BABEL

FROM LONG CYCLES TO QUICK CALLS

Mastering the Cybersecurity Buying Journey

// 2025

1) INTRODUCTION

It's 2025, and the prognosis for cybersecurity spending is...well, the same as most years: rising. IDC data shows that global cybersecurity spend is set to grow 12.2% year-on-year in 2025 and it's easy to see why. The state of the world's security is looking more and more precarious with threats of all kinds on the rise and stepping up both in their frequency and their sophistication. AI-generated, ransomware, phishing and social engineering, you name it and it's probably gotten worse.

But if there's one thing that's also on the rise, it's the complexity of cybersecurity. Cybersecurity is one of the most complex sectors in tech. The buying cycle increasingly involves a broader set of stakeholders – not just cybersecurity professionals but engineers in IT, compliance, business leadership, and more. People are waking up to the fact that cybersecurity is a business risk, not just an IT issue.

There are also more tools than IT teams know what to do with – a tool for seemingly every threat. According to Palo Alto Networks Inc., the average enterprise uses 130 discrete cybersecurity products to protect its infrastructure, applications, and data. That's a lot of tools. How do you stand out if you're pitching enterprise cybersecurity product #131? Getting a foot in the door today is harder than it used to be, which is why differentiating your brand as a cybersecurity vendor has never been more critical. Unlike broader tech buying cycles, cybersecurity is trending towards shorter buying cycles. According to Digitalzone, 53% of cybersecurity buyers select a vendor in just 1-3 months; 30% make their decision in 3-6 months. That means most buyers are making a decision in less than half a year.

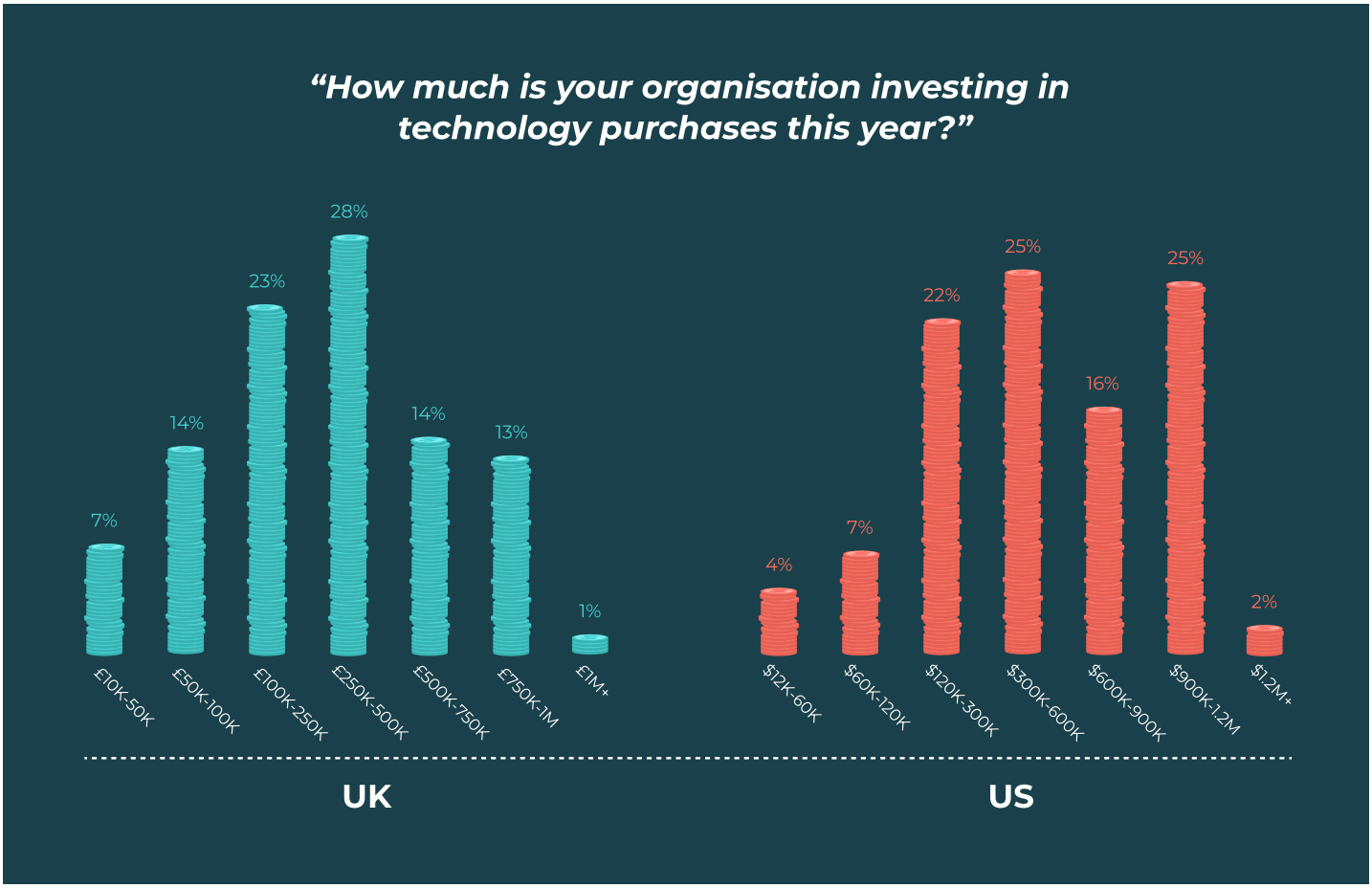
In other words, cybersecurity brands face a unique balancing act: judiciously allocating limited resources to grow trust among inactive potential buyers, while also addressing those who might make swift, panic-driven decisions within hours. No matter how long or short the decision-making process gets, though, you still have to be first in the queue in the minds of buyers. To do that, you have to play the long game, building trust over time with potential buyers. A good PR & Marketing strategy in cybersecurity recognises that you have to make your cybersecurity brand memorable in a way that drives intent to purchase. Our B2B Cybersecurity Barometer breaks down the various areas of consideration for vendors trying to catch the attention of cybersecurity decision-makers in 2025.

SHOW ME THE MONEY

Tech spend in 2025 is healthy – really healthy, actually. Even during economic uncertainty, our data shows 27% of UK companies have invested over £500,000 this year, while 41% of US organisations have spent over $600,000.

The urgency of addressing cybersecurity threats is, no doubt, factoring into this liberal spending, with the global cost of cybercrime set to reach an eye-watering $10.5 trillion annually by 2025. Incidents like those affecting major UK retailers show that attacks aren't just becoming more high-profile, but also disrupting services, even when not a single shred of data is leaked.

So, the appetite for spending is there. But cybersecurity costs are becoming more expensive, replete with upselling, hidden fees, and long-term commitments. Some solutions can range anywhere from a few thousand dollars for small businesses to millions for large enterprises. Many buyers will likely become more sensitive to this over time, and that will make it even more important to establish yourself as a trustworthy and memorable brand. First, however, you need to start by answering: who are the decision-makers looking to spend on security solutions?



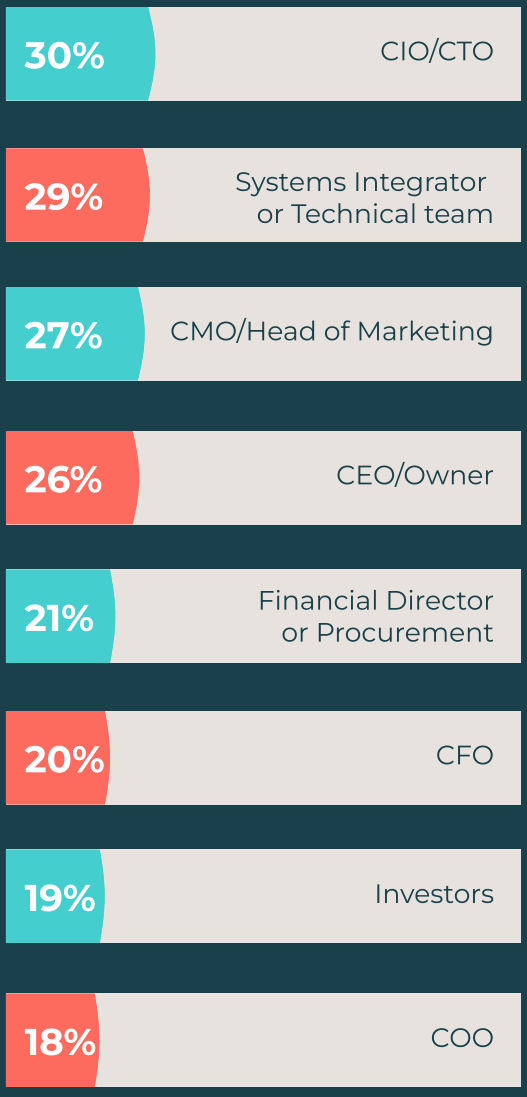
WHO'S BUYING SECURITY TOOLS?

You can't build trust in cybersecurity without understanding who your audience is. If, for example, you're promoting a malware detection tool, you have to know who you're talking to.

As every marketer would say, "know your buyer." That point is perhaps even more important here because cybersecurity tends to have even more stakeholders. It's rarely (if ever) one person's decision. Cyber deals often require input from multiple technical decision makers with specialised knowledge, engineering teams with veto powers, security architects, the CISO, and even risk/compliance stakeholders.

In other words, a lot of stakeholders stand in the way of an enterprise clicking the 'buy' button. The final say might not even come from the same role, from one organisation to another, according to our data. When we looked at tech more broadly, the four most common people to have the final say included, unsurprisingly, the CEO or Owner (26%), the CIO/CTO (29%), the Technical team (28%), and the Financial Director (26%).

"When it comes to major technology investment decisions, which stakeholders in your business have the most influence on the choice of provider, if any?" (Pick up to 3)



*According to 202 UK and 201 US technology buyers within organisations employing at least 1,000 people.

TRUST IS A REQUIREMENT IN CYBERSECURITY, NOT A DIFFERENTIATOR

Above all, you have to understand that cybersecurity requires more trust to drive conversions than your average B2B SaaS product. In fact, trust isn't even a differentiator in cybersecurity; it's a requirement. When buyers look for a cybersecurity solution, they're not just looking for a tool. They're looking for a partner to safeguard their valuable data, company reputation and so much more.

At the same time, you have to be memorable. If you're jumping into a PR or marketing campaign with the mindset of, "here are the problems our cybersecurity tool solves," you're going to struggle. If there are already 130 tools in an organisation on average, then what makes you different?

Remember, too, that buying cycles in cybersecurity are getting shorter. If an enterprise gets hacked and hits the panic button on quickly buying a solution, who are they going to pick? This is where the Rule of Three in Every Purchase Decision comes in. Research [1] by BBN shows that when someone moves into buying mode, the first search engine they use is their head. When they do this, typically only three brands will immediately come to mind, one of which they will buy from in 90% of cases.

That's why you have to invest the time into making your brand synonymous with reliability, innovation, and regulatory alignment. That's especially important for the inactive buyers who may be willing to pull the trigger on a purchase years down the line.

As a cybersecurity vendor, you should be focusing on killer brand-building communications and marketing campaigns that build mental availability. To maximise mental availability, you need to maximise your share of voice and awareness so that you're remembered among buyers when they come to market.

You also need to educate buyers on why your solution should be selected, influencing and shaping the buying criteria. There are many ways to do this, from strategic thought leadership and content marketing campaigns to case studies, certifications, testimonials, and ongoing engagement campaigns. All of these can help support conversion, showcasing the success others have had in choosing you as a vendor to solve their problem.

3) SPHERES OF INTEREST

Which of the following channels most influence what brands you consider when shortlisting solutions/services for purchase?
(Select up to 3)

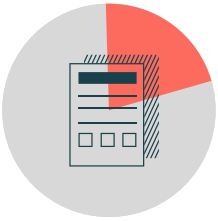
Company website

26%

Analyst reports

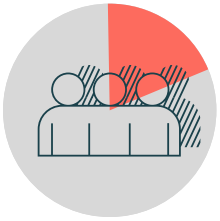
23%

Industry reports



21%

Industry events



19%

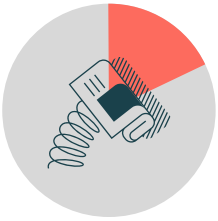
Word of mouth

19%

Search engines

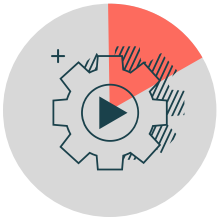
19%

Media coverage



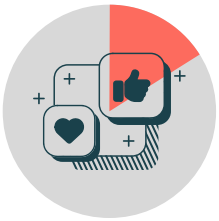
18%

Advertising



17%

The brand's social Media



16%

Company blog and resources

15%

Industry awards

14%

Podcasts

14%

WHICH CHANNELS MOST INFLUENCE PURCHASE DECISIONS?

So we know you have to build trust and be memorable to be first in line in the minds of cybersecurity buyers. But where do you do that exactly? Where exactly should you focus your efforts?

44%

of tech buyers trust analyst or industry reports when choosing a new solutions

Considering how complex and urgent cybersecurity has become, buyers in the space are under a lot of pressure to make fast, informed decisions. And under that pressure, it turns out that one of the first places buyers turn to is the company website. According to 25% of buyers, the company website remains a primary resource. For cybersecurity buyers, a vendor's website is not just a digital storefront but a critical source of technical validation and proof of expertise. It's the home of the brand, so it makes sense that it would be so influential.

There's a lot of emphasis, too, on earned channels, with analyst reports (23%), wider industry reports (20%), and word-of-mouth recommendations (17%) all rating highly for their influence on purchases. This tracks, considering how risk-adverse many cybersecurity buyers are. They want to protect their sensitive assets, and third-party validation makes all the difference when deciding which tool will help do that.

That doesn't mean that being seen on these channels is easy – far from it. It requires careful relationship-building with the right analysts, journalists, and industry thought leaders.

"Trust isn't a differentiator in cybersecurity; it's a requirement. Don't focus on being another tool in an enterprise's tech stack. Be the long-term partner who they rely on to safeguard their data and reputation."

ED COOPER
DIRECTOR

3) SPHERES OF INTEREST

WHAT ARE DECISION MAKERS LOOKING FOR?

With up to $600k at stake, success for any cybersecurity brand hinges on navigating the delicate balance between addressing short-term and long-term buyers. But in a sea of cybersecurity vendors, what makes one stand out from the others?

CREDIBILITY

Brand credibility and trust are key. When we asked technology buyers about their spheres of influence, 44% said that third-party reports (23% said analyst reports and 21% said wider industry reports) had the most influence over their purchasing decisions. Similarly, when we asked what sources they value most when assessing unknown vendors, neutral, third-party sources again came out on top. The advice of contacts, analyst reports, and third-party commentary were all equally valued by 42% of technology buyers, with owned marketing sitting fractionally behind at 41%.

These results are no surprise. For IT teams at companies across virtually every industry, there's a ticking clock for closing security gaps. Larger enterprises are especially driven by regulatory compliance requirements and enhancing their incident response capabilities. They need to hear from independent, trustworthy sources that the vendor they're looking into is credible.

By linking their brand to relevant buying situations through inclusion in analyst reports, media coverage on industry hot topics, and customer success stories, vendors can build their reputation in their category. So when it comes to purchasing decision time, security vendors that have built their credibility up through sources like these will be the first to come to mind.

"When approached by an unknown technology vendor with a potentially relevant solution, how would you assess their offering?"

43%
would reach out to their network for advice on the company

42%
would try to find analyst reports on the company

42%
would research any third party commentary on the company

41%
would read their website and the owned marketing resource they have available

CONSISTENCY

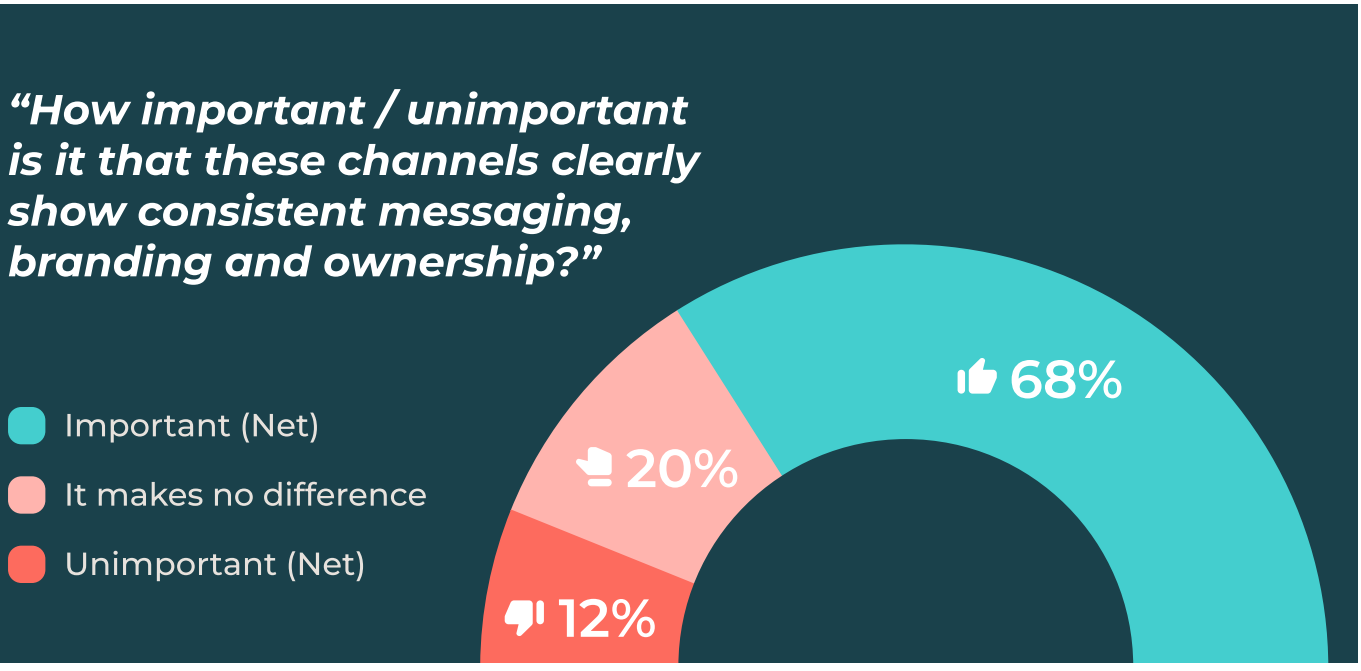
Getting into these neutral, trustworthy sources is no mean feat, but the harder challenge is keeping brand consistency across both owned and earned channels. Over two-thirds (67%) of technology buyers say that consistent messaging across channels is an important factor for them.

Security vendors often comprise many different roles that approach cybersecurity concepts in vastly different ways. Some are more focused on the big picture, others are more technical. Some don't mind wading into geopolitical conversations, others wouldn't touch it with a ten-mile pole.

All of which is to say that consistency is key. If someone is considering your cybersecurity tool or platform, but finds your website has messaging that completely contradicts your messaging in a third-party report, that will sow doubt in the buying process. Doubt leads to indecision, or the outright loss of a potential sale.

It might sound dramatic, but with every buying decision, your brand is rarely considered in a vacuum. If you're showing mixed messages and creating doubt while a competitor is consistently and clearly showing up, you will lose out more often than not.

"How important / unimportant is it that these channels clearly show consistent messaging, branding and ownership?"



"There are over 3,000 companies in the cybersecurity sector – it's crowded and evolves rapidly to keep pace with the constantly changing threat landscape and diversifying tactics of threat actors. We've observed some industry players promoting the message of platformisation – becoming a one-stop shop for cybersecurity solutions and services – which makes sense in the current climate.

In a time of budgetary constraints, simplifying complexity is logical. However, it's not as straightforward as merely reducing suppliers, and we often hear that companies have onboarded even more cybersecurity suppliers over the past year.

The sector is among the least static and fastest growing, and so are the opportunities for marketers and communications professionals in the space to influence potential buyers."

RIK TURNER
CHIEF ANALYST, OMDIA

WHICH CHANNELS MOST INFLUENCE PURCHASE DECISIONS?

You need clear and consistent messaging to cut through the congested cybersecurity space. While there are many different channels, trusted sources are the best way, and that includes media coverage.

Where do cybersecurity buyers get their news from? It's usually the same places they consume advice on how to overcome industry-specific problems, whether it be tool sprawl, security team burnout, or threat sources.

It's tempting to assume these buyers default to national outlets, but in reality, the answers they seek are usually found in the tech, vertical and cybersecurity trade media – from IT Pro, TechRadar Pro, and The Register to Computer Weekly, Bleeping Computer, Infosecurity Magazine, and DarkReading. Nearly half (44%) of the IT decision-makers we interviewed said they get their news from the trades, while only 15% regularly consume national media.

It's also worth observing that nationals and trades cover cybersecurity news in very different ways. National news publications approach cybersecurity as a public interest topic, more concerned with how cybersecurity fits into the broader picture of business, politics, and society. Their audience is the general public, policymakers, and non-specialist readers. Coverage often ties cyber incidents to larger societal impacts, be it national security, privacy, economic consequences, etc. Any technical issues are explained in extremely accessible language.

Trade outlets can afford to dig much deeper into technical details, industry trends, threat intelligence, and regulatory developments – you're unlikely to see a national newspaper using the term 'Zero Trust Network Access' very often, for example. Trades are also far more likely to leverage vendor insights, whereas a national outlet will draw from a much bigger pool of public figures, industry analysts and consumers.

MEDIA THAT MATTERS

Here are some other example topics to illustrate the difference between national and trade media:

National media topics:

- The impact of a ransomware attack on critical infrastructure (e.g train network or energy grid)
- Policy debates around data privacy or government surveillance
- How a major breach affects consumer trust or national security

Trade media topics:

- Technical breakdown of a new malware strain or exploit
- Quarterly spikes in ransomware detection or AI-driven threats
- Analysis of regulatory updates (e.g. SEC enforcement, EU AI Act)
- Best practices for incident response or vulnerability management

Both national and trade news outlets can be great vehicles for increasing brand awareness, but they serve very different functions. You have to understand what you're trying to achieve by obtaining coverage in each one. Is your goal to get your brand name out to the masses and investors? Nationals are well suited to that. Is your goal, on the other hand, to speak directly to C-Suite executives, IT and cybersecurity practitioners? Then trades are your best bet.

WHAT CONTENT DO CYBERSECURITY BUYERS ENGAGE WITH?

It's not all about volume. If no one reads your coverage, it's all for naught.

Quality, educational, and engaging content will not only increase your chances at the decision-making stage but also boost meaningful brand awareness by showing you understand your prospect, their industry, and their problems.

Many cybersecurity vendors sell solutions that can, in theory, be used in various sectors. But the security pain points faced in finance are rarely identical to the ones faced in healthcare, government, or retail. There may be a lot of overlap, but generic content won't cut it. Readers in those industries want to hear details that apply to them specifically. They want to see how much you know about their industry.

Add to that all the idiosyncrasies that exist in cybersecurity today – the complexity of integrations, regulatory pressures (e.g. Cyber Resilience Act, DORA, NIS2), the high stakes of protecting critical infrastructure. There are lots of challenges for organizations to navigate, and they want to know how.

It's not surprising then that 58% of buyers say their interest is most piqued by thought leadership articles. These slightly longer-form pieces let you weave brand messaging in with topical commentary around security challenges in niche spaces. That not only strengthens your credibility but brand familiarity as well.

Research-focused news continues to make a dent, too: 30% say that it interests them the most. It's worth noting, though, that security vendors push out a lot of surveys. If you're investing in your own research, it has to bring buyers some value. Look for gaps in industry data and you'll have much more luck making an impression that will bring buyers back when considering the final purchase.

1 in 4

B2B technology buyers working at organisations of more than 1,000 employees regularly consume their news from tech and vertical publications.

5) RULES OF ENGAGEMENT

"Thinking about the type(s) of business and B2B technology media you consume, what type of content are you are most likely to read?" *(Select up to 3)*

#1	**Long thought leadership article**	(more than 800 words drafted by a tech vendor)	**32%**
#2	**Research-based News**	(Media story based on unique data)	**30%**
#3	**Executive profile**	(i.e. feature of a CEO, CFO, CTO, talking about their career, aspirations etc)	**29%**
#4	**Commentary**	From a vendor, in a trade journalist authored article	**29%**
#5	**Whitepaper**	(in-depth content of 2,000 words or more)	**28%**

HIJACKING THE NEWS AMID CONSTANT BREACHES

News hijacking is the bread and butter of many B2B tech PR campaigns. That's true for both broader enterprise tech and cybersecurity. The difference is that the latter, especially in 2025, is absolutely crawling with news hijacking opportunities. The amount of breaches happening every week has made sure of that.

The early phase of a comms campaign is crucial in defining what you are and are not comfortable with saying. You need to identify a roster of spokespeople who can reliably comment on a range of themes and topics: AI, ransomware, nation-state actors, social engineering, workforce-related issues (like burnout and training).

Partnering with a PR agency can help narrow down the exact messaging you're comfortable sharing with the media. At Babel, for example, we always kick off our PR and marketing campaigns with a position paper, informed by messaging calls with spokespeople, which defines the cybersecurity vendor's unique positions across industry topics.

Each security incident tells a different tale, but the themes are often the same. Security challenges that hounded enterprises last year may yet do so next year. This is where a position paper can prove immensely valuable – a playbook on your company's viewpoints mapped across a slate of issues.

Not everything has to be reactive, either. You might be surprised by how much you can predict in the cybersecurity news cycle. From upcoming regulations and major sports events to elections and anniversaries, it's well worth keeping a calendar of the things that will spark conversation.

Timeliness is king, and it's a lot easier to be timely (and at the top of a journalist's inbox) when you already have messaging you can adapt. With that said, it's not always about being the fastest...as we will shortly get to.

WHEN BEING THE FIRST IS THE WORST

In theory, you can react to any security incident with a rapid-fire comment. But Jeff Goldblum said it best in Jurassic Park: just because you can doesn't mean you should – at least not right away.

In a nutshell, the success of any news hijacking in cybersecurity hinges on three pillars, in the following order of importance:

- Having something relevant and interesting to say
- Saying it in a timely fashion
- Building great relationships with the media

The last point needs caveating. A good relationship with a journalist is not a pre-requisite to securing coverage. You could be the godchild of a security reporter at the Financial Times, but if you've got a bad take, it won't get past the editor's desk. You do, however, need to know that the journalist you're dealing with trusts your information.

Building trust is about consistently giving the media reliable and quality commentary. It's not about being the fastest; it's about what value you're adding to a conversation. In fact, sometimes being first can actually be extremely detrimental, especially if you don't have all the facts.

Remember, every security incident is different. Some incidents have a very short tailpipe, while others have a long one (e.g. Crowdstrike), inviting experts to contribute analysis in the weeks or months to come. A great PR campaign hinges on knowing when it's more tactical to wait for the follow-up analysis article. Sometimes, it really is better to say, "I don't have a comment right now, but when I do, you will be the first to know."

WHAT DO YOU SOUND LIKE WHEN TALKING ABOUT SECURITY NEWS?

Figuring out how your experts will engage with the media is just as important as what they say. The cybersecurity news cycle runs at a vicious pace. React to one breach with a hot take, and you might suddenly find a journalist asking your spokesperson to hop on a Zoom call in the next hour.

Can your spokesperson accommodate that? Can someone else? What's the next-best thing you can offer (e.g. written comments)? Being able to anticipate these questions is critical. That's why you need to establish the rules of engagement at the start of your campaign, not just the messaging itself. It will avoid the risk of overpromising and underdelivering to the media.

Tone of voice is another key factor. What does your brand sound like? Is it matter-of-fact? Tongue-in-cheek? There's a line you have to tow. You want 'punchy' language that draws eyeballs to what you're saying, but you don't want to victim-shame. Ultimately, cybersecurity incidents affect real people, so don't paint your brand as heartless – after all, it could be you one day. Think about being constructive and sympathetic. Use your position paper to establish the boundaries. Assume that every victim is a potential future customer prospect. At Babel, we also regularly provide media training to the spokespeople we work with to ensure they have all the tips and tricks they need at their disposal to carry out successful media interviews.

Remember, too, that even if you do have written commentary ready to go, but you miss the boat on news coverage, there's a lot you can do with it. A few ideas include:

- Save it for follow-up articles with the press
- Turn it into an opinion article – either for the press or your website
- Pitch it as a Letter to the Editor or podcast discussion topic
- Repurpose it for social media

CONCLUSION

The cybersecurity industry in recent times has been defined by relentless growth in complexity, marked by a cat-and-mouse game of ever-expanding threats and toolsets. It might be cliché to say, but the stakes for both vendors and buyers have never been higher. With spending on the rise and decision cycles accelerating, standing out in a crowded marketplace is no longer a matter of simply having a superior product. It's about building trust, credibility, and lasting mental availability among a diverse set of stakeholders.

Enterprises are being bombarded with choices and pressured to make decisions fast. But no matter how short buying cycles get in response to panic-inducing data breaches, you're always going to be playing the long game. There is no shortcut to becoming one of the first three brands a buyer thinks of when they hit the market.

You want to be one of those brands, and the brand-building you need to make that happen has to go beyond spouting technical features. Focus instead on nurturing genuine, long-term relationships with buyers.

Knowing your audience, delivering consistent and credible messaging across trusted channels, and tailoring your content to the specific needs of each sector, are now essential strategies for breaking through the noise. The brands that win will be those that are remembered first, trusted most, and able to demonstrate real value at every touchpoint.

So play the long game. Invest in building a brand that is synonymous with reliability, innovation, and partnership. Don't just be another tool in the stack. Be the solution that decision makers recall when it matters most.