Resonance

CONTROLLING THE CONTROLLABLE

How marketers can effectively engage cybersecurity decision-makers in 2024

A comprehensive guide to creating an effective cybersecurity communications programme that attracts the attention of prospects in 2024.

Insights from 200 cybersecurity decision-makers.



Introduction



The cybersecurity vendor landscape is competitive and moves at a hurtling speed. Selling cybersecurity products or services demands a nuanced marketing and communications approach. Punching above the noise, being seen and heard can feel like throwing jelly at the wall. And that is before you've even reached any level of engagement. It's a challenge, but once you've picked through the things that don't work and hit the right formula, it unlocks huge potential.

Cybersecurity services and products battle against a never-ending list of threats, from nation-state groups to people-related cyber risks. There are a lot of vendors vying for the attention of your target audience. The market is fiercely competitive. As a marketing, PR or analyst relations professional, you need to know what will work and take bold strategies to execute.

Here at Resonance, we have oodles of experience driving cybersecurity communications programmes. When creating these for our clients, we have one focus in mind - your prospect. Our number one recommendation is, whatever you do, know your audience.

Our latest research provides a guided journey through the hearts and minds of your prospects.

READ ON TO LEARN:

- How prospects consume cybersecurity knowledge today
- Where prospects look for vendors in 2024
- The nuances surrounding prospects' internal decision-making
- The trends and challenges topping the charts

If you are a CMO, communications manager, or analyst relations professional, the below insights will be right up your street.

So sit back, grab a cup of something and read on.

Cybersecurity Marketing and PR IS different

Here's what we know

Cybersecurity buyers prioritise trust, technical detail, and regulatory compliance more than other tech buyers due to the high stakes of security failures. They prefer vendors with strong track records and certifications, need detailed product information, and have longer decision-making processes involving multiple stakeholders. The evolving threat landscape and regulatory requirements demand adaptable solutions. Community insights also heavily influence their choices. Vendors should focus on demonstrating reliability, compliance, and technical prowess while engaging with the cybersecurity community.

- **Trust and Track Record:** They seek vendors with strong reputations, validated by certifications and awards, due to the high cost of security failures.
- **Technical Detail and Compliance:** Buyers demand in-depth product information and compliance features to navigate the complex cybersecurity landscape and meet regulatory standards.
- **Long Decision Processes:** The evaluation of cybersecurity solutions involves multiple stakeholders, leading to longer sales cycles.
- **Adaptability to Threats:** With an ever-evolving array of threats, buyers prioritise solutions that can adapt quickly and offer timely updates.
- **Community Influence:** Decisions are heavily influenced by the tight-knit cybersecurity community, relying on peer recommendations over vendor marketing.

For vendors, success means demonstrating not just the effectiveness of their solutions, but their reliability, compliance capabilities, and the ability to foster community trust.

Resonance

THE CYBERSECURITY MARKET IN A FLASH

Over the past few years, the cybersecurity market has witnessed significant consolidation thanks to established players acquiring niche vendors. However, there are also emerging new vendor categories, expanding the remit of cybersecurity products and services.

The industry requires a blend of holistic and innovative solutions. Without this blend, there's no chance it'd be able to keep pace with the threats out there.

THE AI-LEPHANT

Let's not forget the "AI-lephant" in the room. The integration of artificial intelligence (AI) and machine learning (ML) into security solutions represents a significant advancement, enabling proactive threat detection, improved incident response, and a strengthened overall security posture.

But, this works both ways. Threat actors have been handed superpowers - able to create malicious code, phishing campaigns, and many other attack vectors in a matter of minutes. While still quite early, the cyber market will continue to shift as a result and marketers need to be able to capitalise on this - more on this later.

The rise of managed security services (MSS) highlights a growing preference for outsourcing security infrastructure operations. This allows businesses to focus on their core activities while ensuring effective cyber protection. Finally, evolving data privacy regulations like GDPR and CCPA are creating a new imperative for vendors. They must demonstrate compliance and prioritise data security within their solutions.

Cookie cutter won't cut it

In this fast-moving market, out-of-the-box comms strategies just won't cut it. While we can't predict outcomes, as communications professionals we need to control what we can and ensure we focus on creating a programme that helps your organisation stand out from the "cyber crowd".

Establishing thought leadership through insightful content, creating your own news through research, and engaging with industry influencers and analysts, has become crucial for standing out in this competitive environment. Understanding these trends and challenges is paramount for cybersecurity vendors to develop effective strategies and maintain a competitive edge in 2024.

Our research, which interviewed cybersecurity decision-makers found that 40% of cybersecurity budgets will mostly stay the same this year. However, if budgets do shift - they'll most likely be in an upward direction. This is great news for marketers as the door is open for us to place ourselves in the eyesight of decision-makers with a bit of cash.

But before we do that, we need to understand where those eyes are looking.



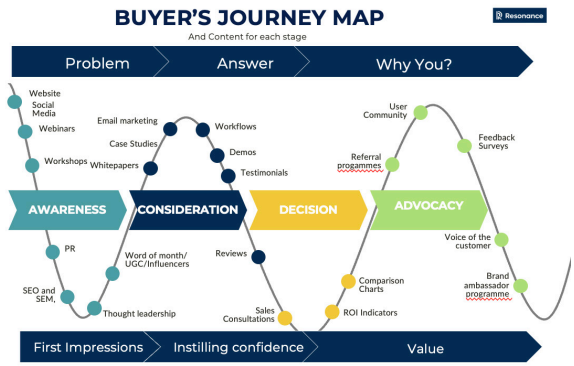
Decoding Your Prospects Info-Diet

Navigating Cybersecurity Information Consumption Trends

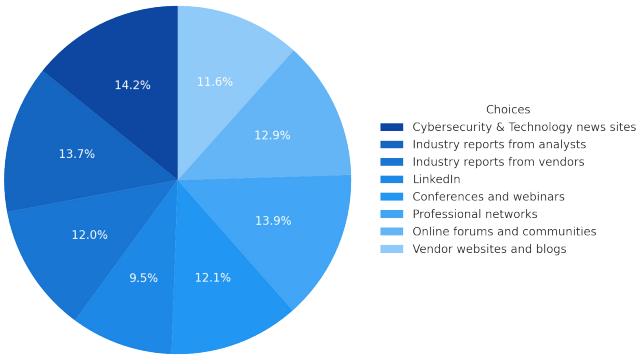
It's all about knowing what information you need to be pushing to your prospects and when. We've categorised the journey into three stages:

1. Information on cybersecurity issues and trends
2. Information on products for exploring your options
3. Information to shortlist solutions in the final decision-making stage

Are you ready? Let's go.



Cybersecurity Trends: How IT decision-makers typically get information about cybersecurity trends



Our research of 200 cybersecurity professionals, ranging from CIOs to CDOs to IT managers shows that cybersecurity and technology news sites are the most popular source for decision-makers to keep up with trends. And let's face it, there's a lot to keep on top of.

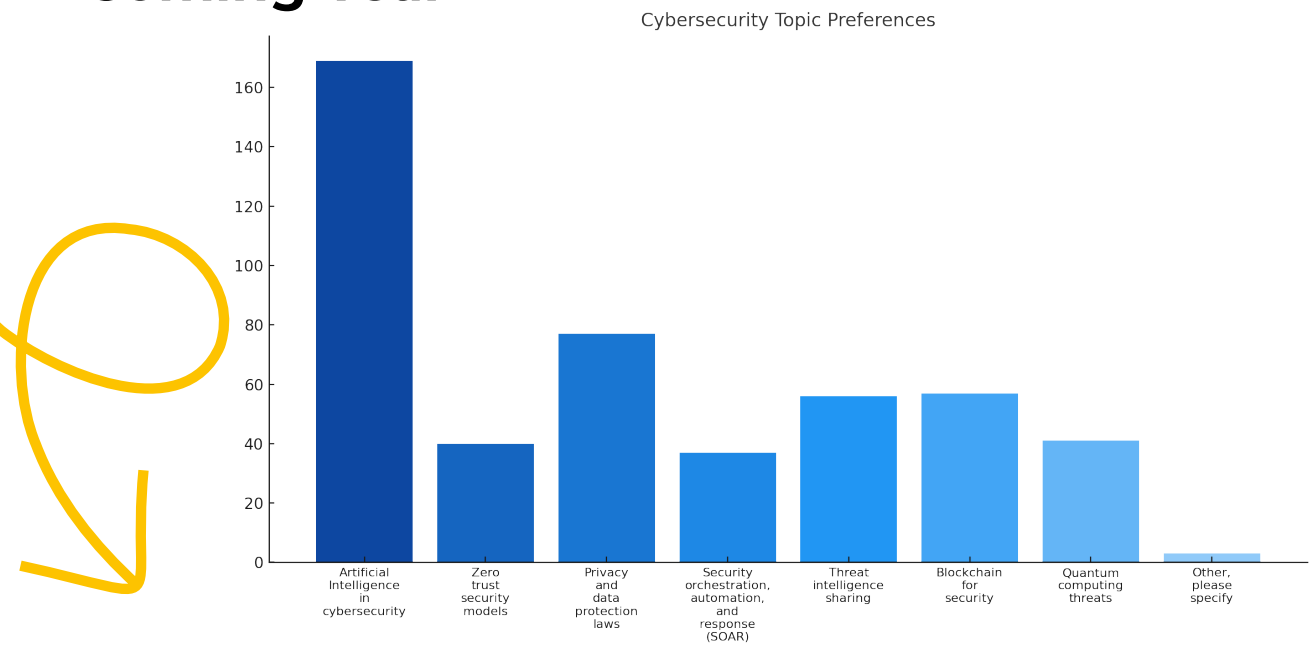
Dedicated news platforms focusing purely on cybersecurity and emerging tech are seen as the most valuable and credible source of insight.

Professional networks and industry analyst reports also scored highly. Leveraging peer perspectives and market analysis likely provides useful context and different lenses through which to interpret cybersecurity developments. The high position of these sources clearly shows IT leaders appreciate external validation and expertise in their day-to-day.

LinkedIn Lags: Why Cybersecurity Pros Crave Credibility Over Quantity

Compared to specialist publications, LinkedIn ranks lower among IT professionals for cybersecurity insights due to its vast but less targeted content. This preference stems from the need for credible, niche information where trust and authority are crucial.

What's Hot and What's Not: Trends for the Coming Year



AI: Riding the wave without wiping out

Unsurprisingly AI tops the charts as the current trending topic for the industry, followed by Zero Trust security models. On top of this, it is also the topic decision-makers are most interested in learning more about in the next six months.

It’s important to understand what your prospects consider the most pressing topics and - *IF* relevant - ensure you are part of the conversation.

The IF here is key. If you don't have an authentic need to discuss a topic, don't do it for the sake of tagging in to the hype. It'll have a negative impact on your brand if you are just seen as bandwaggoning.

While we all might be feeling a slight AI-fatigue, your comms programmes need to adapt. You need to find ways to produce content about AI that fits within your broad messaging plans and that’s innovative enough to cut through the “AI-haze” littering the cybersecurity marketing ecosystem.

Don't get caught out by buzzword bingo

So how can you differentiate and begin to move beyond the buzzword? Your approach needs to be multifaceted. You need to engage in the latest conversations while staying clear of generic AI announcements. You need to delve deeper and focus on specific applications of AI within your cybersecurity solutions or important themes like regulation. Importantly, you need to bring it back to how it is going to help your clients, customers, and prospects. This showcases your expertise and avoids the trap of repetitive, uninformative rhetoric.

From Awareness to Consideration to Decision

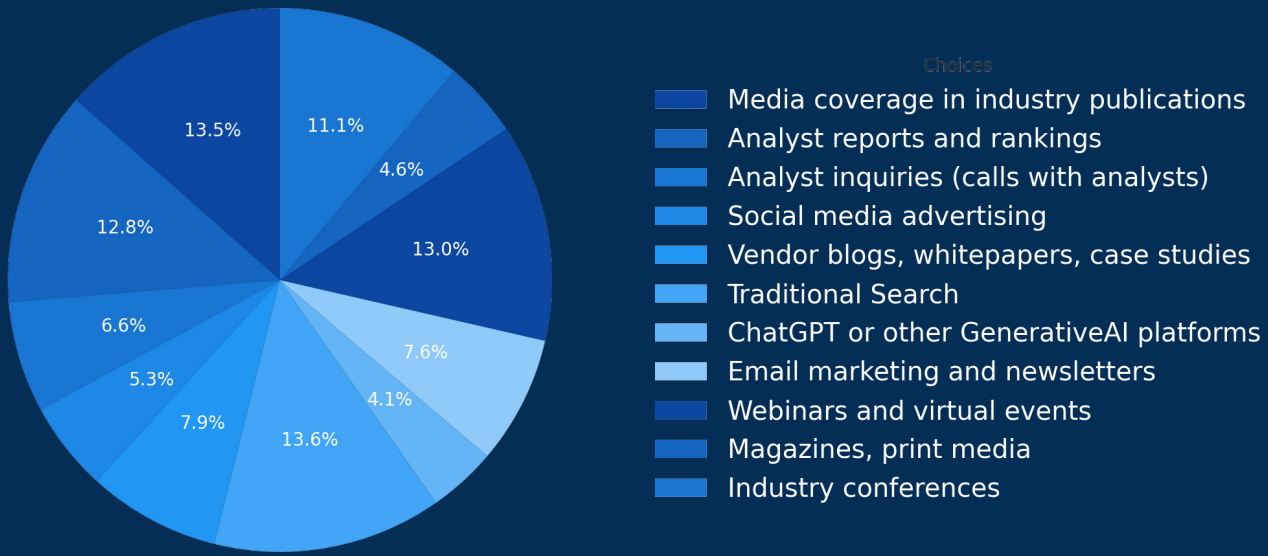
The channels decision-makers use to learn more about cybersecurity products

WHERE DO YOUR PROSPECTS GO WHEN SEARCHING FOR A NEW SOLUTION TO THEIR CHALLENGES?

In cybersecurity, grasping where decision-makers turn for insights at each stage of their buyer journey isn't just useful—it's necessary. With a landscape as diverse as their needs, understanding these patterns offers a golden key for communication and marketing managers aiming to deliver messaging and storylines that resonate.

Our recent survey, sheds light on the multifaceted approaches these decision-makers employ to gather product and service information.

The primacy of traditional search: Standing at the forefront, traditional search engines are the go-to resource for 53% of respondents, emphasising the indispensable role of SEO and online content strategy in capturing the attention of cybersecurity professionals.



Resonance

Where Do Your Prospects Go When Searching for a New Solution to their Challenge?

In today's rapidly evolving digital landscape, understanding where cybersecurity decision-makers turn for solutions to their cybersecurity challenges is crucial for any technology provider. As businesses continuously adapt to changing threats and emerging technologies, the pathways they explore for information are as diverse as the solutions themselves.

This report delves into the multifaceted approaches employed by professionals in the field, examining the primary sources they rely on to inform their decisions and guide their strategic initiatives. From traditional media to the frontiers of generative AI, each channel reflects the complex decision-making process that leaders fo through for cybersecurity solutions.

The Primacy of Traditional Search: Standing at the forefront, traditional search engines are the go-to resource for 53% of respondents, emphasising the indispensable role of SEO and online content strategy in capturing the attention of cybersecurity professionals.

Media and webinars Close Behind: Industry publications and webinars/virtual events closely trail, captivating 53% and 51% of the audience respectively. This underlines the critical importance of PR and interactive digital formats to engage and inform.

Analyst Insights Command Respect: Cybersecurity is a trust game. Garnering the trust of 50% of IT decision-makers, analyst reports and rankings, along with industry conferences (43%), highlight the weight placed on authoritative insights and community engagement for in-depth understanding.

Direct Vendor Communications Influence Decisions: With 31% turning to whitepapers, case studies, and vendor blogs, the impact of your owned media and content in guiding purchasing decisions is unmistakable, pointing to the effectiveness of detailed, problem-solving oriented communications.

Emerging Influence of Generative AI: Platforms like ChatGPT, though in their infancy, already draw the curiosity of 16% of respondents, hinting at the burgeoning interest in AI-driven self-education and information discovery.

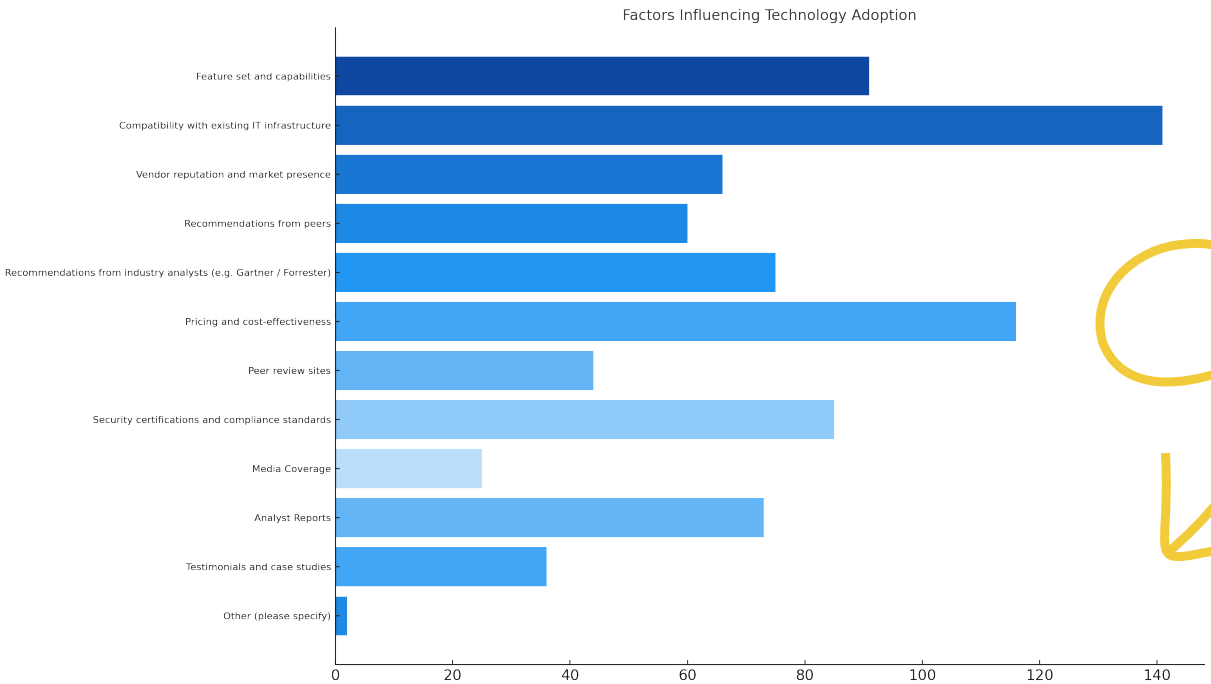
The Value of Personalised Expert Feedback and Peer Insights: Industry conferences and analyst inquiries, engaging 43% and 26% respectively, underscore the significance of experiential knowledge and expert consultations in navigating the cybersecurity ecosystem.

Diverse Channels for Broad Strategies: Email marketing (30%), social media advertising (21%), and magazines/print media (18%) demonstrate the varied strategies employed by IT decision-makers, reinforcing the need for a broad, yet targeted, marketing mix.

It's important to note that finding information out is a very different task to establishing whether you actually want to purchase a solution.

VALUE MEETS VISIBILITY: MASTERING THE ART OF BEING SHORTLISTED

The criteria IT decision-makers use to shortlist cybersecurity solutions for further evaluations



It's no surprise the data reveals pricing and cost-effectiveness carries the most influence when it comes to shortlisting solutions. This highlights the commercial realities facing cybersecurity leaders tasked with security investments – value is imperative even when protecting critical assets and data.

With media coverage bottoming out, followed closely by case studies, it's a clear indication that when moving from the awareness to consideration stage the game changes, and your best chance as a marketer is to gain influence with analyst-focused outreach.

So while headline elements like features and compliance dictate early selection, compelling analyst relations, customer evidence and media visibility offer ways cybersecurity comms teams can showcase credibility and technical excellence to give their solutions an edge. The art is in crafting solution stories that resonate.

HOW CAN YOU BEGIN TO NAVIGATE THESE MUDDY WATERS?

As the research indicates, cybersecurity prospects consume information from a wide range of sources at different stages of the buyer journey, from awareness to consideration to decision.

With stakeholders accessing information across multiple channels, comms strategies need an integrated approach - a holistic communications programme that allows teams to "**control the controllable**". This means implementing coordinated public relations, analyst relations, inbound marketing, and content strategies that work together to amplify your messaging and meet your buyers with the right information, at the right point during the buyer journey.

At Resonance, our holistic communications programmes are designed to help cybersecurity organisations cut through the noise.

Public Relations:
Our PR specialists secure high-impact coverage and thought leadership (guest articles) in national and top tier technology media, profiling organisations as innovative market leaders. Our secret weapon is that we are the best newsjackers around, which allows us to inject our clients into timely news cycles with proactive pitching, placing key messages in leading publications.

Analyst Relations:
We leverage long-standing analyst relationships to showcase innovation and drive adoption amongst influential advisory firms. These include Gartner, Keypoint Intelligence, and Everest Group, which ranked as the top three most trusted analyst firms for insights in our study. Analyst relations boosts market awareness and validation, and as our research indicates, is the most important controllable aspect to get your products shortlisted.

Content:
Resonance creates bingeable, snackable content optimised for search and shares. Branded and ghost-written long-form articles, blogs, infographics, and more, tell client stories that move audiences along the path to purchase.

Inbound Marketing:
With SEO, email marketing, lead gen campaigns, and marketing automation, we fuel a flywheel effect - using content to attract and engage ideal prospects. Our inbound services increase site traffic, generate leads, and accelerate pipeline growth

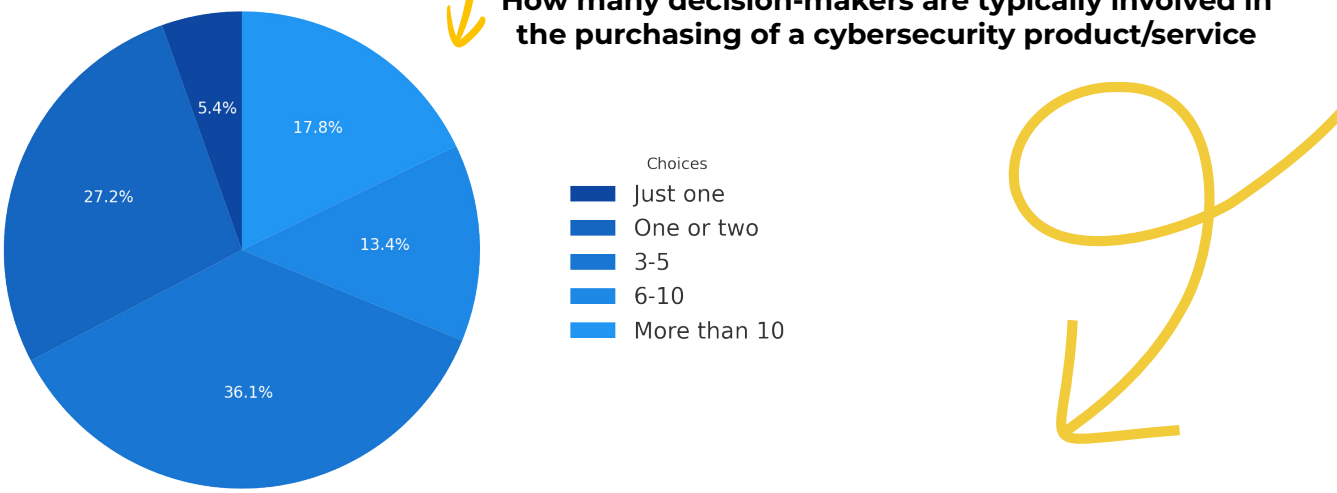
With an emphasis on meaningful measurement, our holistic communications programme delivers targeted awareness, increased consideration, and sales velocity.

UNDERSTANDING THE COMPLEXITIES OF CYBERSECURITY DECISION-MAKING

Understanding the decision-making process behind purchasing new cybersecurity products or services within organisations is crucial for those aiming to effectively target prospects. While each organisation will have varying levels of complexity to navigate - we need to attempt to do so from the outside.

Firstly, let's consider the data:

How many decision-makers are typically involved in the purchasing of a cybersecurity product/service



There are multiple decision-makers involved in the purchasing process, with ten or more involved in some instances. It's a complex situation and it should be. They're choosing to purchase their proverbial armour. In a way, the numbers are almost comforting given that there is so much emphasis on getting cyber solutions correct and ensuring a business is as safe as possible.

So, what does this mean for you?

You need a holistic plan of attack involving all the components mentioned above - and this is exactly where Resonance can help.

By establishing a robust online presence and cultivating positive media coverage through strategic PR initiatives, you can elevate brand awareness and establish yourself as thought leaders within the cybersecurity domain.

The development of high-quality, informative content tailored to the specific needs and challenges faced by different stakeholders within the decision-making process is paramount. This content, such as blog posts, white papers, case studies, and other relevant materials, can serve to educate potential customers, address their concerns, and ultimately position your offerings as the optimal solution.

Through the targeted distribution of this content via social media channels and industry publications, you can ensure your message reaches the "correct eyes" within the complex decision-making sphere.

This comprehensive approach empowers cybersecurity comms professionals to not only effectively engage with all relevant stakeholders but also successfully communicate the value proposition of their products and services.

CHALLENGING THE STATUS QUO: THE EVOLVING LANDSCAPE OF PRODUCT PROMOTION

Over the past few years, we've noticed a shift in how IT decision-makers identify and evaluate solutions.

While issuing press releases announcing product launches may have served in the past, there is now a need for a more nuanced and impactful approach. Our stance is rooted in the diminishing returns associated with solely relying on traditional media coverage. And our research backs this notion as evidenced in the data. When building a comms program, it is critical to recognise this limitation. In other words, only a limited number care about product updates. What people do care about is IMPACT.

You need a multi-faceted product approach designed to resonate with a broader audience and demonstrably influence the decision-making process.

Our research indicates that the best way to achieve this is through AR and a concerted focus on market presence - which go hand in hand. However, as our research also shows, distributing product releases is still important, it's just not what's going to get you through your prospect's door. Instead, success lies in cultivating a broader narrative that fosters industry engagement and thought leadership leveraged within different spaces for enhanced market presence.

While we've already touched on analyst relations - it's important to outline market engagement in a holistic comms program.



Resonance

LEVERAGING MARKET PRESENCE: DIRECT ENGAGEMENT WITH STAKEHOLDERS

Market engagement is an exceptionally powerful tool that underpins any successful cybersecurity comms programme. As such, it's imperative to actively participate in industry conferences, workshops, and webinars, and we constantly push our clients to do so. There aren't any downsides, as this presence allows you to:

Showcase your thought leadership:

Through presentations, demonstrations, and insightful discussions at cybersecurity events.

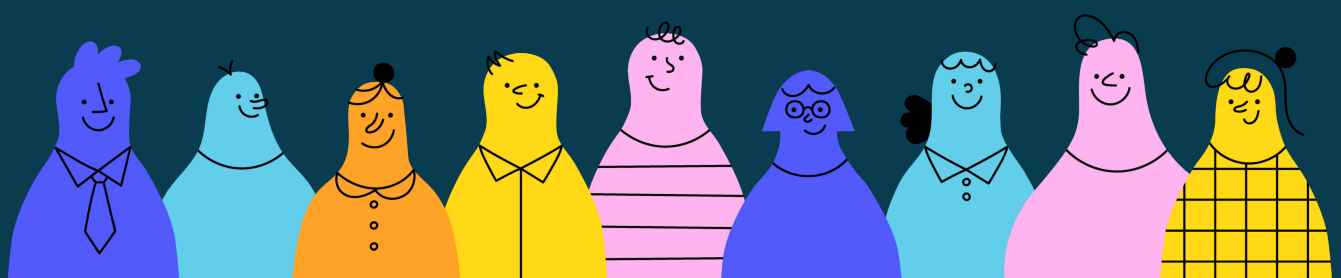
Network with key players:

These events provide valuable opportunities to build connections with decision-makers, understand their specific needs, and address their concerns directly. These learnings can then be applied to the components of a holistic comms programme.

Build brand awareness:

By actively and consistently participating in industry events, people will begin to know your brand, which will help establish your organisation as a trusted provider of cybersecurity solutions.

By implementing this multifaceted and strategic market approach, you will be able to establish your brand quickly with important decision-makers. This coupled with effective thought leadership and AR outreach, will ensure that your prospects know who you are and how you can help them. Let's also not forget that all the other components feed into this too, from newsjacking the latest stories to producing SEO-driven blog content.





Thanks to a threat landscape that will eventually cost the globe over **$13 trillion in 2028**, the cybersecurity market will continue to change shape.

While the myriad threats out there ensure that CISOs will continue to have many sleepless nights, they present the notion that there will always be opportunities for marketers to crack.

But, as our research indicates, getting in front of the many decision-makers involved in purchasing is no easy task given the sprawling nature of available information. Your best bet is to deploy a holistic communications programme, involving PR, AR, content and inbound marketing.

And we are here to help you do that.

If you'd like more information, or a complimentary cybersecurity communications healthcheck, get in touch today.

Hello@Resonancecrowd.com
+ 44 (0) 20 8819 3170