year.

Putting this into action: For information security marketers, this is the definition of the iron being hot and you should strike. Buyers are primed to spend at increasing levels moving into the new year. Start laying the groundwork now with these buyers to reduce purchasing friction in 2025.

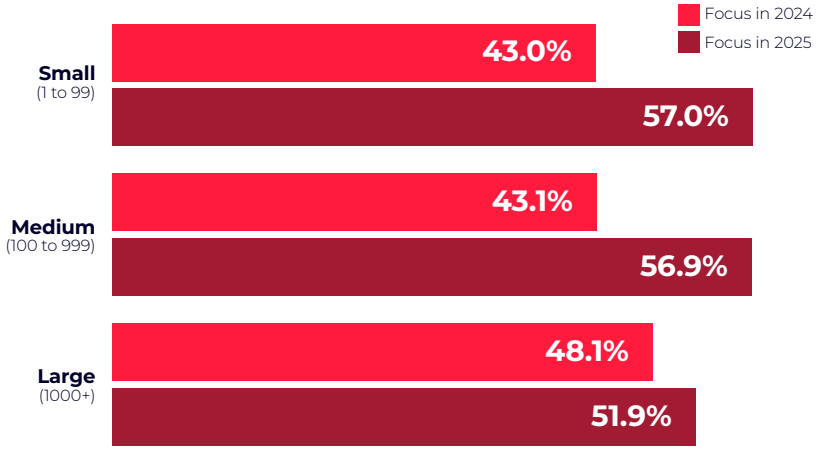


Small and Medium-Sized Organizations Plan Outsized Growth in Security Maturity

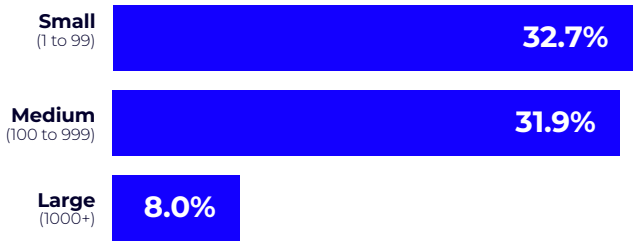
When we break down this survey point by company size, things get more interesting. Here, you can see that while large companies still intend to make cybersecurity a focus in 2025, it's only 8% more. Smaller organizations, though, are looking to increase their protection efforts significantly. 33% more small companies and 32% more medium companies will be increasing their focus on this critical service in 2025.

This isn't particularly surprising, though, particularly as we review other statistics elsewhere in this report. For example, you'll learn that far more large companies report that they're at the top cybersecurity maturity level, as defined by NIST. These larger organizations have substantially improved their security maturity in prior years, so fewer may need to increase their focus in 2025. It doesn't mean it's unimportant to them, but they've already put the work in and have less immediate need to increase that effort in 2025.

2024 vs 2025: YOY Focus on Cybersecurity



YoY Increase on Security Focus 2024-2025



Putting this into action: If you're looking for new pockets of opportunity beyond large companies, it's clear that there's a desire from smaller organizations to adopt more robust security programs. If your ICP doesn't include small and medium-sized companies, or those are part of your secondary strategy, now is the time to reconsider your approach. Smaller organizations will likely need a bit more attention than their larger counterparts, but there's also a far larger market to address.

If your solution currently emphasizes larger organizations, now may be the time to consider the addition of a small and medium business sized version of your product. While our report primarily focused on marketing and sales organizations, there are nuggets that may be of interest to your product management team as well.

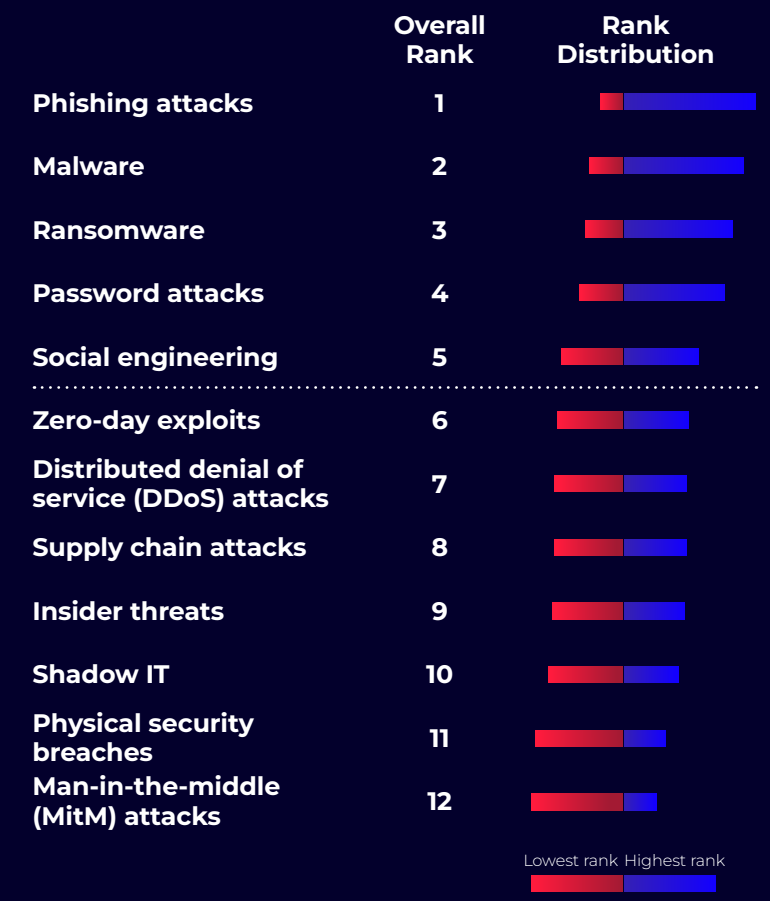
Yesterday's Problems Are Also Tomorrow's

KEY FINDING: THE ETERNAL WEAKEST LINK REMAINS THE HUMAN

If your company provides security tools intended to address the human weakness side of the security equation, you're (still!) in luck in 2024 and going into 2025. By far, respondents ranked threats most often arising to the human element as their key security priorities … again. From phishing attacks that top the list to ransomware, which is often the end result of human failure, to preventing password attacks and reducing the likelihood of successful social engineering, survey respondents are focused on reducing the potential for their people resources to create security incidents.

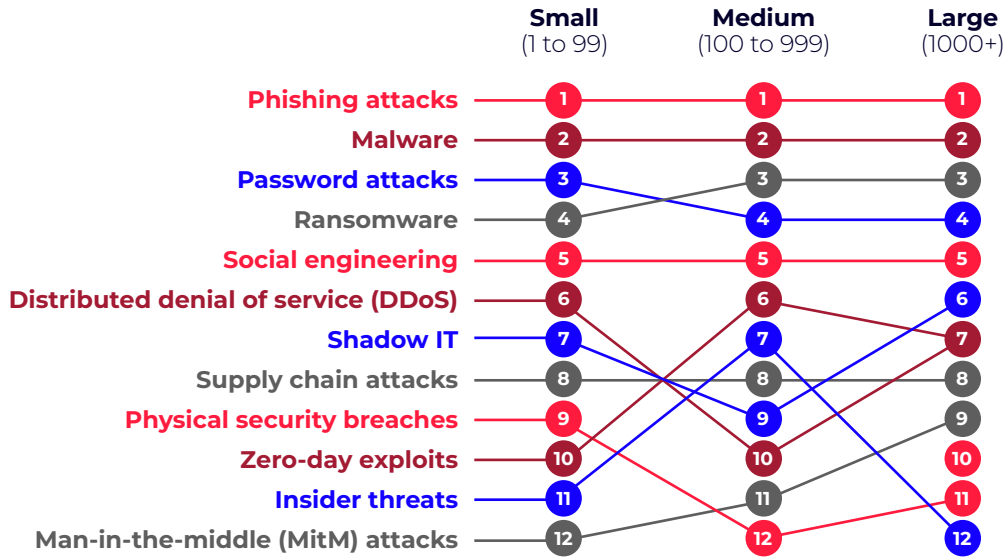
Putting this into action: Regardless of your solution, marketers can almost always use a human angle to demonstrate how their product and people intersect. Please don't stop your other efforts—they're still important—but double down on marketing activities that relate to the frailty of the human in the information security chain. Regardless of what kind of cybersecurity service you provide, you might consider partnering with vendors offering training services, too. At the very least, it could be a powerful marketing channel for you.

When it comes to security, what threats are you prioritizing right now? Place in order of priority:



KEY FINDING: COMPANY SIZE DOESN'T IMPACT HUMAN-RELATED RANKINGS, BUT IT DOES IMPACT THE REST

An interesting dichotomy emerged when breaking down this data point by company size. With minor exceptions, the top five potential threats were ranked the same, with most of these concerning human security. Once we got to items less directly connected to humans, the perceived severity changed dramatically based on the size of the company.



Physical security appears to be much closer to "largely solved" than was true in the past. This isn't a huge surprise as everything evolves and with bad actors more often than not operating from foreign soil, physical security is less of a concern today.

Putting this into action: If your primary focus is on the human aspect of cybersecurity, there's not a lot to change based on this finding. If, however, you want to differentiate some of your messaging around different prospect company sizes, consider how your solution matches the ranked importance identified here. If your solution, for example, revolves around zero-day exploits, you might emphasize this more with medium- and large-sized companies, but deemphasize it a bit for smaller ones, or even slightly adjust your ICP to take this into consideration.

A note to vendors who have small and medium sized companies in their ICP: while we aren't necessarily proponents of scaring people into submission, some reasonable fear-based messaging or messaging around lagging behind larger companies may resonate. It's not quite FOMO but fear of becoming an easy target. Bear in mind that there is a critical difference between using fear as a positive motivator to action and using fear to such a degree that you lose credibility, so find the line and walk it carefully.

SHADOW IT GOES INTO THE SHADOWS

Not long ago, Shadow IT—operating software tools not formally sanctioned or approved by the IT department—was cited as one of the most pressing issues in the industry. Today, it's No. 10 of 12 priorities overall. This raises some interesting questions: Has IT governance evolved to support more third-party tools than were allowed in the past, or do IT decision makers simply understand that shadow IT is going to happen anyway, so IT now focuses on some of the potential downsides, such as the human-induced outcomes discussed elsewhere?

The one notable exception is in smaller organizations, which ranked Shadow IT at 7 out of 12 priorities. In general, smaller organizations often lag their larger brethren in overall technical maturity, which includes establishing governance, so it's not too surprising to see Shadow IT still a more substantial issue for smaller companies.

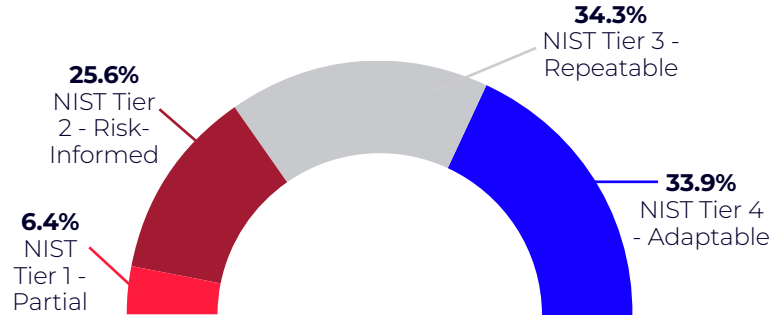
Cybersecurity Maturity Still Has Room To Grow

KEY FINDING: 32% OF ORGANIZATIONS REPORT RELATIVELY LOW CYBERSECURITY MATURITY

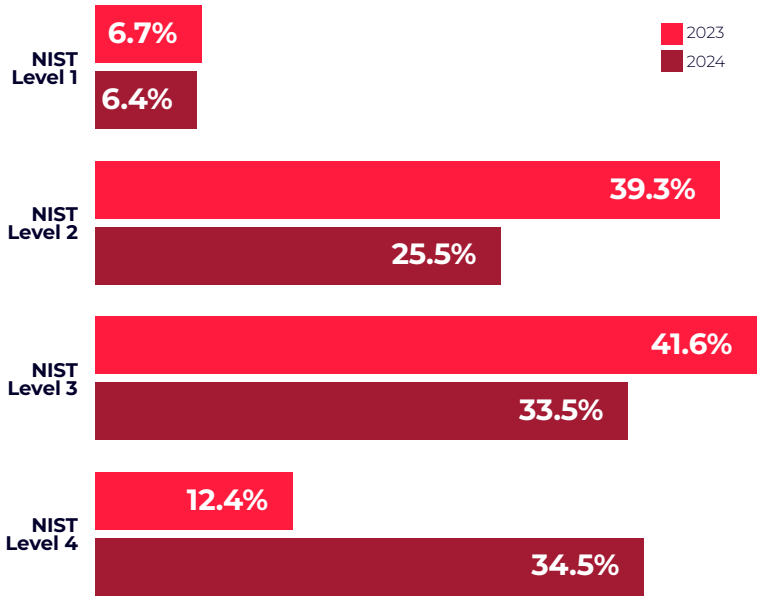
At first glance, this chart seems to be good news with very few organizations identifying at the most basic NIST level - Tier 1 Partial. These organizations have no formalized security processes in place.

A full 68% of the total respondent pool identify as Tier 3 or 4, Repeatable or Adaptable, indicating a high level of maturity in information security processes.

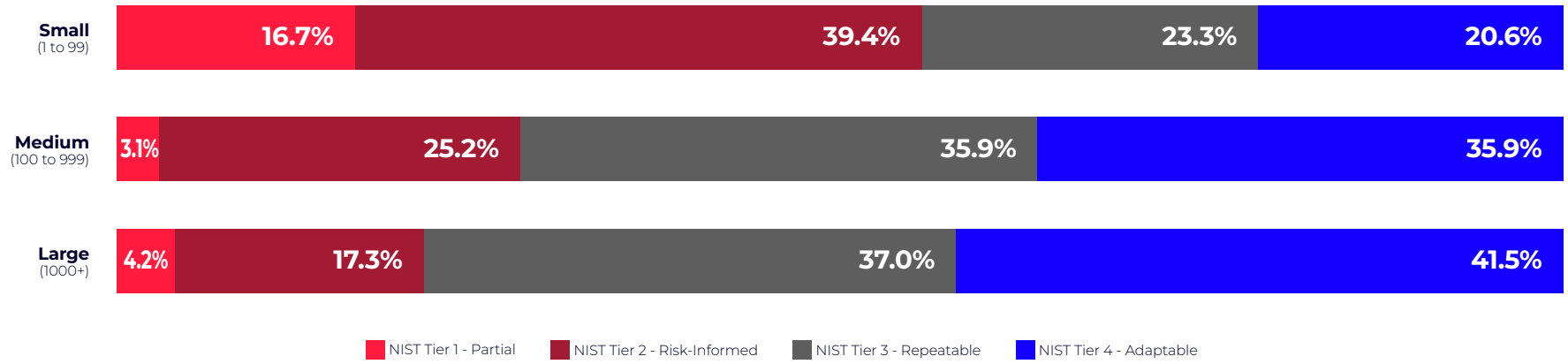
There is some good news in this data. Compared to last year, far more respondents report that they're at a high level of maturity. The number of respondents indicating that they're at NIST Tier 4 roughly tripled over 2023. An important caveat is that this is self-reported information.



Cybersecurity Maturity YoY Change



NIST Maturity by Company Size



Putting this into action: For security solution marketers, use this information to tweak your messaging based on target client size. When you're approaching larger organizations, assume that they have the basics handled and focus on how your solution solves higher-order problems or solves real business challenges. If you're marketing to smaller companies, you're well served to include what might feel like painfully basic guidance. Remember that everyone starts at the beginning and some of your clients are earlier in their security journey.

KEY FINDING: LARGER COMPANIES ARE BETTER OFF THAN THEIR SMALLER COUNTERPARTS

However, it's quickly revealed that company size plays a significant role in security maturity. In fact, 17% of companies with 1 to 99 employees are at the most basic cybersecurity maturity level while just 3% and 4% of medium (100 to 999 employees) and large (1000+) employees are at this level, respectively. The larger the organization, the more likely it is that these organizations have adopted a more mature cybersecurity posture. Smaller organizations are one-half as likely to have achieved the highest level of security maturity as their larger counterparts.

As disappointing as it sounds, this makes sense. Smaller organizations don't always have the same level of investor, regulator, or client pressures to adopt highly mature security solutions and robust security maturity is one of the common areas that scales by necessity as a business grows.

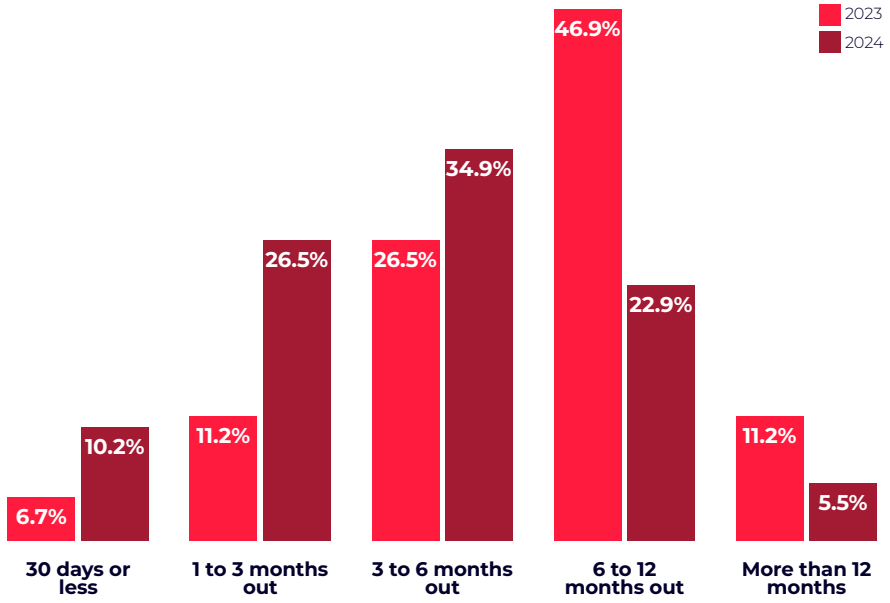
Marketers and Sellers Need a Cadence

KEY FINDING: PLAN ON A MULTI-QUARTER SALES CYCLE

While there will undoubtedly be some variance based on the size of a purchase, our question was designed to look for general guidance on how much lead time organizations give themselves when budgeting for cybersecurity solutions. As you can see from the chart, this is almost a textbook bell curve. Just 10% of respondents move fast, budgeting only 30 days out. 35% budget 3 to 6 months in advance, and just under 6% spend over a year lining up funds for new security projects.

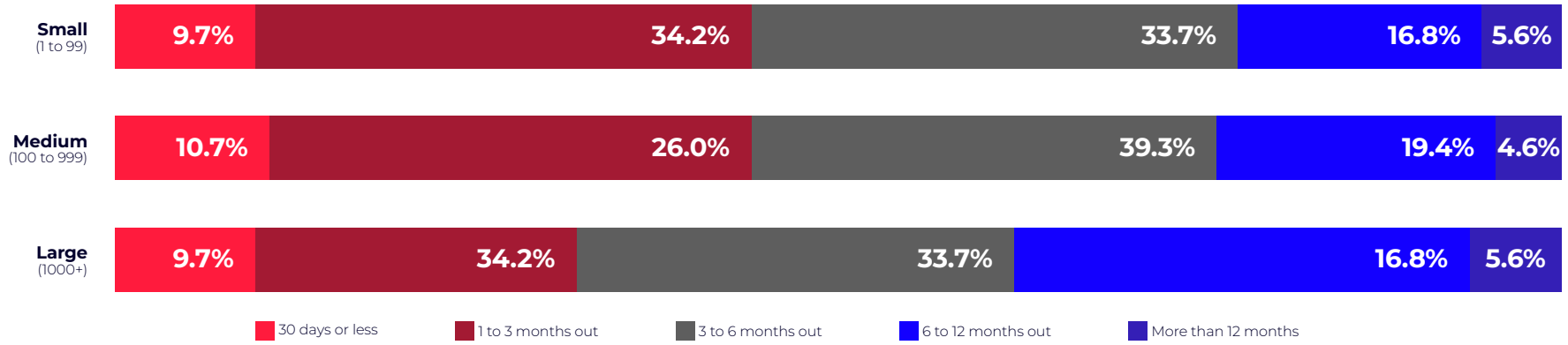
Organizations today seem to be moving far faster than they were just a year ago, though, at least in most cases. Last year, just 4.1% of respondents got budget approval in 30 days or less. This year, that more than doubled to 10%. Likewise, companies buying in 1 to 3 months more than doubled over 2023 respondent feedback. On the other end of the spectrum, there are far more companies this year taking more than 12 months to pull together budgets for cybersecurity solutions. The end result is something of a mixed bag, but with more positive than negative for security vendors.

Budget Planning Horizon for Cybersecurity Purchases



Putting this into action: This is critical information for your sales and marketing teams to understand and integrate into their cadences. In most cases, your target customers aren't sitting on a laptop frantically mashing the "Buy Now" button as soon as they identify a need. Almost one-third of them—28.4%—take at least 6 months to get budget planning in order. As we know, time is the No. 1 killer of deals, so it's vitally important that your sales and marketing teams work in lockstep to keep prospects respectfully engaged throughout their internal budgeting processes.

Cybersecurity Budgeting Planning Time by Company Size



Given the budgeting and purchase timelines involved, prospects will need many touch points, awareness efforts, check-ins, and value-added offers throughout the process to stay top of mind and in the consideration stage. Plan your marketing around this length of cycle.

To think about: What can you do to get in front of the budgeting process with clients? How can you help them plan their budget? What suggested solutions can they bake into their budgeting process?

KEY FINDING: LARGE COMPANIES PLAY BY DIFFERENT BUDGETING RULES

Large companies have extended budgeting cycles compared to their smaller counterparts for cybersecurity solutions. This isn't a surprise, necessarily, but it is something your sales and marketing teams need to take into consideration. In our research, almost 38% of large companies take 6 or more months to plan project budgets, while just 23% to 24% of smaller companies do the same.

Putting this into action: For marketers and security vendor sales teams, make sure you set appropriate internal expectations with regard to expected close times for deals. Since company size plays a big role in budget and lead times are different for larger organizations, ensure that your cadence and nurture processes take these differences into consideration.

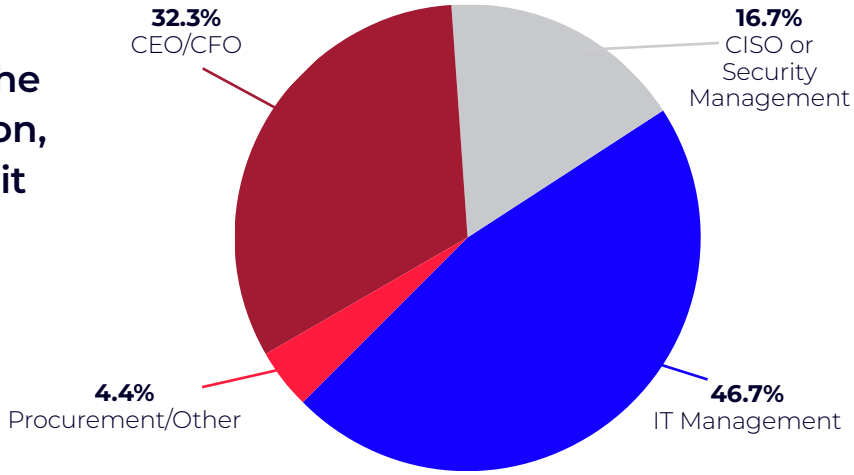
One of the "emerging B2B trends" is the deployment of self-service offerings, and while everyone is clamoring to tailor these offerings, the end-buyer data suggests this will be a slow up-take for larger organizations, but tailoring such a solution for smaller organizations may be a winning strategy.

Security Buying Approval Comes from Everywhere

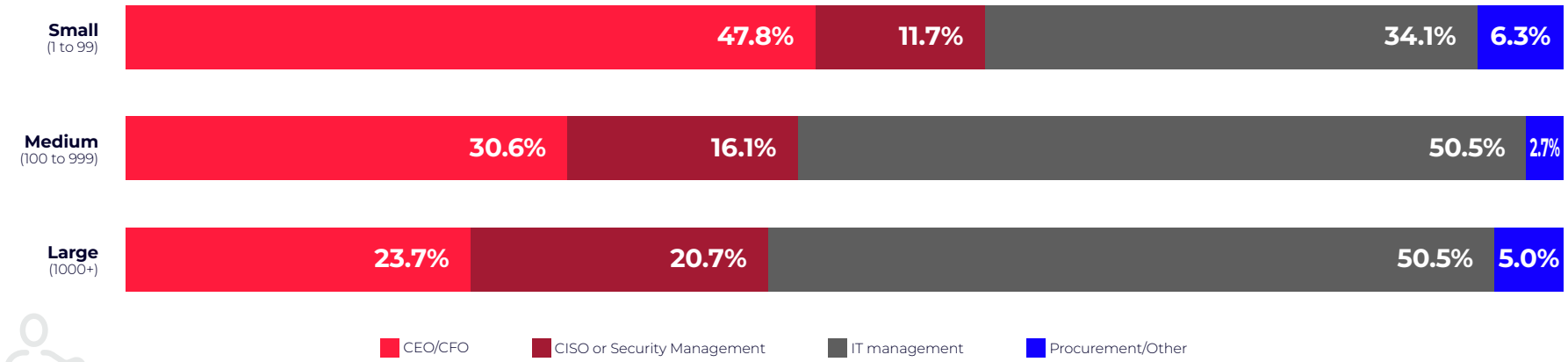
KEY FINDING: IT MANAGEMENT LEADS THE PACK, BUT CEOS AND CFOS DON'T SIT SECURITY OUT

Most sales and marketing teams want to know who makes final buying decisions in their client organizations. Executive-level leaders—the CEO and CFO—generally have the final say in just under one-third of our responding organizations. The biggest decision-maker set is, unsurprisingly, IT management, who has the final say about 47% of the time. The CISO or other security management takes the lead about 17% of the time, while procurement and others are the lead in a minimal number of companies—about 4%. As a caveat, it's important to remember that the security and IT functions are combined in many places, so several CISO responses are likely included in IT management.

When it comes to the final decision, who does it sit with?



Security Solutions – Final Decision Makers by Company Size



KEY FINDING: COMPANY SIZE HAS SIGNIFICANT IMPACT ON FINAL SECURITY PROCUREMENT DECISIONS

Unsurprisingly, smaller companies have a lot of involvement from the CEO and CFO on purchases of all kinds. Almost 50% of small companies in our study require a sign-off from the CEO or CFO as a final step in procuring a security solution. As organizations get larger, a lot of that decision making gets delegated to the CISO or IT management. In large companies, the CEO and CFO are present less than one-quarter of the time, but combined, just over 71% of these organizations delegate these activities to trusted leaders managing security or IT. In a tiny number of cases, final approval happens in the procurement department or some other far-flung corner of the organization.

Putting this into action: As you develop a marketing communications strategy, understand who will make the final purchasing decision and tailor your outreach materials toward that role. Bear in mind that this is just the final decision maker. There's almost certainly a much larger buying group that includes appropriate representation from all levels of the organization, so don't completely ignore the other personas you may want to target. It's still important to ensure your message reaches the individual contributors that will inform the decision of the person identified in this chart.

Trusted Sources Rule the Solution Education Roost

KEY FINDING: ANALYSTS, FRIENDS, AND WEBINARS ARE TOP-RANKED SOURCES OF SOLUTION EDUCATION

Regardless of company size, survey respondents prefer to turn to analyst reports, recommendations from industry friends, and webinars as their source of education when it comes to educating themselves on new cybersecurity solutions. This isn't really too surprising as all three of these channels have options to provide people with unbiased, on-demand information.

Trailing the pack are live trade shows, social media, and podcasts. Webinars beating out trade shows is not surprising at all, since trade shows require a more expensive and time-consuming commitment from people that generally have very full plates. Webinars are about as on-demand as it gets, and channels in that space do fantastic work in providing viewers with what boils down to speed-dating for new solutions to help busy IT pros and decision makers more quickly assess their options.

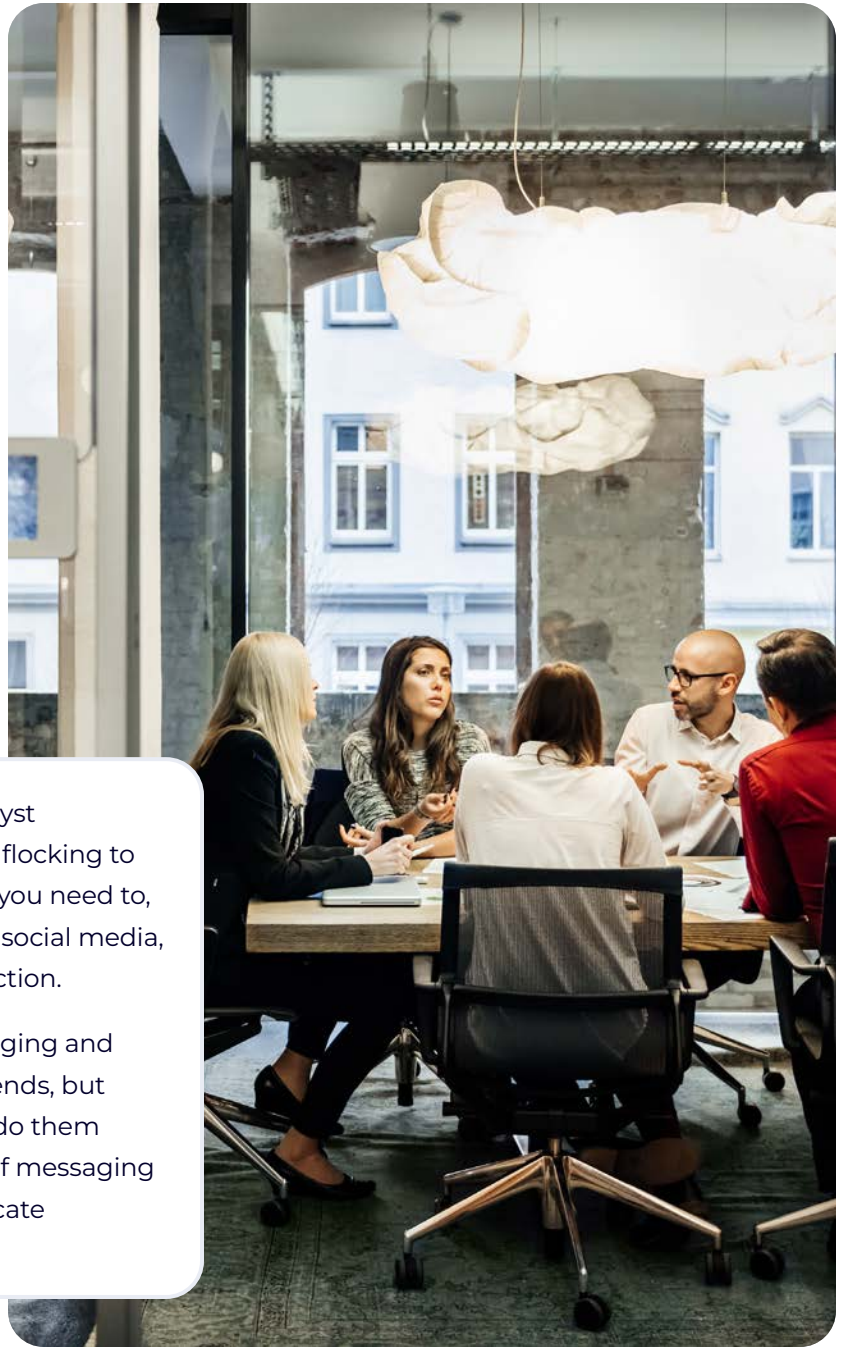
Where do you typically like to learn about new cybersecurity solutions?

1. Analysts reports
2. Recommendations from indsutry friends
3. Webinars
4. Trade shows
5. Social media
6. Podcasts

Social media's position toward the end of the pack is also somewhat unsurprising, particularly as those channels have become more splintered over the years.

Podcasts have always been at or near the bottom of the response list in our research. As some podcasts sport millions of listeners, it is sometimes baffling that they're ranked so low by end users. However, those massive podcasts are only sometimes in the tech space (although there are some fantastic ones). Podcasts are often also used as silence fillers during commutes, and getting real value from them requires more listening concentration. Further, many podcasts focus more on general tech education, trends, and consumer IT than business IT, which is far more niche.

Amazingly, when analyzing the content both by company size and general role (e.g., C-level, Security Management, and so forth), the rankings were identical. We expected to see some difference in the ranking, but there was none.



Putting this into action: This is easy: double down on your analyst relationships, case studies, and webinar investment. People are flocking to those resources to learn about what's coming down the pike. If you need to, reallocate budget somewhat away from in-person trade shows, social media, and podcasts in favor of these activities that get more prospect traction.

We'd be remiss to not remind you that you don't control the messaging and content in analyst reports and recommendations from industry friends, but you can fully manage these in webinars you operate, whether you do them internally or with a partner like Future B2B and ActualTech Media. If messaging control is critical to you, your top way to reach people eager to educate themselves on new solutions is to amp up your webinar output.

Organizations Are Getting Proactive About Security

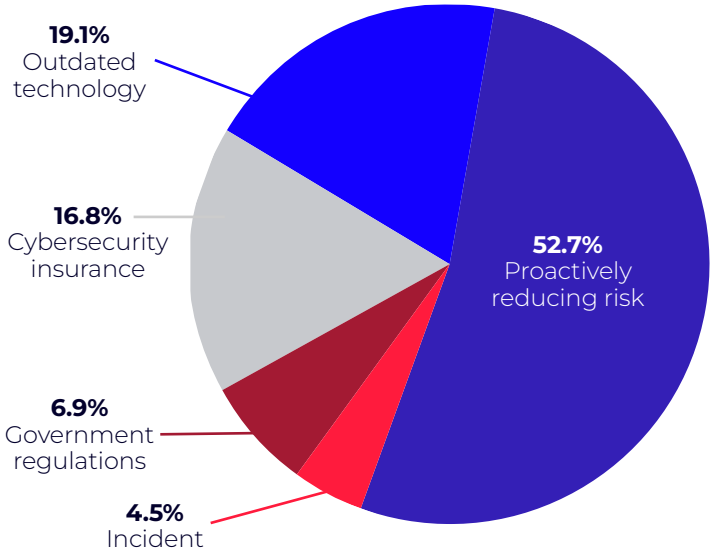
KEY FINDING: 53% OF RESPONDENTS ARE GETTING AHEAD OF THE GAME

For this year's set of responses, we asked respondents to identify the key motivator that makes them acquire new security solutions. For over half of them, finding ways to proactively reduce their risk or close security gaps was identified as the main reason. The rest identified motivators that we would define as more reactive in nature.

As government regulations on cybersecurity increase, organizations are reacting to that reality. The same goes for requirements imposed by cybersecurity insurance policies. Of course, in the world of technology, there's always technical debt to contend with, and security is no exception, with 19% of respondents replacing outdated solutions.

In what seems like good news to an extent, just over 4% of respondents indicate that they're *so reactive* that they wait until an incident before procuring a security solution.

Primary motivator for engaging in a new solution purchase

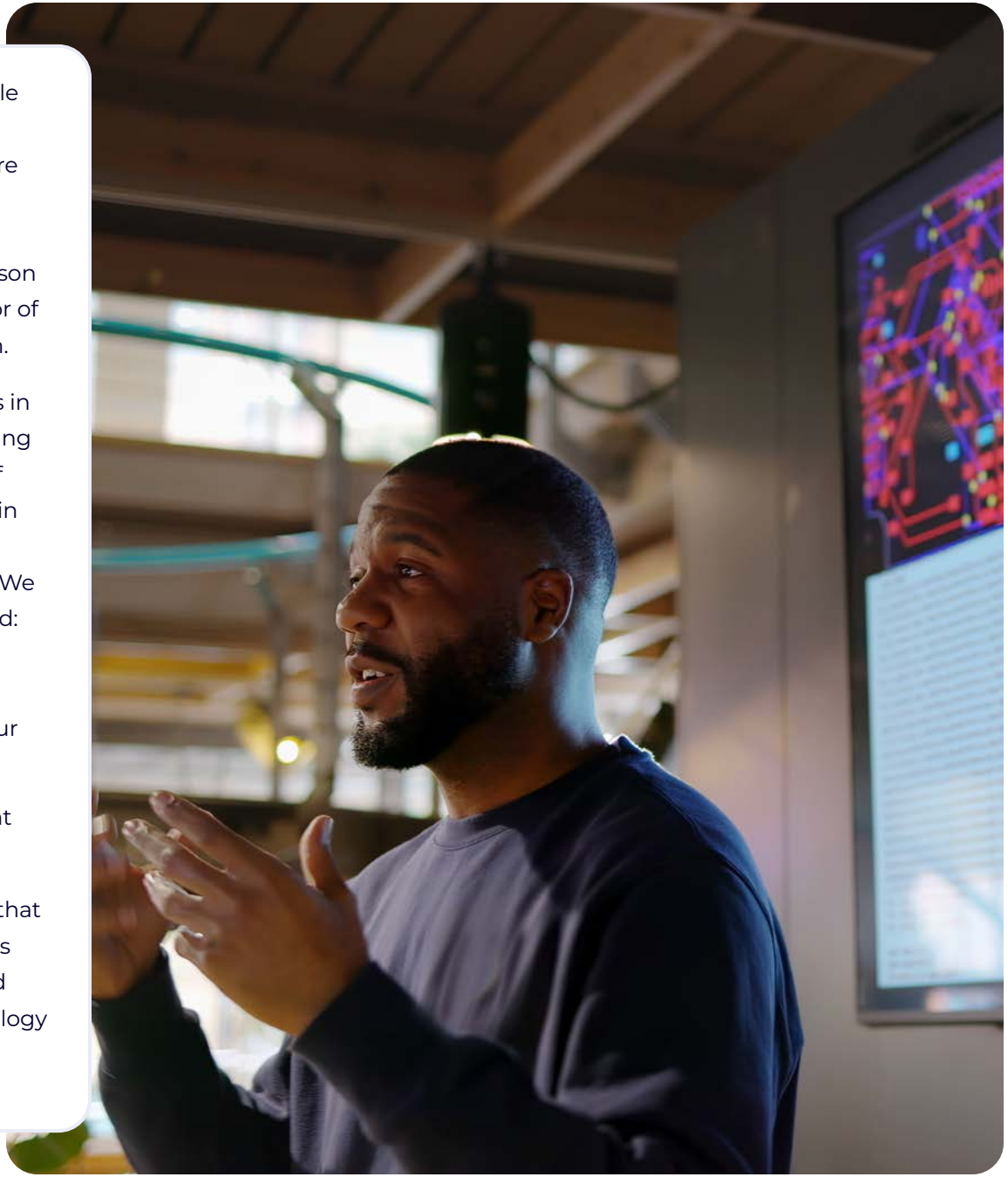


Putting this into action: This is easy: double down on your analyst relationships, case studies, and webinar investment. People are flocking to those resources to learn about what's coming down the pike. If you need to, reallocate budget somewhat away from in-person trade shows, social media, and podcasts in favor of these activities that get more prospect traction.

There's an incredible opportunity for marketers in this data point. There are a plethora of messaging opportunities that can be leveraged for each of these areas, and you'll undoubtedly hit on a pain point no matter which direction you go. Create robust messaging around each of these areas. We see significant messaging opportunities around:

- Future-proofing security tools
- Closing the gap before insurance forces your hand
- Staying on top of ever-evolving government regulations

And the list goes on. Come up with a cadence that provides prospects and even current customers with ongoing guidance for staying current, and you'll not only be a trusted security and technology partner but also a trusted thought leadership partner.

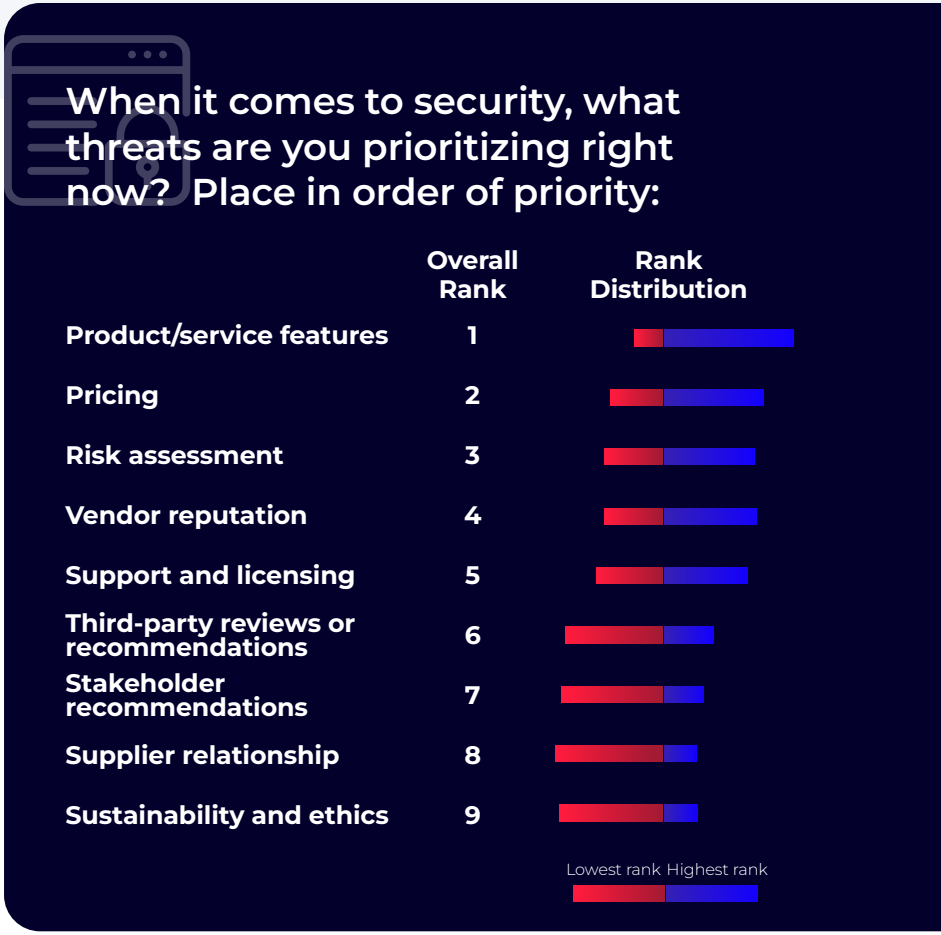


Product Capabilities Reign Supreme in Vendor Bakeoffs

KEY FINDING: IN ALL CASES, CUSTOMERS CARE MOST ABOUT PRODUCT FEATURES OVER ALL OTHER PARTS OF A DEAL

Even though sales and marketing people often end up in tense negotiations on price as deals progress, by a wide margin, respondents admit that product features and capabilities are the most important considerations in their purchasing process. Although this seems obvious, when mired in the swamp of negotiations, it may not always feel like that!

Of course, price is a significant factor. It's No. 2 on the priority list. Beyond that, the potential level of risk in a solution, your company's reputation, and your support capabilities were all ranked very close to one another.
Less important were third-party reviews and recommendations, although we hesitate to say that these are unimportant.
Remember that this was a ranked choice question, so these are all important considerations with respondents simply ranking them in the order of importance.

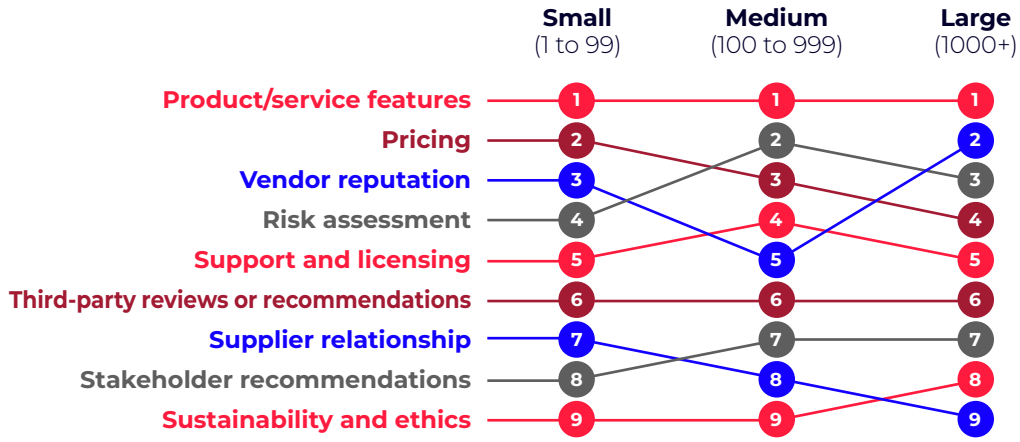


Putting this into action: Keep your capabilities at the forefront of your marketing messaging, particularly in your nurture programs. Play up your reputation and your support capabilities. Deemphasize messaging around sustainability (which is really disappointing to actually write out!), but bear in mind, again, that this ranking doesn't mean that those things aren't important, but they're just less important as compared to other factors.

KEY FINDING: LARGER COMPANIES PLACE LESS IMPORTANCE ON PRICE THAN SMALLER ONES

It's not exactly a secret that larger companies don't often place as much emphasis on the price of solutions they acquire, instead favoring the potential benefits that they're getting with a solution, but it was still interesting to see that, as we progress through our three company size silos, price drops down the list by one rank each time. And, for larger companies, the company's reputation is second only to what the product actually does.

What is your typical decision criteria when selecting vendors?



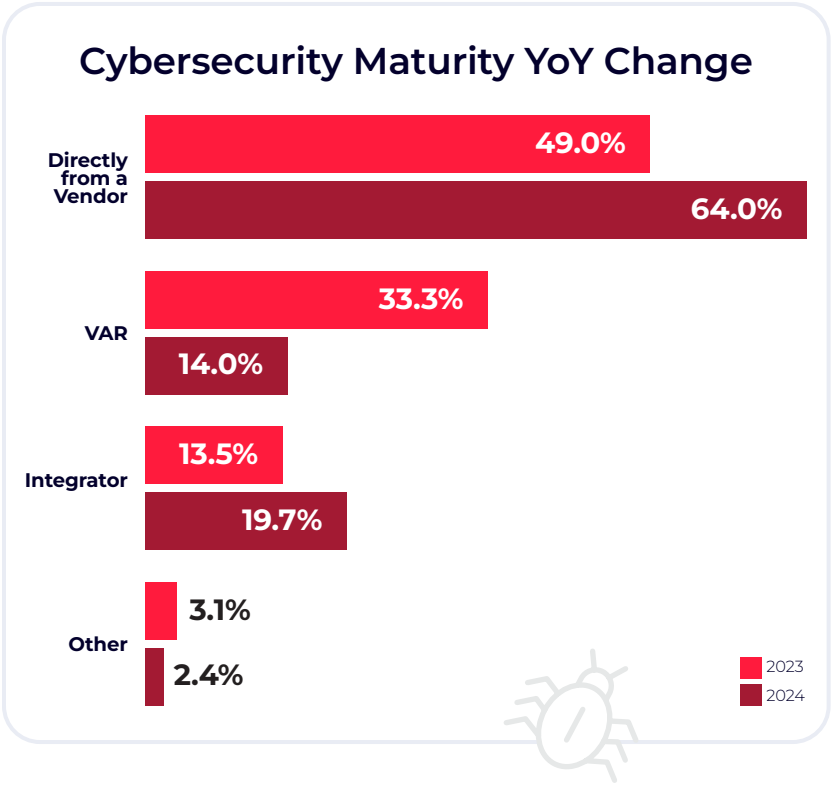
Putting this into action: Stay out of the news for the wrong reasons :-).

Direct Sales From Solutions Vendors Skyrocket in Popularity

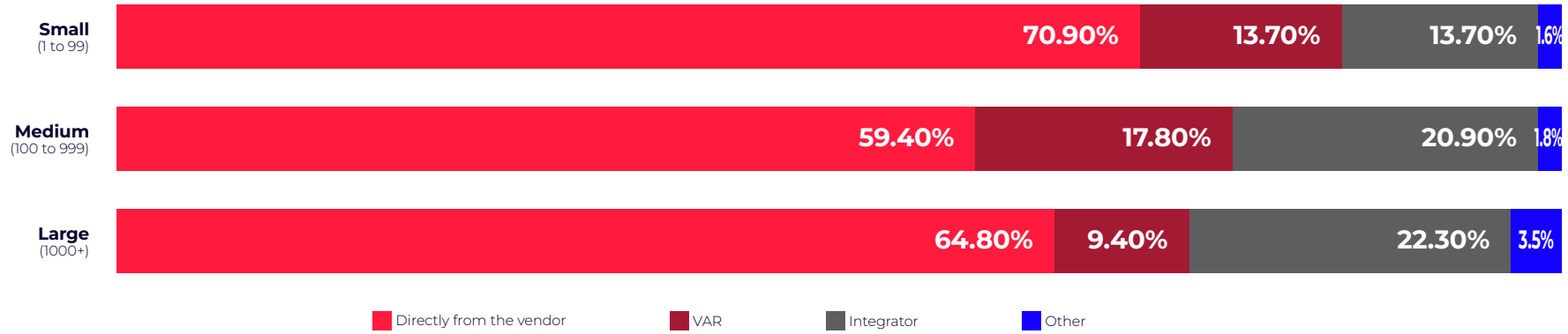
KEY FINDING: SOLUTION VENDORS AS A PREFERRED SOURCE JUMPS OVER 30% YEAR OVER YEAR

In 2023, 49% of respondents indicated that they prefer to procure solutions directly from vendors as opposed to VARs, Integrators, or other sources. In 2024, solutions sourced directly from security vendors is the preferred response by 64% of respondents, a jump of over 30%. It's important to note that this doesn't mean that everyone is heading to your website to Buy Now, but most *want to*.

The channel remains a critical part of the technology solution ecosystem, but direct sales and full-service integrators—those with an emphasis on solution selling vs. product sales—are emerging as significant competitors to the land of the VAR, which used to be seemingly impenetrable.



Preferred Cybersecurity Solution Source by Company Size



KEY FINDING: SMALLER ORGANIZATIONS - TO AN EXTENT - PREFER TO GO DIRECT

We're not getting too excited by this statistic but are including it more because it's more surprising than particularly useful. Yes, there's a big difference between small and medium organizations that prefer to go direct when possbile - 71% vs. about 59% - but that gets pretty much eliminated once we include large organizations in the mix, of which about 65% prefer to go direct. We expected this result to have a greater slant toward smaller organizations preferring to go direct. As such, it's included here primarily as an interesting data point, but we don't have a lot more to say about it.

Putting this into action: This one is difficult to guide as so many of our cybersecurity vendor partners need to rely on the channel. It makes it challenging to recommend moving to a more direct sales model, particularly as this is primarily a preference question rather than an action question. And, it's not possible for many, anyway.

In a perfect world, most companies would likely love a direct sales model, but it's not feasible for many. You need VAR and integrator distribution to reach a large portion of the market.

So, ask yourself a few questions: What's your current distribution strategy for VARs and integrators? Are you providing your VAR or integrator partners all the marketing support you can? Are you running programs with those VARs that will help them put you to the front of the line as they go to market?

If a deal originates with you directly but the buyer wants to go through their VAR or an integrator, do you have the relationships in place to ensure that deal doesn't fall off the table or get routed to another player who is somehow incentivizing the VAR or integrator to push their solution?

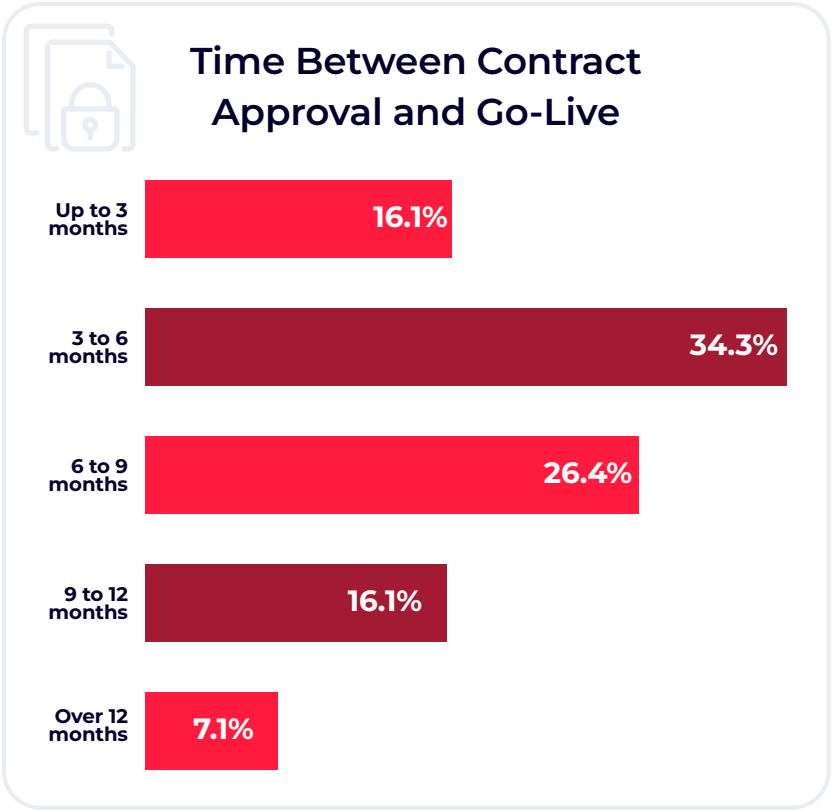
Security Vendors Need Patience with Client Deployment Timelines

KEY FINDING: ONLY ONE-HALF OF PROJECTS DEPLOY WITHIN SIX MONTHS OF CONTRACT APPROVAL

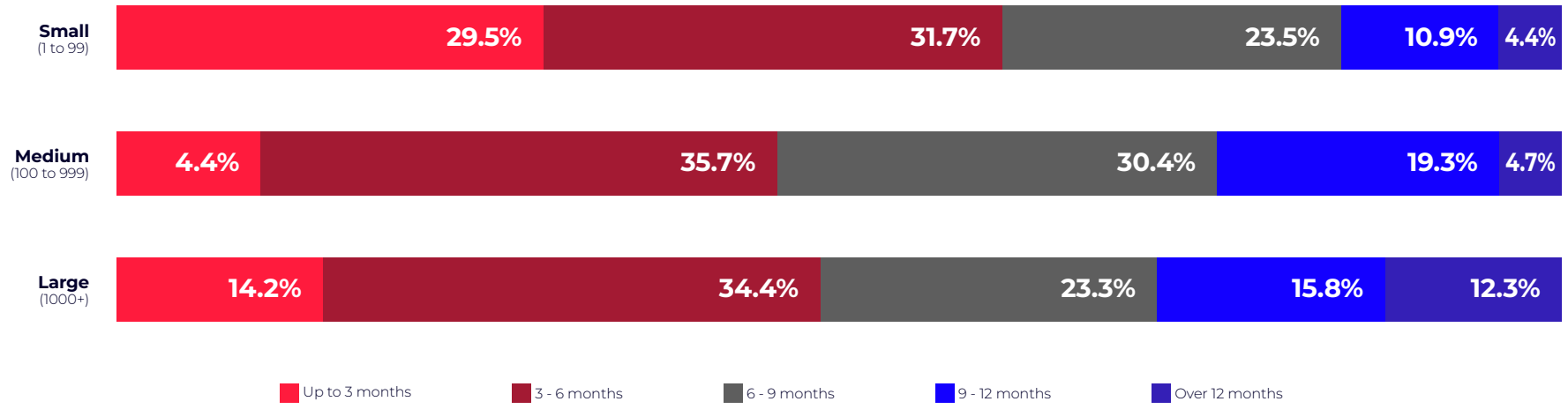
Many surveys like ours focus a lot on sales and marketing outcomes. However, they're just a part of the story and exist primarily at the start of a new client relationship. What comes after marketing and sales have done their jobs gets turned over to client success or your professional services arm. Like all service organizations, they're at the mercy of the client, so having an understanding for how long clients take between a sale being given the green light and go-live is important.

Like many statistics in our report, we recognize that project scope plays a considerable role in this data point. However, in general, only one-half—50.4%, to be exact—of clients indicate that their go-live happens within six months of contract signature. Another 42% take between 6 and 12 months, with a minority—about 7%—taking longer than 12 months to push the go button.

Putting this into action Expectation setting is the key to a strong relationship. For client success and professional services organizations, alignment on deployment timelines is a critical expectation to get right from the beginning. Ensure that these groups in your company have early conversations with clients and understand that the over/under on being done in 6 months is typically a flip of a coin.



Time Between Contract Approval and Go-Live By Company Size



Putting this into action: As with the primary finding in this section, set expectations and prepare your deployment teams for longer project cycles in medium and large organizations. This is another data point indicating the importance of Solution Vendors knowing their ICP, and ensuring their acquisition support and deployment cycles meet client needs rather than frustrate them.

KEY FINDING: LARGER ORGANIZATIONS ARE SUBSTANTIALLY SLOWER THAN SMALLER ONES

There are two ways our team thinks about company size in terms of solution deployment. The first is that larger companies take longer to deploy solutions because projects are often larger, involve more people, and, therefore, there's more organizational inertia to overcome. The second is that larger organizations have more people and, therefore, can deploy at the same speed as their smaller counterparts.

Our first thought appears to be reality as we consider this statistic by company size. Almost triple the number of respondents—12.3%—indicate that deployments don't go live until past the 12-month mark.

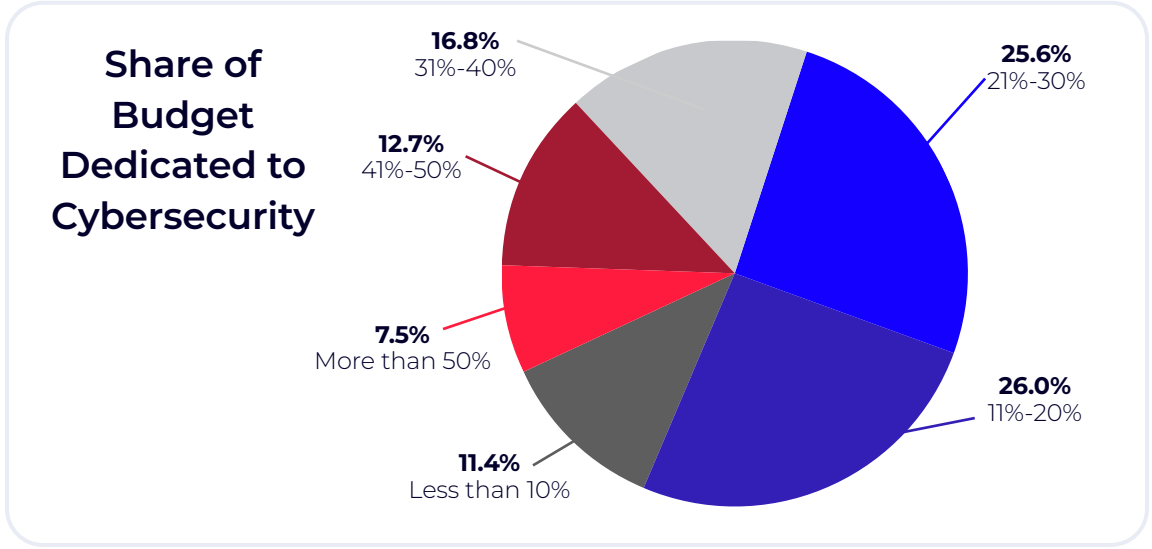
Even medium-sized organizations are a bit less nimble than their smaller counterparts. In small companies, 61.2% of deployments are complete in 6 months or less, but this drops to 45.6% for medium-sized companies. Smaller organizations definitely skew the average a bit in this statistic.

Security Share of Budget Can Be Significant

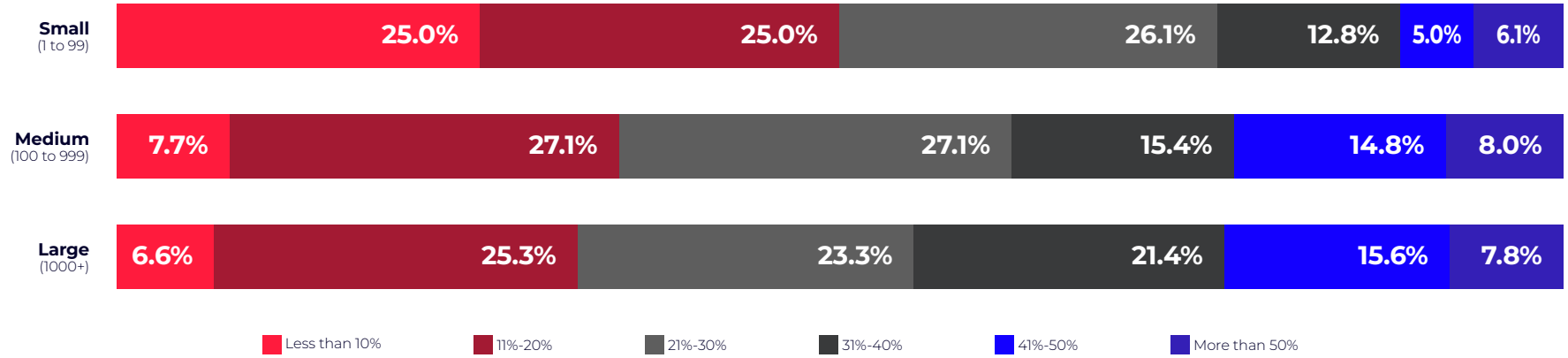
KEY FINDING: SMALLER COMPANIES SPEND A MUCH SMALLER PROPORTIONAL SHARE OF BUDGET ON CYBERSECURITY SOLUTIONS

As the adage, paraphrased, says, where you spend money is an indicator of what's important to you. Of course, there are always competing demands for budget dollars, and expenditures for cybersecurity solutions are no exception. For our respondents, about 11% are spending less than 10% of their IT budgets on cybersecurity tools and services. On the other end of the spectrum, 7.5% spend most of their IT budgets on these items.

Everyone else is in the squishy middle with just about 50% spending between 11% and 30% of their IT budgets on such services.



Share of Budget Dedicated to Cybersecurity



This isn't necessarily *that* interesting, but does show that there is a strong budgetary appetite for security enhancement, which bodes well for companies that sell cybersecurity. Where things get interesting is when we dig slightly deeper and analyze this result by company size.

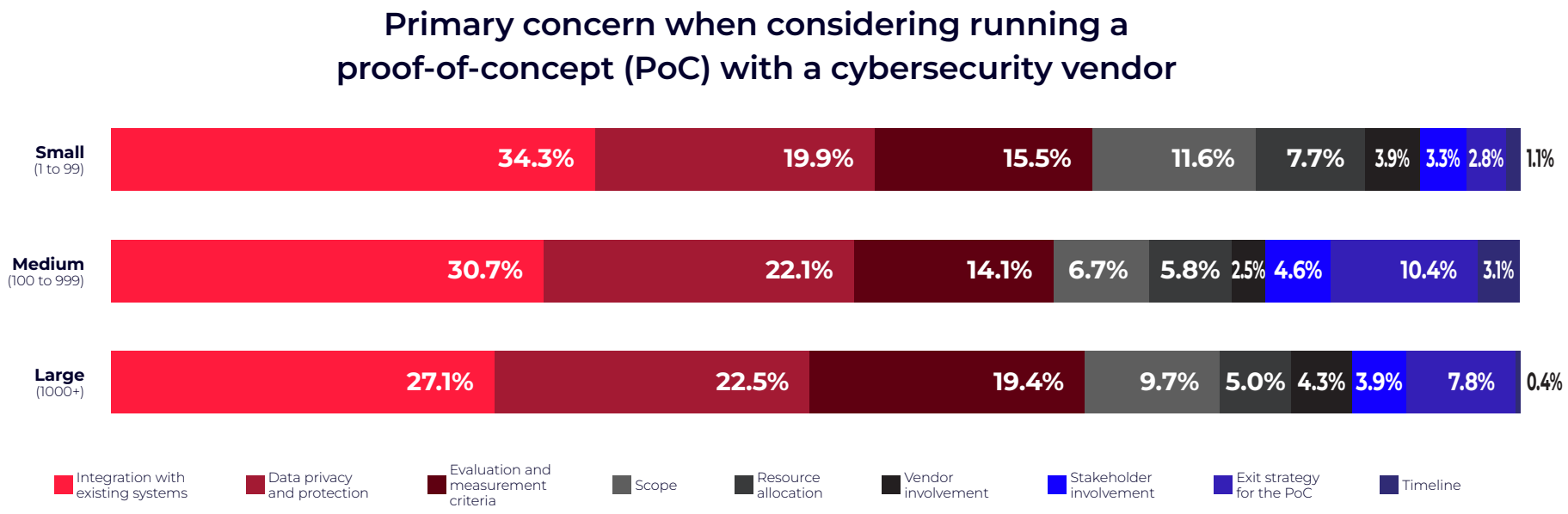
Here, you can see that, again, company size skews this data point. Smaller companies are dedicating a smaller share of their IT budgets than their larger brethren. A full 25% of small companies dedicate less than 10% of their budgets to cybersecurity. 50% of small companies spend less than 20%.

Why is this? Remember that smaller companies also have smaller budgets, so the total pie is not as large as it would be in a larger organization, so a single tool acquisition may have an outsize impact on the budget. Some security tools are also less expensive at the lower end of the market, so customers may not have to dedicate as much budget. Regardless of the reason, this is an important statistic.

Putting this into action: This is the kind of data point that makes data-centric people developing ideal customer profiles lop off the bottom of the market because it's more difficult to unlock customer spend. We're not suggesting you pull out a hatchet, but do stay mindful of the fact that the small business space can be markedly different than that enjoyed by medium and large companies.

We recommend ensuring that your marketing hits companies of 100 employees and up, but not completely at the expense of smaller companies. After all, if you can manage to scoop one of those companies into your sales net, their money spends the same as everyone else's. Further, small companies have a way of evolving into medium and large companies, so completely ignoring them is not necessarily a sound strategy, but it's understandable if they're not a foundational part of your go-to-market strategy.

Reducing Operational and Reputational Risk Reigns Supreme in Proofs of Concept



KEY FINDING: THERE ARE PRODUCT, MARKETING, AND SALES IMPLICATIONS IN EVERY POC YOU UNDERTAKE

Regardless of company size, the top three concerns that respondents cited as their top potential issues in a proof of concept were the ability for a solution to integrate with the rest of their stack, maintaining strong data privacy controls, and what metrics they would use to measure the overall effectiveness of a solution. While the next six concerns weren't necessarily outliers, in aggregate, they all amounted to only about 25% of respondents' top concerns.

Putting this into action: A proof of concept (PoC) is one of the most important parts of your sales process and, done correctly, will have implications for most parts of your company, from product management to marketing to sales. These are powerful educational opportunities during which you can learn what worked well and what didn't so that you can evolve your product, processes, and promotions.

All company sizes cited the ability to integrate with existing systems as their top primary concern, often by a wide margin. What does this mean? Simply put, they want to know that a new tool isn't going to create a new silo that they have to support or a whole new set of monitoring metrics that they need to figure out. They want certainty that the tool you provide them becomes a part of their existing ecosystem and isn't an island unto itself. It's up to you to ensure that your product can support that desire and that your sales and marketing teams can effectively message it.

This also means having your data integrations front and center in your messaging, don't bury it on your website under some obscure heading or page. Put integrations at the top of your product pages in clear and easy to understand terminology. Add a button entitled "Not seeing your current product? Let us know." This may be the type of messaging that prevents potential customers from bouncing too soon.

Data privacy and protection was cited next. During a PoC, you're squarely in the "do no harm" phase of the evaluation process. If your product somehow mucks about in a way that exposes the potential customer to enhanced risk, you're probably in for an early exit for the PoC. So, make sure you've battened down the hatches to eliminate the potential for becoming the cause of an exposure for a prospective customer.

ABOUT FUTURE B2B

Future B2B is a global platform that connects sellers with B2B buyers across 15+ industries through specialist-led content, events and advertising. Our brands – which include SmartBrief, ActualTech Media, ITPro, TV Technology, AV Technology, and Tech & Learning, – inform and inspire nearly 10 million leaders daily. Future B2B delivers relevant news, webinars, and content to a highly engaged global audience.

ABOUT ACTUALTECH MEDIA

ActualTech Media, a Future B2B company, is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services. ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience. Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.