

# Insights and Reflections from RSA Conference 2023 that are Shaping the Future in Technology and Cybersecurity

With RSAC 2023 officially in the books, it is time to quickly pause and reflect on what we saw and learned (And we do mean “quickly,” Infosecurity Europe and Black Hat are just around the corner!). Big Valley Marketing represented top-tier cybersecurity clients at the conference, attending sessions, walking the floor, developing blogs, and facilitating media interviews.

From a media perspective, the show brought a level of energy that resembled the final game in a playoff series. If you were a cybersecurity journalist, you were at the show. If you work in the cybersecurity industry, you were at the show. If you were not able to attend, you were online daily, «virtually» at the show. Being at the show, surrounded by 40,000 of our closest friends, put us all in our element.



For the past 4+ years, Big Valley’s Research + Analytics Practice has been tracking the top 200 conversations in technology by breaking down which topics are trending and evolving. When it comes to security related topics, **‘cybersecurity’** has shown continued growth over the past four years and does not show any sign of stopping. This is due in large part to increased ransomware attacks, Russia’s war on Ukraine, the rise of ChatGPT and other topics mentioned below. According to Big Valley’s own research, the term ‘cybersecurity’ registered just shy of 2M mentions in 2022 1.92(M) and Q1 2023 and Q1 2022 by 60% ( 561K vs. 347K).

## One thing RSAC'23 made clear:

Artificial intelligence (AI) is at the top of everyone's mind. Hardly surprising, given the exponential increase in overall media coverage for topics like AI + Security, which has already posted 75% of the story volume seen in 2022. According to our research, Generative AI is a topic that has already produced 50x the mention count from 2022 compared to 2023, and it garnered a ton of attention at the show. We sat in on **"Hype and Reality: How to Evaluate AI/ML in Cybersecurity,"** a session that underscored the growing interest in learning more about the value – and risks – of AI to security operations. BUT, while it is great for brainstorming and research, the consensus is that it is not yet producing accurate, trustworthy results.

As the story goes, this evolution will continue. According to the session, ultimately AI will provide benefits to defenders. Just as the internet was once disruptive, now it is intertwined in everything. The prediction stands that AI too will become part of the fabric of cybersecurity defense.



## Through the Story + Content team's attendance of more than twenty conference sessions, other emergent themes that inspired and informed included the following:



### Diversity and mental health discussions (on- and off-stage):

The theme for this year's event, **"Stronger Together,"** threaded through many of the show's keynotes and sessions, from Claire Malone's inspiring keynote, **"The Universe's Missing Pieces,"** and panel discussion **"Diversity, Equity & Inclusion: The Paradoxical Effect & Impact on Security"** led by Colonel J. Carlos Vega to **"Under Pressure: What Cyber Can Learn from First Responders."** Cydermindz launched at the nearby Contemporary Jewish Museum. The fact that these conversations are taking place more openly is a good start, but there is a lot more work to be done. The good news is that Cybersecurity Staffing Issues/Burnout discussions are becoming more the norm, and in the first few months of 2023 have already reached over 50% of the related story volume we saw in 2022.



### **Innovation is outpacing cybersecurity:**

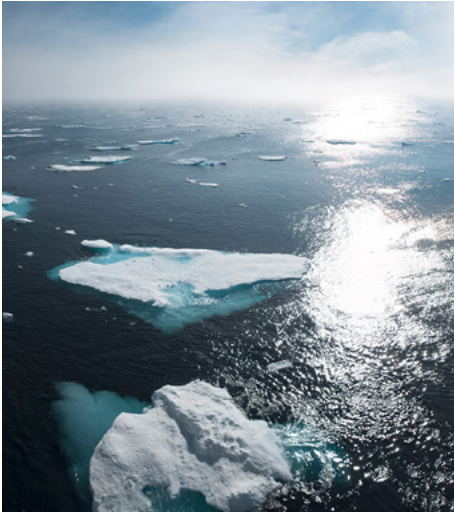
In her keynote, Vasu Jakkal, Corporate Vice President Security, Compliance, Identity, Management & Privacy, Microsoft, shared that industrial revolutions have accelerated the pace of innovation, adding that we are currently living during Industrial Revolution 5.0. “For ChatGPT, it took 3 months to reach 100M users. For mobile phones, it took 16 years to reach 100M users. For the internet, it took 7 years to reach 100M users.”

*“For ChatGPT, it took 3 months to reach 100M users. For mobile phones, it took 16 years to reach 100M users. For the internet, it took 7 years to reach 100M users.”*

### **Big Valley sees this echoed in its own Top Conversations research:**

ChatGPT+ Security had fewer than 300 stories from January 2019 through December 2022. Thus far in 2023? ChatGPT + Security has notched over 6,000 mentions. So, a key learning here is cybersecurity professionals must be ready to evolve -- fast.





### **Climate change is increasing cyber risks: In her session, “The Elephant in the Security Room: Climate Change,”**

Chloe Messdaghi, CEO and Founder, Global Secure Partners stressed that cybersecurity risks will only continue to grow as the world struggles to deal with climate change. The rise of green technologies and emerging technical ecosystems such as EV-connected systems and charging networks expand the attack surface. Climate change may also pressure nation-states to conduct cyberespionage to find solutions. The ripple effect of climate change across all sectors, including cyber, is barely getting attention today, but must be addressed now.

### **Nation state attacks are a pervasive threat:**

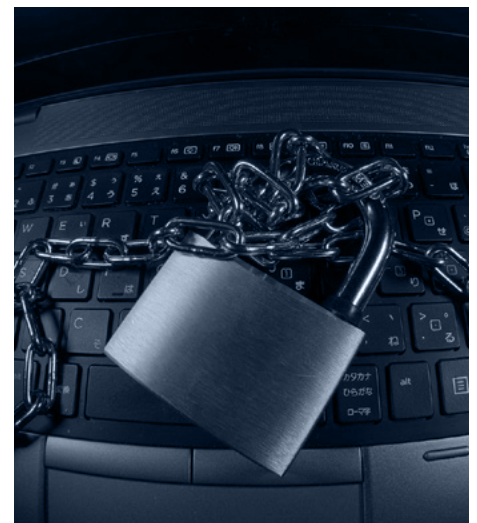
There has been a “huge uptick in intelligence gathering by Russia against Ukraine and its’ allies over the last few months” according to Rob Joyce, Director of Cybersecurity, National Security Agency. “Where is that nation state intelligence gathering being focused on? The logistic chain – we see a lot of activity against the U.S. defense industrial base and logistics companies who are helping to move aid into Ukraine.”

Yet Joyce went on to say, “China is the most active and most persistent espionage threat to the U.S.,” and companies in the pharmaceutical, healthcare, military, and medicine sectors can expect to be challenged by PRC (People’s Republic of China) intrusions. He added that there has been a significant uptick in China’s use of zero days and warned that, “If you are a high-end target for China, you need to start thinking about how to posture for a world of increasing zero days, especially against your edge devices.

*“China is the most active and most persistent espionage threat to the U.S.,” and companies in the pharmaceutical, healthcare, military, and medicine sectors can expect to be challenged by PRC (People’s Republic of China) intrusions.*

### **Tangible gains in collaboration between public and private sectors:**

From “Public-Private Partnerships to Operational Collaboration” and “The Promise and Peril of a UN Cybercrime Treaty” to “Cyber Safety Review Board – Looking Back to Move Forward” and more, the show revealed many tangible proof points that collaboration between the private and public sectors is resulting in measurable and meaningful results in the fight against cybercrime.



**Through our work with our clients and Media + Influencer teammates, we increased this year's media interviews by 100% YoY. After digesting the experience, our key takeaways include:**



**Having deep relationships with the media is foundational to success.** With more than 42,000 people in attendance, there was a significant amount of competition for journalists' time. Journalists were pressed to decide well in advance of the show what stories they wanted to focus on and whom they would need to speak to for each story.



**The line between earned and paid interviews has become increasingly blurry.** As the strain on media outlets has become even greater over the past few years, and with recent layoffs across several media outlets, more media outlets are turning to a hybrid strategy at conferences. While of course there are plenty of opportunities to meet with journalists for straight editorial purposes, there are an increasing number of opportunities that require a financial commitment up front. With that, the final product (a piece of coverage) can very often look the same, regardless of how the opportunity was secured.



**You must be bold to stand out.** With thousands of PR professionals vying for reporters' time and attention, the ability to stand out is key. That means being respectful, while also keeping a watchful eye out for the right opportunity. Sometimes the X factor can be as simple as walking up to a reporter in person, introducing yourself, and striking up an interesting conversation (even at a nearby falafel restaurant).



**Listen, listen, and listen some more.** During the actual interviews, we were reminded of the importance of listening to the flow and rhythm of each interaction. We talked to our clients ahead of time about the importance of staying on message and providing real world examples, not just hypotheticals. And sometimes we get lucky. A spokesperson may say something on a topic relevant to another client that elicits a response from the reporter -- prompting us to pitch the reporter, after the interview of course. This can lead to another interview and a deeper relationship with the reporter. Win-win.

The cybersecurity industry – and the threat and media landscape – is constantly evolving. Big Valley is a dedicated partner who shares continuous insights and analysis with our clients to help them build awareness and stay competitive in a crowded market. Looking ahead to the rest of the summer, there is no rest for the weary. We are already gearing up for Infosecurity Europe, Black Hat and the Aspen Security Summit happening over the next several months.

**Want to learn more about how we can partner with your company?**

Check out our latest video [here](#)

Contact Joshua Swarz at [jswarz@bigvalley.co](mailto:jswarz@bigvalley.co), or Karen Burke at [kburke@bigvalley.co](mailto:kburke@bigvalley.co)

