All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Another day, another RSA

The RSA conference never fails to disappoint – and yet I keep coming back to it.

Maybe it's because I live in the area. I doubt if I would have flown thousands of miles to attend it, but then one of my colleagues flew in from Chicago. It took him about 36 hours total time, cost under $1,000, and I think he got about 4 good and 35 decent leads out of it. Considering what it takes to do sales in this world, that's a pretty good deal.

What did we find?

Here's how I summarized it yesterday at an NSF live online remote (LOR) meeting:

- The talks are mildly interesting, the show floor is fascinating – to me
- There were 623 booths, some with 4+ companies in them
- There were an estimated 50,000 attendees
- The show runs for 3 days (starting on Monday night, ending Thursday afternoon)
- It is always very noisy, non-stop, has no seating, and is underground
- It's at the San Francisco Convention Center, which is a great place for it.
- Companies ranged from from Akamai to Zscaler (A-Z that is)
  - They are of all sizes and types – in cyber security related areas
    - [Hardware, Software, Wetware], [Attack, Defense], [Governance.. Execution], ...
- There were "startups" and the real startups
  - "Startups" were at the "early stage expo" and were/are mostly:
    - Venture backed at $3-10M, which in most cases translates into:
      - Bragging about how much funding they got – lots of ego
      - Telling us, in effect "I'm better than you because I got funded"
  - On the main floor, another 80+ real startups
    - Many are at their first show ever
    - Many are self-funded with only a few people
      - Many come in hope … and leave in despair

What's it all about?

A show like the RSA is about what's popular. It's a marketplace where hundreds of companies compete for the attention of tens of thousands of attendees. As such, it's about getting enough attention to engage some number of potential buyers in what you are selling. "How many?" you might reasonably ask… but first... **What's hot and what's not!**

What’s hot?

These are the “hot button” topics and tag line components from RSA this year:

- **Machine Learning / AI (BS) :**
  - With the emergence of ChatGPT and BARD, AI is all the rage, large language models, and so forth are the added buzz words to let them know you know what they don’t. We call BS largely because adding ChatGPT to a firewall is… just that.
- **Zero Trust (BS):**
  - As I coined the phrase: “Don’t trust zero trust”. The reality is you cannot walk out your front door without trust, or even have a front door. Most identity management firms have added “zero trust” to their market speak, because that’s largely what it’s about. So adding meaningless buzz words being the thing, I call BS on it.
- **SBOM (real):**
  - Software Bill of Materials (SBOM) and related inventory and supply chain issues are real issues that people are just starting to come to as important at large scale, there is a viable technical solution, and as a field, inventory has been here for at least thousands of years. This is a real set of solutions to a real issue.
- **Cloud security (ongoing):**
  - Companies continue to move to the cloud for it’s great cost and performance benefits, the far better physical security, redundancy, and reduction in staff and automation of management and scalability, and … Anything that moves to the cloud that required “security” before requires “security” during and after. So it just makes sense. This is a market that has been here for a while and will continue to be here for a while. It makes sense and is likely a good overall investment area.
- **“Threat” (event) detection [not actors]:**
  - They call it “threat detection” but it’s really almost entirely the use of indicators of compromise (IOCs) in automated detection and response. This is largely the logical result of STIX and TAXII applied to cyber security issues over time, information sharing through what was first called ISACs and then ISAOs, but basically the beginnings of the use of information sharing by defenders and their combined efforts to defend. Over time, the field will likely grow and become much more, but for now, the term “threat” is being misused, as they are ignoring the actual actors that are the actual source of the attacks.
- **Passwordless (eternally trying):**
  - Finally, the eternally trying and never really succeeding field of removing all use of passwords from all systems. Here’s a little secret: “NoWay”. Oops… another great password I can no longer use. Single sign-on was all the rage, but in our little analyst community, we called it reduced sign-on, because it never really should get to “single”. Why is that? Because privilege escalation is required at times, and we don’t really yet even have one identity for each person, and of course we need to identify a lot of things that are not people these days, and and and… It will long be an issue and we will not likely see it resolved during my lifetime.

What's not?

A few years ago, before the pandemic to rolling, there were some hot topics that were all the rage. They have largely disappeared from the marketeering, and for a good reason. Marketing is about reputation and attraction. Security is largely about fear and resolution. Let's look at a few:

- **Blockchain (see distributed database consistency methods):**
    - Blockchain is a fine approach to many classes of distributed ledger. Just as other distributed database consistency methods are. The question is:
        - "Why do I care as a buyer of information technology services?"
    - And the answer is, I don't care. And neither do the customers. Because by now they have figured out that it's just another way of doing distributed database consistency with a different set of technical tradeoffs. I know I will get argument from those who see a political positive in so-called democratization (actually anarchization), but from a standpoint of a commercial customer seeking solutions to commercial security problems in the cyber arena, it just doesn't cut it.
- **Tokenization and cryptocurrency (Ponzi schemes and other frauds):**
    - Why would a security focused person working for a corporation or government want to be associated with the many frauds and Ponzi schemes that have taken place in these areas in the last several years? They would not, the do not, and that's why this is no longer hot. Indeed it may be downright chilly.

A breakthrough in marketing technology

The RSA is one of the best places to test out your new breakthrough in marketing technology. For clarity, I do not mean a {breakthrough in [marketing technology]}, often a good thing in terms of smoothing the path to market efficiency. I mean a {[breakthrough in marketing] technology}, a better way to get people to look at your technology.

Which brings us to…

Generative AI

Of course it does. This year there just wasn't enough time before the RSA to really show off how generative AI could help sell more cyber security stuff. But next year, I expect it will be well embedded to lock your eyes and ears into booths and possibly grab your spirit as well. Here's what I predict as the future of the show floor…

- A flash of light will hit the corner of your eye, forcing your wetware line detection mechanisms to focus your attention on the booth.
- As you react, it will see you turning your eyes toward it, and focusing entirely on you, a voice will come into your head saying, based on your scanned badge information, in the proper accent, language, and expression, just the right words to get you to come over to talk to a person who appears to be dressed and look like the ...

Conclusions

Maybe next year we will get a booth...