BIG VALLEY MARKETING

# Insights and Reflections from RSA Conference 2024.....

THE ART OF POSSIBLE

During his opening keynote, RSAC Executive Chairman and Program Committee Chair Hugh Thompson called this year's 33rd RSA Conference the "G.O.A.T." [Greatest. Of.All.Time]. He wasn't wrong.

With more than 40,000 attendees, RSA Conference 2024 combined serious, headline-making policy discussions about national security and AI led by U.S. government officials such as Secretary of State Antony Blinken, Secretary of Homeland Security Alejandro N. Mayorkas, and Senator Mark Warner with more lighthearted entertainment keynotes featuring actors Matthew Broderick and Jason Sudeikis and a joyful, closing keynote performance by Grammy-awarding musician Alicia Keys.

After attending more than 20+ past RSAC conferences, we think this year's event stood apart from the rest due to its remarkable agenda. As we stand at this important inflection point in our industry, we wanted to share some of the insights we learned from this year's show.



## Move over AI – national security and geopolitics take center stage

Over the last several years, U.S. government officials increasingly have secured speaking slots at the RSA Conference to talk about the importance of private-public collaboration. Although AI was expected to dominate this year's show, national security quickly took center stage when U.S. Secretary of State Antony J. Blinken's keynote was added to the agenda. During his keynote, **"Technology and the Transformation of U.S. Foreign Policy"** unveiled the U.S. International Cyberspace and Digital Strategy, "which treats digital solidarity as our North Star. The test before us is whether we can harness the power of this era of [technological] disruption and channel it into greater stability, greater prosperity, greater opportunity. Building consensus around an affirmative vision is the first line of our tech diplomacy."

During his discussion with Dave DeWalt, Founder, CEO, Managing Director, NightDragon, on **"Ensuring Intelligence, National Security in a Rapidly Changing Technology World,"** U.S. Senator Mark Warner said, "Over the past 10-12 years, I have worked to redefine national security. Because I think in 2024 national security is not simply what nation has the most tanks, guns, ships and planes, but it is who is going to be dominant and most successful in technology. In China, we face the greatest economic and technology competitor our country has ever faced." Late in the conversation, Senator Warner warned, "One of the secret sauces of our country was one, our innovation, two, even if we didn't innovate here, we got to set standards, rules and protocols for technology. With those standards, we could put our values in those standards. I'm afraid that leadership and standards-setting is receding. China is flooding the zone on a lot of these standards-setting bodies and large corporate America has said we're not sure it's worth our time to send our engineers to these standards-setting bodies. We need to get back in the game."

*"The test before us is whether we can harness the power of this era of [technological] disruption and channel it into greater stability, greater prosperity, greater opportunity. Building consensus around an affirmative vision is the first line of our tech diplomacy."*


## Still early days when it comes to AI governance

During her keynote, **"A World On Fire: Playing Defense in a Digitized World...and Winning,"** Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly said, "AI has captured the imagination but avoided the failure of imagination. It will be one of the most powerful weapons of this century." Yet we are still in early days when it comes to developing guardrails for this technology. During his keynote, **"Homeland Security in the Age of Artificial Intelligence,"** Secretary of Homeland Security Alejandro N. Mayorkas spoke about the first meeting of the AI Safety and Security Advisory Board (AISSB), which is developing First Principles around AI and later will establish use guidelines for the safe and secure implementation of AI and then develop a national plan. "There is an absolute need for harmonization around AI governance and creating standards and resolutions and that's a work in progress. We work closely with our international partners like Five Eyes" to drive harmonization."

During his talk, **"A Constitutional Quagmire: Ethical Minefields of AI, Cyber, and Privacy",** attorney Daniel Garrie said that the laws that will govern AI are still 10 years behind and added that "auditing AI is very complicated and not many people are qualified to [do it]. It took decades to build the auditing process for the airline industry."

*"AI has captured the imagination but avoided the failure of imagination. It will be one of the most powerful weapons of this century."*

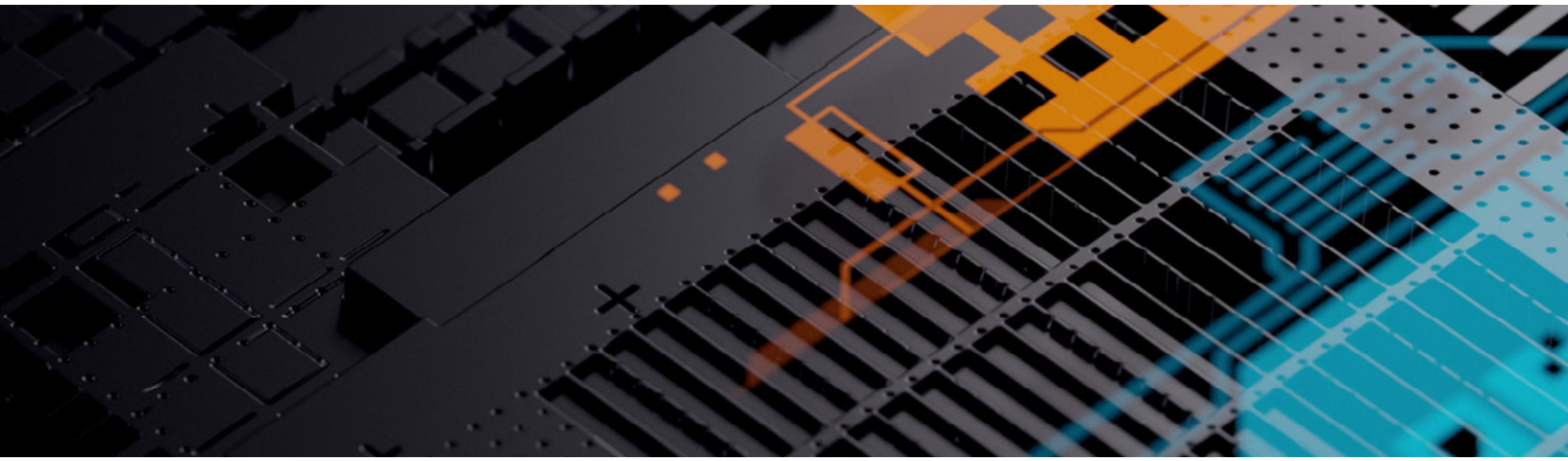
## CISOs in the Hot Seat

During his panel discussion, **"CISOs Under Indictment: Case studies, lessons learned and what's next,"** Joe Sullivan, the former Uber CISO who was sentenced to serve a three-year term of probation and ordered to pay a fine of $50,000 last year, remarked, "Things are heating up for CISOs in that the role is getting more attention than ever before and expectations are much higher. And the challenge for a lot of people in the role is that they got in the role, or they thought about getting in the role before the expectations and before the heat. They want to make sure they are doing the right things to navigate that heat." CISO's personal risk calculus has changed. We are targeted and it is not unintentional; the world of cybersecurity has become of critical importance to the world and every person in it now. Every business – every consumer – is dependent on the Internet. And yet the quality of security that we've been delivering hasn't grown up at the same pace."

*"Things are heating up for CISOs in that the role is getting more attention than ever before and expectations are much higher."*

"The government hasn't done a good job engaging with the CISO community, " said Charles Blauner, Cyber Aegis LLC, a panelist for the session.
**"The integrity of an organization starts with the CEO,"** concluded Sullivan.
During his panel discussion, **"Life After the Breach: A Survivor's Guide,"** Tim Crothers, Director, Office of the CISO, Retail Sector, Google, advocated for the need for corporations to do wargames and other tabletop exercises to prepare for an incident. "If you are a CISO, general counsel should be your best friend – [after an incident] first call the general counsel to get it under privilege."

"We have made it impossible for CISOs to win. We need to reframe the discussion, bring in resilience," said Bipul Sinha, CEO of Rubrick, during his session, **"The Human Impact of Cyberattacks: Reframing the Defender Role."**



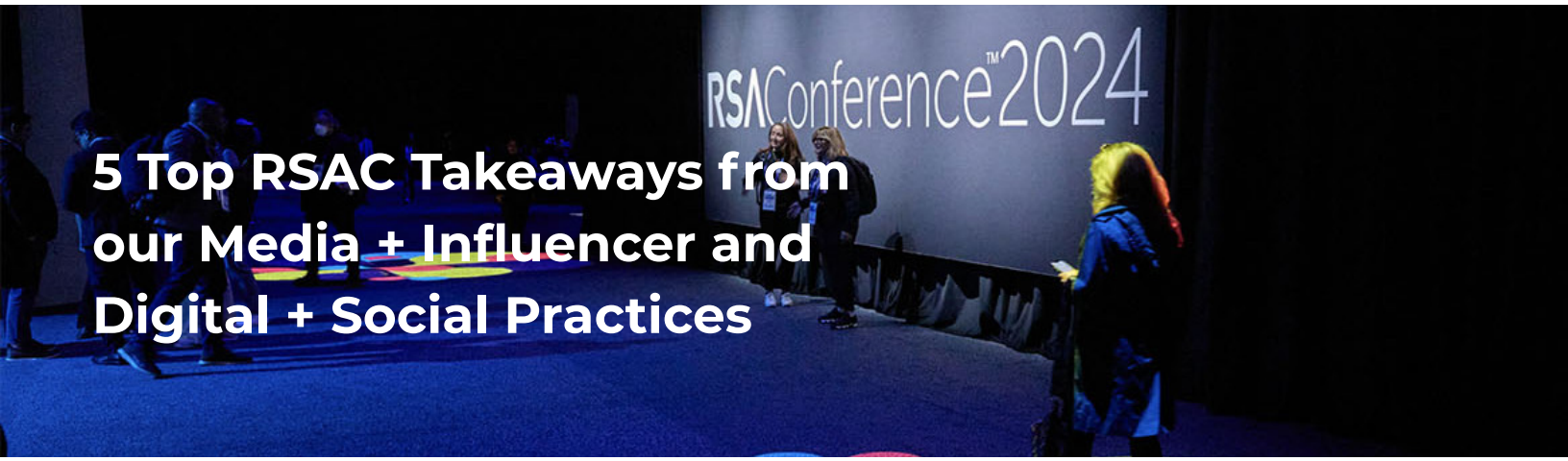
## Beyond script kiddies: Today cybercrime is a multimillion-dollar business

During his talk, **"A New Era of Fraud: What role can cyber play?,"** Rich Agostino, SVP & CISO, Target said, "When we talk about a hacker, people get a specific picture in their head – guy with a hoodie. Over time, the public understands that when we talk about hacking, we are talking about organized groups – they are businesses. Just like we need to think differently about the hacker in the hoodie, we need to think differently about organized retail crime."

In his talk, **"Global Threat Overview,"** Alex Stamos, Chief Trust Officer, SentinelOne, argued that there is currently a nation state "cyber arms race" and that knowledge inevitably leaks out, benefitting other cybercriminals. "The quality of skills of ransomware cybercriminals are as good as Russian and Chinese threat actors." As the criminals have become more sophisticated and better armed, they too have refocused their activities on the most lucrative targets. "Today there is a broad set of industries that are being targeted. In 2005, the Chinese were targeting the defense industrial base, oil and gas, maybe banks. By 2010, we had the Aurora attacks – a state actor is attacking big tech companies, big law firms that have intellectual property. Today financially motivated actors will go after anything. Today local hospitals, school districts are a big target because they have poor security, and they have a huge amount of money backing them."


*"The quality of skills of ransomware cybercriminals are as good as Russian and Chinese threat actors."*

BIG VALLEY MARKETING




# 5 Top RSAC Takeaways from our Media + Influencer and Digital + Social Practices

**Yes, it's about AI, but not just AI.** The cybersecurity media continues to have a strong interest in RSAC yet seems to have a hunger for bigger industry scoops versus traditional product news announcements. AI was a centerpiece in RSAC, of course, but national security, misinformation, nation-state attacks, and emerging technologies like quantum computing and cryptography were also key topics, along with industry collaboration, the central theme of the conference. It was quite commonplace, during a client interview, for the media to say, "Okay, now I'm going to ask you the obligatory AI questions."

**We are continuing to see some media move to paid models.** The strain on media is more evident than ever, with recent layoffs across several media outlets and some outlets shuttering. It appears that more media outlets are turning to a hybrid strategy of paid and earned or paid only at conferences, with an increasing number of paid media opportunities that require a financial commitment upfront. With that, the final product (a piece of coverage) can very often look the same, regardless of how the opportunity was secured. Several clients took full advantage of paid and earned media.

**It's still about the relationship and story (at RSAC and beyond).** With more than 40,000 people in attendance, the show floor felt like it was back to pre-pandemic levels. There was a significant amount of competition for journalists' time and attention. Focusing attention solely on securing an RSAC briefing is a mistake — working the relationship, positioning yourself (and your client) as a resource, and 'matching' the right story with the right journalist is the way to go. We had several journalists set up interviews with our clients after RSAC given time constraints.

**Digestible, informative content trumped all.** Many vendors try to drive as much traffic to their booth as possible with the same social media tactics as everyone else: repeated posts encouraging attendees to come to the booth for [insert surprise here]. At an event as large as RSAC, we see this strategy working less and less every year. Instead, we saw great successes with content that was brief, engaging, and informative. These provided either practical event information (a timelapse video on how to find the booth, for example) or emphasized high-level messaging, like carousels of key session quotes. These posts require little-to-no audience action and little time yet end up encouraging people to stop by the booth to learn more.

**Social doesn't have to be limited to a screen.** At events like RSAC, "surprise and delight" drives the booth strategy (this year included grocery store-themed booths and Warhol paintings), but often stops there. Social media is ripe for both extending and encouraging these interactive experiences. For example, one of our clients coordinated a scavenger hunt throughout Moscone, with clues for each hidden item tweeted out. Anyone who found an item could bring it back to their booth for a free prize – and it worked.

**Want to learn more about how Big Valley Marketing can partner with your company? Feel free to reach out to hireus@bigvalley.co**


## RSA Conference: Coverage Drivers

| | Volume – 2024 | Volume –2023 | Percent of Overall Conversation |
|---|---|---|---|
| **TOTAL** | **122** | **215** | **-** |
| #1 Secure/Security | 108 | 200 | 89% ˉ |
| #2 Threats | 73 | 148 | 60% ˉ |
| #3 Artificial Intelligence | 61 | 120 | 50% ˉ |
| #4 Risks | 59 | 93 | 48% |
| #5 Ransomware | 30 | 41 | 25% |
| #6 Adversaries | 20 | 45 | 16% ˉ |
| #7 National Security | 18 | 19 | 15% |
| #8 Cybercrime | 15 | 19 | 12% |

*Percents may add up to more than 100% because more than one topic can be mentioned in a single article. Percents calculated volume of topic out of the overall search. How to read: arrows indicate in-/decrease YoY from 2023 to 2024. Example: Threats accounted for 60% of the 2024 conversation, down from 2023; cybercrime, despite only accounting for 12% of the overall conversation, increased YoY, which shows that outlets were more interested in covering cybercrime content in association with RSAC 2024.

**Analysis:**
Big Valley's proprietary list of top-tier cybersecurity outlets provided a nuanced perspective into what topics experts deem important. Secure/Security drove the most mentions, outranking both threats and artificial intelligence. Notably, artificial intelligence keyword phrases only accounted for 50% of coverage, demonstrating how top-tier media outlets are moving beyond a strict AI focus within cyber technology discussions.

Compared to last year, expert cybersecurity outlets produced fewer articles overall—a decrease of 43%. According to RSAC, there was a drop in media attendance this year (400 media members vs. 500 media members in 2023). In addition, we saw a high proportion of vendor news was product related, which typically doesn›t get much coverage. Aside from the AI governance discussions at the show, the AI «news» didn›t have a lot of substance -- it is early days on the value -- and risk -- of AI. Outlets focused more on a handful of topics: risks, ransomware, national security and cybercrime. Organizations should keep an eye on the rising interest across these topics to understand how experts perceive their overall impact across the cybersecurity space.

**Methodology:**
Big Valley Marketing utilized its proprietary tool set to analyze RSAC coverage leading up to and following the 2023 and 2024 conferences (April 17 – May 1, 2023, and April 29 – May 13, 2024). Coverage included: traditional (news, blogs, etc.) and social media (X, Reddit, etc.).