CyberRisk ALLIANCE

CyberRisk Alliance 2024

End of Year Report

CyberRisk Alliance 2024 **End of Year Report**

CyberRisk Alliance provides business intelligence that helps the cybersecurity ecosystem connect, share knowledge, accelerate careers, and make smarter and faster decisions.

Through our trusted information brands, network of experts, and more than 250 innovative annual events we provide cybersecurity professionals with actionable insights and act as a powerful extension of cybersecurity marketing teams.

Our company is organized into three core divisions, which all funnel data to and from and which benefit from our unified data and intelligence engine called **CyberCept**.

Our three divisions are:

CRA Connect, a full-service agency that offers solutions, crafts omnichannel campaigns and acts as an extension of your marketing team.

CRA Events hosts national conferences such as Identiverse, InfoSec World and MSSP Alert Live.

CRA Communities nurtures communities of local cybersecurity professionals through regional events, peer-to-peer collaboration, training and education, and resources for decision making support.

Our brands include SC Media, the Official Cybersecurity Summits, Security Weekly, CyberRisk TV, InfoSec World, Identiverse, CyberRisk Collaborative, ChannelE2E, MSSP Alert, LaunchTech Communications and TECHEXPO Top Secret.

Learn more www.cyberriskalliance.com

CRA Brands

SC Media – A CRA Resource

The Official Cybersecurity Summit – A CRA Resource

Security Weekly – A CRA Resource

CyberRisk TV – A CRA Resource

InfoSec World – A CRA Resource

identiverse – A CRA Resource

CyberRisk Collaborative – A CRA Resource

ChannelE2E – A CRA Resource

MSSP Alert – A CRA Resource

LaunchTech – A CRA Resource

TECHEXPO Top Secret – A CRA Resource

CyberRisk Alliance

Contents

OPENING COMMENTS 04

WHAT WE HEARD FROM OUR CUSTOMERS 06

WHAT OUR AUDIENCE ENGAGED WITH 12

- Topics 14
- SC Media 17
- MSSP Alert 18
- ChannelE2E 19
- Virtual Conferences 20
- Webcasts 21
- Podcasts 24
- Events 25
- Video Content 28

CISO AND CYBERSECURITY PRACTITIONER PRIORITIES 30

THE STATE OF CYBERSECURITY PUBLIC AND MEDIA RELATIONS 34

THE YEAR IN RECOGNITION 36

CLOSING THOUGHTS 38

CyberRisk ALLIANCE

Opening Comments

It's been a year unlike any other in cybersecurity. From major breakthroughs in AI technology to groundbreakingly widespread healthcare data breaches, the security landscape seemed to evolve minute by minute.

Our headlines included the CrowdStrike software update failure, devastating healthcare system breaches that put patient privacy at risk, and the revolution and proliferation of deepfake technologies. While the U.S. election cycle turned out to be less of a cybersecurity story than expected, there was no shortage of drama elsewhere—especially at OpenAI, whose internal turmoil and uncertain future influence has kept everyone on high alert. And if that weren't enough, Jen Easterly's departure from CISA and the peaceful transition of power following the U.S. presidential election signals a new era in federal cybersecurity leadership, one we will all also be watching closely.

Here were just a few of the top stories of the year as we were tracking them:

Chinese CyberEspionage Campaigns

Salt Typhoon Attacks: Chinese hackers, identified as the Salt Typhoon group, infiltrated major U.S. telecommunications providers, including AT&T, Verizon, and T-Mobile. This breach enabled them to geolocate individuals and intercept communications, affecting high-profile figures such as President-elect Donald Trump and Vice President-elect JD Vance.

MirrorFace Operations: Japan attributed over 200 cyberattacks targeting its national security and high-tech sectors to the Chinese hacker group MirrorFace. Targets included government ministries, the Japanese space agency, and private companies.

Major Global IT Outage Caused by the Crowdstrike Update

In July, a faulty update from cybersecurity firm CrowdStrike led to a global IT outage, causing widespread disruptions across various sectors, including aviation, healthcare, and finance. The incident highlighted vulnerabilities in critical infrastructure and the cascading effects of software failures.

The Biggest Ransomware and Data Breach Stories

Change Healthcare Attack: A ransomware attack on Change Healthcare disrupted services across the U.S. healthcare system, impacting over 100 million individuals. The breach exposed sensitive patient data, underscoring the healthcare sector's vulnerability to cyber threats.

Snowflake Customer Breaches: Cybercriminals exploited stolen credentials to access accounts of several prominent companies using Snowflake's cloud data platform. Victims included Ticketmaster, Santander Bank, and Neiman Marcus, leading to significant data theft.

Intensified Iranian Cyber Activities

Iranian state-sponsored hackers intensified cyber espionage efforts, targeting U.S. political campaigns and Middle Eastern affairs specialists. Notably, they attempted to breach a high-ranking official's email from a U.S. presidential campaign, reflecting ongoing geopolitical cyber tensions.

Cybersecurity Ecosystem and Industry Developments

IronNet's Collapse: IronNet, a cybersecurity firm founded by a former NSA director, ceased operations after failing to achieve profitability. Its downfall serves as a cautionary tale about the challenges even well-connected cybersecurity startups can face.

In this report, we'll explore what cybersecurity professionals engaged with from our portfolio of offerings, and explore the trends that stand to define the year in cybersecurity marketing that lies ahead.

What We Heard **from Our Customers**

What We Heard from Our Customers

We were honored to present the opening keynote at this year's CyberMarketing Con, hosted by the Cybersecurity Marketing Society. In our presentation delivered by CyberRisk Alliance President, John Whelan, we summarized key points of guidance we gleaned from the 1st party data in CyberCept, and what we've heard from our 600+ customers, that we feel will and should inform cybersecurity marketing strategies in 2025.

First, it's important to set the overall background context. In the current realm of B2B marketing, the pervasive sentiment is that investments in ABM and marketing automation technologies and the promise of attribution haven't quite paid off as marketing teams and senior leadership had expected them to. In the second half of 2024 there were countless think pieces on LinkedIn that outlined the overwhelming disillusionment related to core B2B marketing tactics and technologies that many companies had built their marketing strategies on or around in the last decade.

This isn't all that surprising when you look at the timeline of events and trends the last 5-7 years in B2B marketing. Most marketing teams have been under immense pressure to demonstrate lead gen and pipeline gen since COVID-19 brought tremendous uncertainty to the global economic climate and everything moved swiftly online. One of the unfortunate results of a marked overcorrection toward attributable lead-generating budgetary spend was a near-abdication of focus on harder-to-measure contributions such as brand and thought leadership.

In the immediate post-COVID years we witnessed a big swing in budgets toward in-person activities and events but there is now some recognition that those tactics on their own aren't producing the expected results, and there's renewing interest in tactics that represent greater economies of scale such as digital marketing and advertising.

To add to all this, procurement processes among cybersecurity buying teams are only growing more complex as their budgets are also being scrutinized- which means all B2B marketers are observing longer sales cycles and being required to engage more members of the buying team than ever before on tighter marketing budgets.

So where should cybersecurity marketing teams turn their attention and focus? Here are the highlights from our presentation:

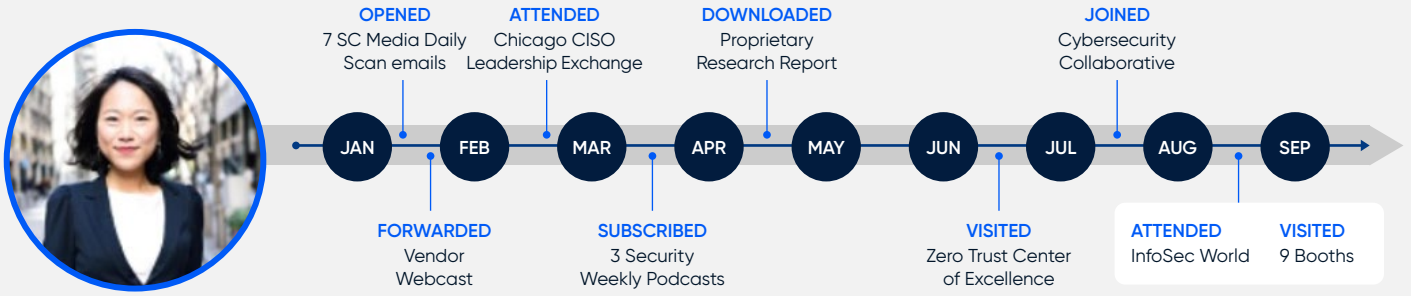
Bad ABM is worse than no ABM.

Good ABM has to begin with a strong knowledge of your ICP, great research and analysis that produces the right list of key accounts, very strong messaging and positioning, and then super tightly aligned marketing and sales efforts. If you're not equipped with all of that, it's highly likely to fail. Not only that, but ABM is not measured on the basis of a single activation or event, i.e. a webcast - it's the accumulation of many different touchpoints with members of your buying teams over time. If you fall short on any of the core elements of ABM, your attempts could achieve the opposite results you're looking to achieve among crucial decision makers for your business. Don't skimp on the fundamentals.

Integrated marketing **works.**

Compiling multiple tactics into coherent programs and campaigns is still the foundation of effective B2B marketing. Integrated marketing works and, in fact, solid integrated marketing execution can lead, mature, and evolve into a strong ABM strategy. But rarely, if ever, does a company execute an ABM strategy without having a solid integrated marketing framework.

If you haven't quite figured out how to launch and execute successful multichannel or omnichannel campaigns that effectively target the buying teams of your ICP, that's the first step. Here is an example of real reporting we've delivered to our customers who are driving success with integrated marketing campaigns, and it's representative of the kind of exposure that's required to get everyone on that buying team hearing the same message, positioning, and brand prominence that they'll use to put together their shortlist of solutions to evaluate.



Jamie P.
Health Systems CISO

Name: Jamie P.
Title: CISO

Organization Name: Health Care System
Role: CISO

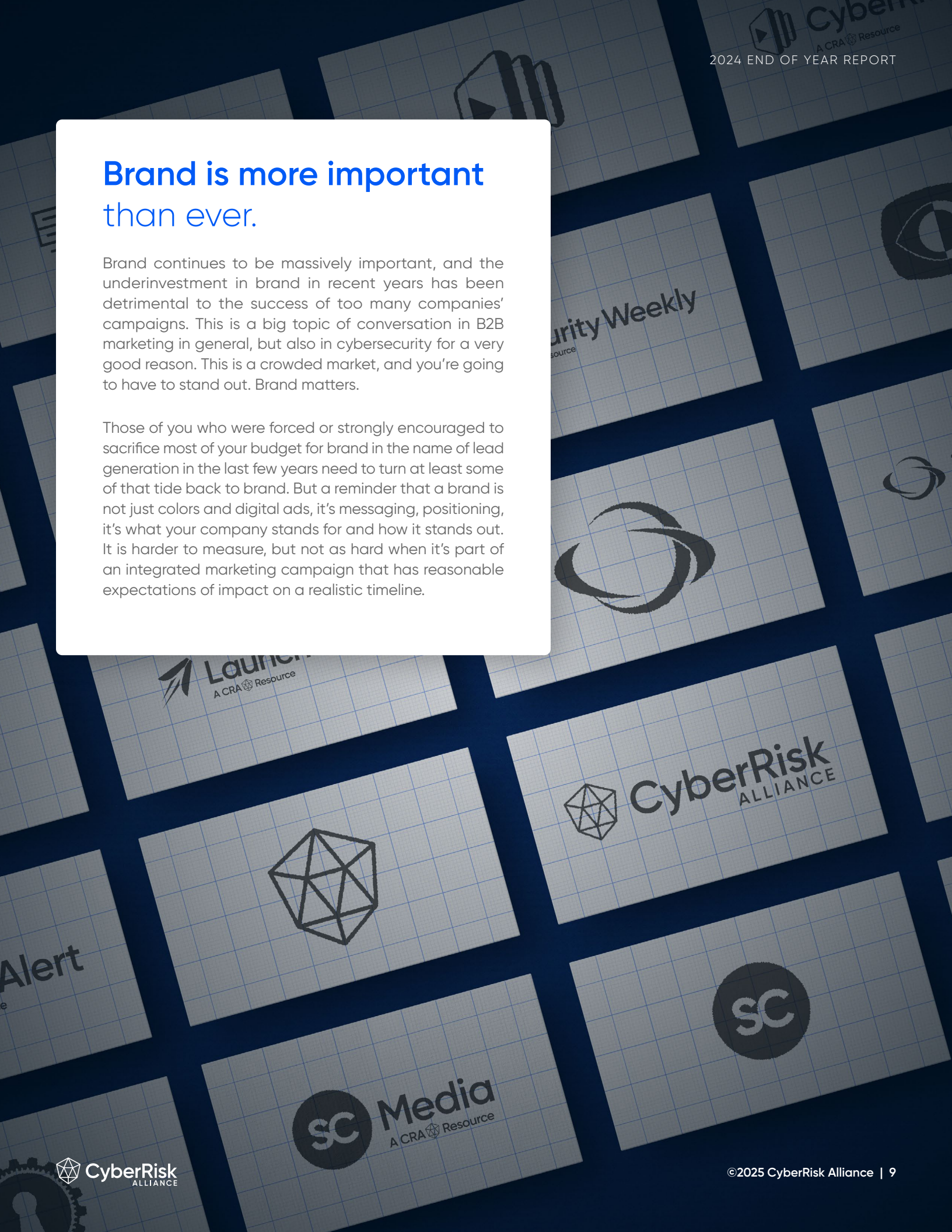
Topics: Zero Trust, Identity, Ransomware
Solutions Explored: Arctic Wolf, Sophos

Chief Information Security Officer	1					1						2
Director, Information Security		1					1					2
Director, Information Technology		1	1						1			3
Security Engineer				1	1						1	3
Senior DevOps Engineer						1		1				2
Senior Information Security Engineer					1				1			2
Program Manager		1			1							2
Director, Security Engineering				1	1						1	3
IT Program Manager					1		1					2
Manager, IT Operations					1					1		2
TOTALS	1	3	1	2	6	2	2	1	2	1	2	23
Activity Type	Live Event	CRA Custom Content	CRA Custom Content	eBook	eBook	CRA Custom Content	eBook	eBook	Webinar	Webinar	eBook	

Brand is more important than ever.

Brand continues to be massively important, and the underinvestment in brand in recent years has been detrimental to the success of too many companies' campaigns. This is a big topic of conversation in B2B marketing in general, but also in cybersecurity for a very good reason. This is a crowded market, and you're going to have to stand out. Brand matters.

Those of you who were forced or strongly encouraged to sacrifice most of your budget for brand in the name of lead generation in the last few years need to turn at least some of that tide back to brand. But a reminder that a brand is not just colors and digital ads, it's messaging, positioning, it's what your company stands for and how it stands out. It is harder to measure, but not as hard when it's part of an integrated marketing campaign that has reasonable expectations of impact on a realistic timeline.



Events are still popular, but you have to sponsor events that **move your strategy forward**.

Obviously, you've got to be generating leads too and events have been a very popular way to generate leads in the past few years - we know because we host over 150 of them every year.

Remember that a customer has already done a ton of their own research and had multiple conversations before your sales team ever talks to them, but you're also on the hook for getting your salespeople in front of people who are actively evaluating products. Events remain a really impactful and influential way to do that and to establish relationships and rapport with key members of the buying team. However, not all events accomplish everything - you should be using a range of different event types to accomplish your goals depending on the maturity and velocity of your pipeline.

Larger-sized trade shows are best for increasing your brand awareness. Smaller, more community-based regional events are generally better to directly engage with cybersecurity practitioners from your target accounts and help them kick the tires on your technology. Partner and experiential events are where you wine and dine or provide unique experiences for members of the buying team from your target accounts on midfunnel sales opportunities to try and actively close a sale. There are a lot of options out there, so ensure you're selecting the right one(s) to invest in for the business.

Side note here for demand gen leaders - ensure you're seeing all leads coming through across all regional events! We have seen regional teams reject strong leads that were firmly in our customer's ICP and even from their target account lists, but because they weren't on that specific rep's target account list for their territory, they were rejected. Don't let that happen! It's a waste of money and a waste of a potentially good lead (see the above point on bad ABM being worse than no ABM).

To summarize: next year won't be about massive, disruptive innovation – it's about getting back to some of the basics, and optimization of what has worked in the past.

Balance, diversification, and integrated marketing programs work. There is no new "silver bullet," no disruptive technological advancement, no simple answer in marketing right now despite the rise of generative AI. Most likely we'll need to wait until 2026 to see what settles as the best application of generative AI technologies to the practice of B2B marketing.

Until then, 2025 is the year to hone and optimize the basics and ensure your foundation is solid. You need to have a great, differentiated brand with a clear and distinct voice and position. You need to be designing and executing great integrated marketing programs and campaigns that reach the right buying teams and influence them where they are seeking information. You need good data and research that gets you the answers to the most basic questions (ICP, target personas) and then to build from there you'll need a good supply of great content and subject matter experts who are capable of speaking publicly, intelligently and engagingly on the subjects that matter most to your core audience. Simple, right?

The remainder of this report will provide you with insights from across the CyberRisk Alliance portfolio on what cybersecurity professionals engaged with, what resonated with them, and what they're likely to be looking for more of in 2025.

We encourage you to use the insights to build better programs and campaigns this year, and if you're looking for support we hope you will reach out and set up time to learn how we can help:

www.cyberriskalliance.com

What Our **Audience Engaged With**

What Our **Audience Engaged With**

CyberRisk Alliance has the unique benefit of observing trends on the cybersecurity and IT security practitioner side as well as trends from the cybersecurity marketing teams we work so closely with on a daily basis. Our job is to synthesize these two points of view into an always-on interchange of information, needs, desires, and interests to serve the creation of authentic connection between hands-on-the-keyboard practitioners, senior cybersecurity leadership, and cybersecurity technology vendors.

To help further that initiative, we are happy to provide some insight on what content, topics, and themes were most popular across our portfolio of brands. Here is some of our top-performing content from 2024.

CyberRisk ALLIANCE

News Media

Topics

CyberRisk Alliance tracks 25+ topics that represent a wide swath of the full catalogue of cybersecurity security technology categories that exist in the ecosystem today. We actively maintain tagging and reporting on all of these categories and produce SC Media newsletters, Security Weekly podcasts, and Virtual Events programming throughout the year that is directly aligned with these topics.

Here are the top performing (by visits) articles in each of the top categories we track:

ARTICLE	TOPIC	
 Biggest AI trends of 2024: According to top security experts	AI/ML	View
 4 key takeaways from NIST's new guide on AI cyber threats	AI/ML	View
 'ASCII Smuggling' attack exposes sensitive Microsoft Copilot data	AI/ML	View
 Qualcomm chip vulnerability enables remote attack by voice call	Application Security	View
 AppSec survey reveals troubling trends	Application Security	View
 PCI DSS 4.0: What changes for AppSec?	Application Security	View
 Broadcom Relaunches VMware Cloud Service Program With New Benefits	Cloud Security	View
 Abandoned VMware Partners Courted by Broadcom Competitors	Cloud Security	View
 Cloud 2024: SaaS nightmares, API security boom and the impending cloud 'identity crisis'	Cloud Security	View
 5 cybersecurity compliance deadlines in 2024	Governance, Risk, & Compliance	View
 Organizations Scramble for Cyber Insurance	Governance, Risk, & Compliance	View
 MSP, Backup Vendor Sued Over Cybersecurity Breach	Governance, Risk, & Compliance	View
 Huawei: Banned and Permitted In Which Countries? List and FAQ	Identity	View

News Media

Top performing (by visits) articles continued

ARTICLE	TOPIC	
 U.S. House Bans Microsoft Copilot for 365 for Staffers	Identity	View
 Spyware behind nearly 50% of zeros-days targeting Google products	Identity	View
 Huawei: Banned and Permitted In Which Countries? List and FAQ	Network Security	View
 Ubiquiti router users urged to secure devices targeted by Russian hackers	Network Security	View
 Black Hat USA: Wi-Fi tracking flaw puts the 'BS' in BSSID	Network Security	View
 Over 2M Mr. Cooper customers' records exposed by unsecured database	Ransomware	View
 Comcast Faces Lawsuits over Breach of 36M Accounts	Ransomware	View
 Over 1.3M PandaBuy customers hit by data breach	Ransomware	View
 Top 10 Cyberattacks of 2023	Threat Management	View
 NPM registry prank leaves developers unable to unpublish packages	Threat Management	View
 Akira ransomware group's changing tactics: What you need to know	Threat Management	View
 Exclusive: Cyberattack on Change Healthcare was an exploit of the ConnectWise flaw	Vulnerability Management	View
 CrowdStrike discloses new technical details behind outage	Vulnerability Management	View
 CISA breached by hackers exploiting Ivanti bugs	Vulnerability Management	View
 What are the foundational pillars of an effective zero-trust solution?	Zero Trust	View
 How to evaluate and compare zero-trust platforms	Zero Trust	View
 What you need to know before you can modernize your network-security architecture	Zero Trust	View

News Media

Our Key Takeaways

Of this list, the three highest engagement articles were those about the Change Healthcare, Mr. Cooper and Comcast breaches. Data breaches still lead news coverage, supporting the age-old adage, "if it bleeds, it leads." You might be asking yourself, so what's noteworthy about that? Every organization remains worried about becoming one of these headlines. It's always worthwhile to stay on top of the latest big breaches in your target industries to use as compelling, real-life and recent use cases for demonstrating why cybersecurity technologies can help reduce that kind of risk for their organization.

For emerging technology or emerging-adjacent categories such as AI, the top articles generally reflect broader guidance and overarching trend content, vs. categories that are more mature or "well-trod," such as Network Security, Cloud, or Identity where the highest-engagement articles are "weedier" in terms of the incidents and sub-topics they cover.

Among our most engaged cohort within our CyberCept audience, we found that the most popular topic in 2024 was governance, risk and compliance (GRC), with identity closely following behind, and the third topic of favor was cloud. No doubt the engagement in the GRC topic was driven, at least in part, by those seeking some guidance on how to create some governance around the use of generative AI.

Also worth noting here is the topic-based growth rate for each of the topics. Over the past 21 months the following topics saw the most growth in terms of engagement:

- **Privacy grew 3400%**
- **Third Party Risk grew more than 2800%**

On the surface it seems counterintuitive that AI isn't at the top of this list. However, we are confident that because AI can be a nebulous topic that has applications which extend far beyond just the confines of AI, it most likely was responsible for some of the growth in engagement with the privacy and third party risk topics.

SC Media

The Most Popular SC Media Articles of 2024

(measured in visits)

ARTICLE	
 NPM registry prank leaves developers unable to unpublish packages	View
 Exclusive: Cyberattack on Change Healthcare was an exploit of the ConnectWise flaw	View
 Over 2M Mr. Cooper customers' records exposed by unsecured database	View
 Deadline looms for alleged LockBit extortion of Feds over 33TB of data	View
 CrowdStrike discloses new technical details behind outage	View

Our Key Takeaways

All of the top most visited articles from 2024 on SC reflect stories that depicted major breaches or business disruptions. Similar to the key takeaway from the topic articles for each topic, there is an obvious interpretation that "what bleeds, leads" here that we attribute more to the anxiety the industry feels about becoming the next headline.

Contrary to the cynical point of view that could be easily taken from this information, we instead attribute this to the cybersecurity industry's constant aim to improve, learn from where others have failed and to prevent the next potential breach. In-depth use cases, case studies, and strategic teardowns perform very well for teams who are able to produce and distribute them for this exact reason.

MSSPAlert

The Most Popular MSSP Articles of 2024

(measured in visits)

ARTICLE	
 Top 10 Cyberattacks of 2023	View
 Comcast Faces Lawsuits over Breach of 36M Accounts	View
 Law Firm Sues MSP Over Black Basta Ransomware Attack	View
 Organizations Scramble for Cyber Insurance	View
 IT Consulting Firm Blames MSP for Data Breach	View

Our Key Takeaways

Threat intelligence, data breach stories, legal implications and insurance offerings took the top spots for our MSSP audience in 2024. These topics paint a clear picture of an MSP and MSSP ecosystem that is assuming more and more responsibility for securing small to medium businesses and doing their best to stay on top of the evolving threat landscape, legal strategies and protections they require to maintain their businesses, and what role cybersecurity insurance will play in impacting their businesses now and in the coming years.

ChannelE2E

The Most Popular Channel E2E Articles of 2024

(measured in visits)

ARTICLE	
 Huawei: Banned and Permitted In Which Countries? List and FAQ	View
 Abandoned VMware Partners Courted by Broadcom Competitors	View
 MSP, Backup Vendor Sued Over Cybersecurity Breach	View
 Kaseya 365 Subscription Debuts at $3.99	View
 EY Announces Layoffs in Response to Economic Struggles	View

Our Key Takeaways

ChannelE2E provides stories, analysis, and insights related to the business of the channel, which is exactly what is reflected in the most popular articles from last year. From existential risks such as bans on certain technology providers, to legal liabilities for MSPs and vendors as repercussions of data breaches, and analysis of layoffs and reductions in workforce associated with the industry, those working in the channel had their own share of worries in 2024. Still, there were some new product and pricing launches and strategic market share opportunities that helped to counterbalance any sense of doom and gloom.

CyberRisk ALLIANCE

Virtual Conferences

Top 5 Virtual Conferences of 2024

(by registration)

CONFERENCE

Virtual Nationwide Official Cybersecurity Summit 2024

The 2025 event will take place in November

View 2024 | View 2025

AI as a cybersecurity enabler and threat: The story so far

View

Threat intelligence: Unleashing the full potential of your security arsenal

View

Application security: Key trends, tools and techniques

View

Virtual Finance & Risk Official Cybersecurity Summit 2024

The 2025 Finance Virtual Conference will take place in June

View 2024 | View 2025

Our Key Takeaways

Our annual Virtual Conference offerings provide a mix of industry vertical and solution category themes. Unsurprisingly, AI, Threat Intelligence, Application Security and Financial Services dominated the slate of 2024 events from a popularity standpoint, which reflects the trends we observed in other formats as discussed in sections above. Virtual conferences remain a highly efficient and effective way to demonstrate thought leadership, increase brand awareness, engage with buying teams all without paying for travel for your team. Attendees appreciate the chance to ask their questions, evaluate technologies, and earn CPE credits.

Webcasts

Top 5 Webcasts of 2024

(by registration)

WEBCAST

View

A CISO's Guide to Harnessing the Power and Managing the Risks of Artificial Intelligence (AI)

This briefing was based on the findings of a cross-sector task force of CISOs and staff who shared their challenges and best practices for helping their organizations securely implement AI solutions, like ChatGPT. Discussion topics included: (1) CISO guidance for supporting the demand for rapid AI adoption; (2) navigating the AI landscape; (3) implementing effective AI governance structures and practices; and (4) developing safe AI operating environments.

Supporting tools shown during the briefing included: (1) A CISO's Quick Guide for Secure AI Adoption; (2) AI Acceptable Use policy templates; and (3) AI Boardroom Presentation Template.

View

A CISO's Guide to AI Technologies

Generative AI has taken over the conversation and, in time, will be transformative to the cyber industry and our society. But the models are still in development, and ultimately, CISOs must discern the appropriate places to leverage AI tools to help their company as well as define the acceptable risks and proper usage. This panel discussion explored:

- Current uses of AI in security programs and where it adds the most value
- Key risks of leveraging AI tools and how you decide to accept the risk or not
- Impact of AI on attack trends and how your security posture should shift
- How to vet AI technologies and key questions security leaders need to ask

Webcasts

Top webcasts (by registration) continued

WEBCAST

View

Ransomware Attack Lessons, From MOVEit and Doubledrive to MGM/Caesars

This webcast dissected the lessons derived from ransomware attacks involving MOVEit, Doubledrive, and the MGM/Caesars breach in order to empower organizations in fortifying their cybersecurity defenses.

The session began with an in-depth analysis of the MOVEit ransomware attack, unraveling the tactics employed by threat actors to exploit vulnerabilities in file transfer systems. Drawing parallels, it then explored the Doubledrive incident, emphasizing the significance of robust backup strategies and the role they play in mitigating ransomware risks.

The webcast also examined the MGM/Caesars breach as a case study to underscore the evolving sophistication of ransomware tactics, shedding light on the importance of proactive threat intelligence and incident response planning.

View

Key GRC Priorities for the Second Half of 2024

As organizations navigate the dynamic landscape of governance, risk, and compliance (GRC), this webcast explored the critical priorities that would shape the second half of 2024.

Our experts provided insights into emerging regulatory landscapes, the integration of advanced technologies in compliance, and the strategic alignment of GRC frameworks with organizational objectives.

Webcasts

Top webcasts (by registrants) continued

WEBCAST

View

CISO Insights: Navigating the GRC Landscape

A robust GRC program fosters the ability to manage key risks and protect sensitive data, aligning security initiatives with organizational objectives; and ultimately allows the CISO to establish trust and confidence with key stakeholders. However, the constantly evolving regulatory landscape is resource-intensive to manage and requires striking a delicate balance of security controls that won't stifle productivity or innovation. In this panel discussion, CISOs from diverse industries shared insights on:

- Determining and implementing appropriate policies and security controls
- Addressing challenges to integrate GRC practices into organizational operations
- Securing adequate resources to implement and maintain a GRC program

Our Key Takeaways

Practical advice for mitigating the risks of generative AI and seizing the opportunities that it represents for cybersecurity dominated the most popular webcasts of 2024. This was seen in the focus on AI topics head-on, as well as in the popularity of the governance, risk and compliance (GRC) topics as well. The ransomware attack lessons webcast did a great job diving deeply into real-world use cases and providing pragmatic lessons learned that cybersecurity professionals could take and implement in their own organizations.

Podcasts

Security Weekly News won the votes on podcast programming with all three of the most popular Security weekly episodes of the year.

Top Podcast Episodes of 2024

PODCAST

Analyzing the CrowdStrike Incident and Its Ripple Effects

View

Dronepocalypse, Microsoft, DLINK, Home Depot, Phishing, NIST, VenomRat, Josh Marpet

View

Win 95, LastPass, Kubernetes, Sandworm, Bloomtech, Frontier, 911, Aaran Leyland

View

Our Key Takeaways

News is still a very powerful format of information transfer. And what bleeds, still leads. Coverage of the Crowdstrike incident on Security Weekly News episode 399 won the day for the most listens this past year. That will likely surprise no one, given how much the incident rocked the world and the cybersecurity ecosystem. And Microsoft dominated the other two most popular Security Weekly News episodes. This is validation of the earlier point related to brand- brand matters. Whether the news and media coverage is good or bad, if you're a household brand in cybersecurity or technology such as Crowdstrike or Microsoft, you will lead the headlines.

Events

Identiverse, the premier event for the digital identity security community, celebrated its 15th year in 2024 with a record-breaking 3,000 attendees and high engagement over four days of comprehensive programming at the ARIA Resort & Casino in Las Vegas, NV.

The 2024 conference featured over 260 industry-leading experts and innovators who provided invaluable insights through thought-provoking keynotes and interactive breakout sessions. A wide range of established and emerging solution providers also showcased the latest advancements in digital identity solutions.

This year's content spanned 13 core topics and numerous additional subjects, including applications of identity, architecture, standards, engineering, deployments and leading practices, identity verification and proofing, identity for security, privacy, ethics, public policy, professional development, the business of identity, vision, strategy, and futures.

Get the AI-generated Identiverse 2024 Trends Report for a full summary of what was covered

View

Hear the 2024 Identiverse session content and access transcripts of the sessions

View

Identiverse 2025 is scheduled for **June 3-6, 2025**, and will be held at Mandalay Bay in Las Vegas, NV. For more information, visit Identiverse.com.

Events

InfoSec World, the leading educational event for senior-level information security and cybersecurity professionals, celebrated its 30th anniversary with record-setting attendance September 23-25 at Disney's Coronado Springs Resort in Lake Buena Vista, Florida.

With more than 2,000+ professionals from around the world participating, InfoSec World 2024 showcased the latest in cybersecurity technology, innovative solutions, and cutting-edge educational programming over the course of six days, with pre and post conference workshops and summits.

2024 InfoSec World attendees had the opportunity to hear keynotes from distinguished speakers like Amy Bogac, Chief Information Security Officer at Elevate Textiles, and Zack Kass, AI Futurist at OpenAI, run with 3-time Olympian Shannon Rowbury, engage in one-on-one meetings, visit the live-streaming CyberRisk TV booth, win prizes, and gain insight into the latest industry trends.

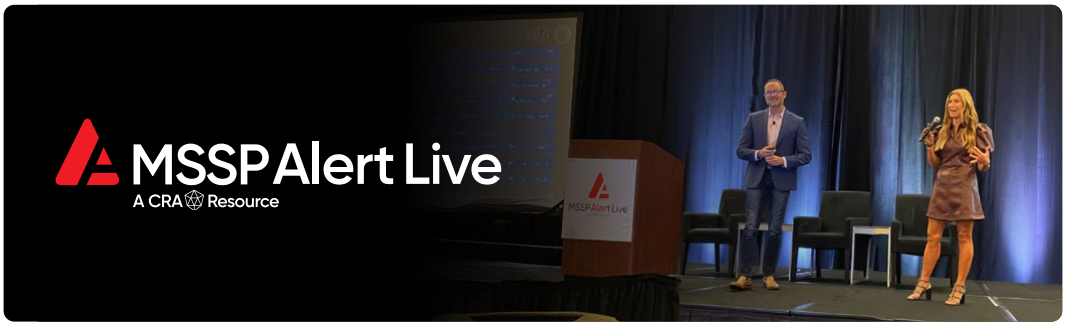
Highlighted session topics included artificial intelligence (AI), ransomware mitigation, cloud security, zero trust frameworks, and the evolving landscape of cybersecurity regulation. Attendees also explored workforce development strategies, diversity initiatives, and the latest technologies shaping the industry. During the 'Women in Cyber' breakfast, women leaders in cybersecurity gathered to collaborate, share insights, and empower one another. A new CISO track engaged attendees in executive sessions, lightning talks, a book signing, and other VIP opportunities.

Our most attended InfoSec World sessions in 2024 were:

 **GenAI - The Good, the Bad and the Ugly**	View
 **Preparing Your Cyber-Resilience Strategy for Operational Survivability in 2025**	View
 **Beyond the Ordinary Red Teaming: How Knowing the Offences Helps Execute and Defense**	View
 **Here's My Password - Building Effective Phishing Pretexts**	View
 **The Modern Application Security Rocket Ship**	View

InfoSec World will return to Lake Buena Vista, Florida, on **October 27-29, 2025**. For more information, visit infosecworldusa.com.

Events



MSSP Alert, the leading source of news, analysis, and research on managed security services providers (MSSPs), hosted its annual MSSP Alert Live event from October 14-16, 2024 in Austin, Texas. The event served as a powerful convergence of cybersecurity leaders, bringing together leaders and influencers from MSSP and MSP organizations worldwide for three days of networking, collaboration, and industry insights.

The 2024 MSSP Alert Live event featured a range of impactful sessions from industry leaders. ConnectWise revealed for the first time how they leveraged AI to navigate the ScreenConnect crisis, offering key lessons in real-world crisis management. A standout Cybersecurity Insurance and Warranties panel discussed the growing importance of insurance in managing cyber risk and how warranties are shaping security investments. Additionally, cybersecurity attorney Eric Tilds provided insights into cyber liability after a breach, advising MSSPs and MSPs on how to minimize legal risks and ensure compliance.

The event culminated with the unveiling of the 2024 Top 250 MSSPs list, recognizing the most influential companies in managed security services. For the first time, the list was revealed live, adding an exciting dimension to the conference and celebrating the achievements of the honorees in person.

A more in-depth look into the most important discussions at MSSP Alert Live 2024 can be found in our coverage of the event.

2024 Top 250 MSSPs list

View

MSSP Alert Live 2024 coverage

View

MSSP Alert Live will take place in **October, 2025**.

Video Content

In 2024 CyberRisk Alliance launched our **CyberRisk TV** brand and began to offer a broader range of video content and solutions beyond the on-site interviews we had captured at RSAC and Black Hat for the last several years.

We now include a CyberRisk TV studio on the show floor at our Identiverse and InfoSec World conferences, we kicked off a new video interview series profiling Cybersecurity founders called **Founder Stories**, and we offer media partnerships to provide coverage of key industry events.

You can catch all of the best cybersecurity event video content on CyberRisk TV by becoming a subscriber.

The Most Popular Interviews from RSAC 2024

Watch the full playlist

Introducing Nightwing - A New Intelligence Services Company, 40 Years in the Making - Jon Check

View

Security through Data – Cisco Hypershield - Jeetu Patel

View

The Enterprise Browser: The First Win-Win-Win For CISOs, CIOs and End Users - Mike Fey

View

CTEM: Understanding the essentials and why it matters - Zaira Pirzada

View

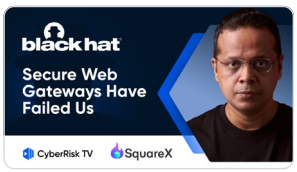
Identity is Security: Okta is leading the fight against Identity-based attacks - David Bradbury

View

Video Content

The Most Popular Interviews from Black Hat 2024

Watch the full playlist



Secure Web Gateways Have Failed Us - Vivek Ramachandran

View

The shift from risk to resilience - Justine Bone

View

Addressing the Rise of Deepfake-Driven Scams: Expert Insights - Allison Miller

View

SaaS Security Beyond Just Misconfiguration: Insights from Adaptive Shield's CEO - Maor Bin

View

Understanding and Reducing Supply Chain Risk and Software Vulnerability Risks - Danny Jenkins

View

What makes for a compelling interview?

Product announcements and company announcements are always exciting. Beyond that, a unique piece of research or threat intel, or pragmatic and quick tips for improving your security stance will draw viewers. As a baseline, make sure your interviewees are subject matter experts, media trained and coached, and that they have a vibrant personality.

CISO and Cybersecurity Practitioner **Priorities**

The Official Cybersecurity Summit
A CRA Resource

The Official Cybersecurity Summit

As part of our standard registration process for our Official Cybersecurity Summit events we query our registrants to ask about their most important cybersecurity challenge to ensure we stay aligned to what they want to learn about. Here is a word cloud that represents a distillation of their 2024 responses:

Our Key Takeaways

The top important cybersecurity challenges reflected here are unsurprising: AI, Ransomware, Phishing, Cloud Security, Data Security, Compliance, and Vulnerability Management.

CyberRisk Collaborative
A CRA Resource

CISO Executive Management and Technology Investment Priorities

The CyberRisk Collaborative (CRC) is a leading provider of peer-driven collaboration, decision support and career acceleration for cybersecurity practitioners. In addition to CRC benefits, members receive special access and discounts to events, research, news and more.

On a quarterly basis, we survey a group of our 2,000+ CISO and senior-most cybersecurity leader members to inquire about their executive management and cybersecurity technology priorities. What follows is an excerpt of the analysis of their priorities in each category.

CISO Top 10 **Executive Management**

Q1 2025

RANK	PRIORITY	TREND
1	Security Metrics	↑ Up from **4**
2	Governance, Risk, and Compliance (GRC)	↓ Down from **1**
3	Strategic Planning	+ New Entry
4	Data Privacy	+ New Entry
5	Business Continuity/IR/ Crisis Management	↓ Down from **3**
6	Stakeholder/Board Engagement	↓ Down from **5**
7	Technology Selection, Use, Integration	↓ Down from **5**
8	Budget and Resource Allocation	+ New Entry
9	Role of the CISO	↑ Up from **10**
10	Leadership Development	+ New Entry

Dropped Priorities

- Risk Management
- Personal Liability as a CISO
- Security Awareness & Education
- Workforce Recruitment, Development, Retention

Key Takeways

The rise of Security Metrics as the top priority highlights the increasing emphasis on measurable outcomes and accountability in cybersecurity, driven by stakeholder demands for transparency. Emerging priorities such as Strategic Planning, Data Privacy, and Leadership Development focus on long-term, holistic approaches to cybersecurity, positioning CISOs as key organizational leaders. The decline of standalone priorities like Risk Management and Security Awareness & Education indicates that these areas are now integrated into broader frameworks, becoming operational standards rather than strategic initiatives. The addition of Budget and Resource Allocation underscores organizations' financial pressures, emphasizing the need for effective resource management. Overall, these changes demonstrate the evolving role of CISOs, who must now balance technical expertise with strategic leadership to align cybersecurity efforts with business objectives and drive organizational resilience.

CISO Top 10 **Technology**

Q1 2025

RANK		PRIORITY	TREND
1	↑	Cloud Security	↑ Up from **2**
2	↑	Identity and Access Management (IAM)	↑ Up from **3**
3	↑	Data Security	↑ Up from **4**
4	↓	AI/ML/Automation	↓ Down from **1**
5	+	Application Security/API Security	+ New Entry
6	↓	Vulnerability Management	↓ Down from **5**
7	↓	Supply Chain Cybersecurity	↓ Down from **6**
8	—	Zero Trust	— No Change
9	+	Attack Surface Management	+ New Entry
10	↓	Security Operations	↓ Down from **7**

Dropped Priorities
- Policies, Standards, and Procedures
- Asset Management

Key Takeways

CISO priorities have dynamically shifted to address emerging challenges while balancing innovation with risk management. Cloud Security has risen as the highest priority due to the increasing reliance on cloud services and the associated risks. Identity and Access Management (IAM) and Data Security have gained prominence, focusing on safeguarding sensitive data and managing identity in digital environments. New additions, such as Application Security/API Security and Attack Surface Management, highlight the urgency to secure development pipelines and address emerging threats. Meanwhile, the decline of Policies, Standards, Procedures, and Asset Management signifies a pivot toward more actionable, technology-focused initiatives. Though still vital, AI/ML/Automation has taken a secondary role to immediate priorities like cloud and data security. These changes underscore how CISOs are evolving their strategies to align with the rapidly changing threat landscape, ensuring that organizational objectives and resilience are met effectively.

The State of **Cybersecurity Public** and **Media Relations**

The State of **Cybersecurity PR in 2025**

Differentiating Your Brand Requires Authentic Thought Leadership

By Wayne Schepens

The cybersecurity PR market in 2024 was more competitive than ever, overcrowded with solution providers and categories. Vendors continued to battle for the attention of overwhelmed reporters who were bombarded by press releases, pitches, and marketing materials masquerading as "news." The glut of information led to a growing disconnect: reporters craving real insights, while vendors suffer from limited media coverage.

At the same time, as anyone who has been deeply invested in B2B marketing for the last 10 years will attest, investments in all of the marketing technology and in-person events in the world won't help distinguish your brand if you're not doing the foundational work to position what's new, novel, and noteworthy about what your company stands for.

One of the most critical and recently overlooked elements of building and maintaining a distinctive cybersecurity brand is authentic thought leadership. In the past, executives and key senior leaders inside of cybersecurity companies would take the time to generate original ideas, offer insights, and engage in meaningful dialogue about their industry's future. However, in today's fast-paced environment, executives often blame their busy schedules for their lack of contribution to the conversation. Worse, they rely heavily on their PR teams to both find opportunities and create compelling, contrarian narratives—only to dilute those ideas during the approval process.

But here's the simple truth: *to be a thought leader, you have to successfully distribute compelling thoughts. Thoughts that are delivered in the form of insight, analysis, and that demonstrate a unique point of view.*

In 2025, the stakes are only rising. The cybersecurity landscape will continue to evolve and proliferate rapidly, with new threats, categories, and technologies emerging daily. This offers an opportunity for companies that are willing to step up, invest in genuine thought leadership, and encourage their executives to take a proactive role in the conversation. By cultivating original, impactful ideas, vendors will not only cut through the noise but also establish themselves as trusted voices and brands in the industry.

For both PR teams and vendors, the message is clear: stop outsourcing thought leadership. Embrace it, and let your executives drive the conversation. The reporters—and your customers—will thank you.

The Year **in Recognition**

SC Awards

In 2024 for the SC Awards we recognized leaders and innovators in 33 different categories. This year's winners came from a diverse array of categories, with a mix of established players and emerging startups making their mark. From the evolving threat landscape to the rapid rise of AI-driven defenses, the 2024 SC Awards celebrate those who've not only kept up with these challenges but have pushed the industry forward.

This year's competition was impressive and inspiring with over 150 finalists representing a thriving cybersecurity industry. The winners were selected by a panel of over 50 independent experts from across the cybersecurity community. From advanced AI-driven solutions to groundbreaking approaches in cloud security, winners represent the cutting-edge advancements necessary to combat today's most pressing cybersecurity challenges.

All 2024 SC Award Winners	View
Trust Award Winners	View
Excellence Award Winners	View

In 2025 our SC Award winners will be announced and celebrated during the week of RSA in San Francisco. Get your nominations in for the 2025 SC Awards before **February 5th**!

Women in IT Security Awards

The SC Women in IT Security Awards celebrate the transformative role women play in shaping the future of cybersecurity and the power of their unique leadership. This year's program received 50% more nominations than the previous year, a welcome signal of increasing enthusiasm for recognition of the critical role that women play in the cybersecurity field. Honorees were chosen by a panel of women judges consisting of CISOs, cybersecurity directors, and privacy and governance experts from leading organizations.

The 2024 Women in IT Security honorees represented a diverse array of industries, ranging from finance and cybersecurity consulting to government, healthcare, and technology innovation. Among this year's honorees were Chief Information Security Officers, founders, senior intelligence analysts, and executive vice presidents, each bringing unique expertise to their roles and making essential contributions to security organizations of all sizes.

See all outstanding 2024 Women in IT Security honorees	View

We extend our heartfelt congratulations to all the honorees once again and thank them for their unwavering dedication and achievements.

Nominations for Women in IT Security Awards will open in **May, 2025**.

Closing Thoughts

The CyberRisk Alliance 2024 End-of-Year Report encapsulates another pivotal year for the cybersecurity ecosystem. From the rise in adoption and new uses cases for applying generative AI, the CrowdStrike update incident and its impact on the platform vs. best of breed dialogue, to the intensification of ransomware and nation-state sponsored cyber campaigns in alignment with the uneasy geopolitical climate, 2024 demonstrated the urgent need for adaptable, strategic marketing. As a trusted partner to cybersecurity professionals and to cybersecurity marketing teams, CRA leveraged its expansive portfolio to deliver actionable insights, foster collaboration, and drive measurable results. Our mission remains clear: to help you connect with your target audience, elevate your brand, and navigate an increasingly competitive market.

For cybersecurity marketing teams, our report underscores a crucial takeaway: 2025 is the year to focus on optimization, alignment, and balance. While the promises of Account-Based Marketing (ABM) and attribution may have often fallen short of expectations, we've identified what works—and what doesn't. Effective ABM requires a deep understanding of your ideal customer profile (ICP), strong data to identify target accounts, and tightly integrated sales and marketing efforts. Integrated campaigns remain the cornerstone of success, providing the foundation to mature into strong ABM strategies. At the same time, underinvesting in brand and thought leadership has left too many companies struggling to stand out in a crowded market. Building a differentiated, authentic brand must take center stage, alongside well-executed multichannel campaigns and carefully curated event sponsorships.

Our analysis of engagement trends reveals that cybersecurity professionals are drawn to actionable, real-world insights. Governance, risk, and compliance (GRC), identity, and cloud security were among the most popular topics in 2024, driven by the ongoing need for clarity around regulatory shifts and emerging technologies. Breaches and ransomware stories captured significant attention, highlighting the persistent anxiety about being the next headline. This presents a key opportunity for marketing teams: leverage compelling use cases and success stories to demonstrate your value.

As 2025 unfolds, we hope these insights provide a roadmap to elevate your marketing strategy, and we're here to help at every step of the way with the power of our entire portfolio.

Learn more and reach out:

www.cyberriskalliance.com

CyberRisk ALLIANCE

About **CyberRisk Alliance**

CyberRisk Alliance provides business intelligence that helps the cybersecurity ecosystem connect, share knowledge, accelerate careers, and make smarter and faster decisions. Through our trusted information brands, network of experts, and more than 250 innovative annual events we provide cybersecurity professionals with actionable insights and act as a powerful extension of cybersecurity marketing teams. Our brands include SC Media, the Official Cybersecurity Summits, Security Weekly, InfoSec World, Identiverse, CyberRisk Collaborative, ChannelE2E, MSSP Alert, LaunchTech Communications and TECHEXPO Top Secret.

Learn more at **www.cyberriskalliance.com**

Book a Call with Us

For more information: