All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

The RSA: Science Fiction and Humor

"Welcome back my friends to the show that never ends."[1] The RSA was quite a show this year. It started with William Shatner rapping a version of "Lucy in the Sky with Diamonds" calling out the "girl with the APT eyes" and similar changes reflective of security. It was funny, a great show, and reminiscent of what was to follow.

The next piece of science fiction came from the first real keynote, which started by explaining that RSA was innovative but the government made it too hard to succeed, so they decided to get along to go along, and then they ended up not innovating but following and making a fortune by doing what the NSA said to do via NIST. Now they were somehow claiming innocence because all they did was follow. RSA wasn't a leader, but now, in an attempt to claim to lead, they suggest that NSA only be allowed to do offense and that defense be extracted and placed elsewhere. Yes, they took money and provided what the government wanted to customers around the World, but they were only taking money from the "defense" side of NSA. Some more unworkable notions to get them off the hook, and then when the talk converted to the same old crap, I tuned it out.

The big signs about the show said it was "redefining" things, and that seems consistent with what the show did and does year after year. No real innovation to speak of, but new words to describe the same old fictions. Claims that somehow "big data" would solve our problems (Pay far more for sharing more information with more people to protect your privacy?) were rampant, but with no proof at all. Sharing more data with more people for better security somehow doesn't seem to me to solve anything much, even though I think that some level of information exchange is very important.

What I really think is going on is that (and they admit it) the defense is losing big time. The biggest players in the industry keep failing to protect others and getting hacked themselves. They cannot or will not take the necessary steps to protect themselves, won't recognize the magnitudes of the risks they are aggregating, and can't find ways to make more and more money without putting more people at more risk. So they keep accepting risks they should never accept, reducing costs (if you aren't going to be effective you may as well be less expensive), but increasing services (you have to make money somewhere, so if the costs come down you need to add more things to sell) to generate more income.

And the buyers keep coming because they are more afraid and more desperate than they were last year, because more of them are getting attacked more successfully and with larger consequences. They outsource in the hopes that lower costs and less responsibility will somehow help them, but in fact they get higher costs, more lock-in, and more responsibility.

The fear cycle is in full force at the RSA, and there is little there to really get control over the situation. Many fractional solutions, some suites that are incomplete in their coverage and cover the wrong things, and mostly, hyperbole. Nothing new for the RSA.

---

1 From "Karn Evil 9, 1st Impression Part 2" by Emerson, Lake and Palmer (from ELP's 1973 "Brain Salad Surgery" album) "

On the other hand...

At RSA this year, the security was noticeably – nicer. And I liked it. There is no reason for security to be nasty or inconvenient, and this year for the fist time in a long time, the RSA started to move in the right direction.

Hacking the RSA

This was originally going to be an article titles “Hacking the RSA”. But to my very pleasant surprise, what I originally scoped out was not to be. While there was some fun and game to it, at the end of the day, the RSA came out on top, not because they were ultra secure, but because they were ultra nice. And in my view, niceness with security just makes it all the better.

The booth

Of course if you are going to hack a security conference, you need to have a booth. But to get a booth at RSA for next year, you need to have signed up on the waiting list by Thursday (of this year's show) at 3PM. There is one hour when folks who didn't have booths this year can get one for next year – or at least on the list of companies eligible to do so. Whether you actually get one is another question entirely.

Of course we got one, but not in the usual manner. Rather, we showed up with some rapid deployment roll-up posters (6' high nicely printed with the FearlessSecurity name and reasonably useful information with nice graphics). We identified a booth where the owners hadn't shown yet, took a seat at the table and chairs, set up the posters, and took possession.

The scanner

Next, we wanted to get a scanner so we could scan badges of participants as they walked by, and so we could scan back anyone at a booth who wanted to scan us. This was not cheap, but we told them whatever they wanted to hear, and we got the badge scanner. It requires a credit card and the booth number, which I gladly provided for the booth we were squatting in. This may have triggered the issues that followed, but one way or another, we proceeded.

Being friendly

At the booth, we were basically very friendly toward anyone who stopped by. Welcoming them to have a seat and chat, not standing out front or being pushy in any way, being helpful to folks around us in other booths, etc. Folks we knew stopped by and we said hello, chatting with them. We did an interview with a media person, handed out cards, scanned folks who came by (if they wanted to be scanned), etc.

One of the experiences that is unique to sitting in a booth all day is that you get a real sense of what booth folks experience on a day-to-day basis. At the RSA, plenty of folks walk around in a sort of daze. We asked some of them to come have a seat and chat if they liked, and they told us various reasons for their daze. Too much stuff to see, exhaustion from the night before, too many meetings, and so forth. And it gave me more empathy for booth folk.

What happened next?

Of course we were eventually discovered. Around 1600 on the first day of the show, I was visited at the booth by a gentleman who asked if I was from FearlessSecurity, to which I answered yes, introduced my self, and asked him to have a seat and join me. He very politely

explained that he was from the show and indicated a discrepancy between the name of FearlessSecurity and the name of the folks who rented the space. I explained that we had gotten their permission to use the booth, and he explained that it wasn't his call, asking me to join him in visiting his boss. I happily complied, asked and sent an email to my partner in the adventure that I was heading back there to let him know and so he could return to the booth while I was away, and want back to see the show runner.

The show runner was also very nice. We have a brief and friendly discussion, he indicated that even though I had permission from the folks who paid for the booth, the contract prohibited use by anyone under another name, and that they couldn't give me permission to violate the contract (he wasn't legalistic in any way, just reasonable and friendly about it). I indicated that I understood and would move, then asked if I could pay for the booth and remain for the rest of the show, to which he indicate it was already paid for, and that I could not pay for it. I asked if I could remain for the rest of the day, and he said that would be fine! Talk about being very nice about it, this is outstanding. I wasn't escorted our or anything like that, they didn't take names and inspect badges, etc. and I wasn't even showing my official show badge, but rather a cobbled together one that looked something like a show badge.

In summary, they were very nice and easy to deal with, completely reasonable in every way, and I compliment them on it.

Doing it safely

We are not here to get people, we are here to learn. When we hack the RSA, we do no harm, take nothing from anyone, don't name names, and never lie. It's part of our standard approach for such things. It keeps us safe and makes it reasonable for the places we go. In this case, as always, we wanted to make sure we were legal. So we (1) got permission from the folks who actually paid for the booth and didn't show at the show, (2) made sure we didn't do anything not technically allowable under the conference rules, (3) didn't break any laws, and (4) were nice about it in every way.

We didn't kick anyone out of the booth, we only invited folks to have a seat at the table intended for having a seat. We were legally and contractually allowed to be where we were all the time, as we had legitimate press passes, and were only present at times authorized for folks with those badges. The posters we brought in didn't consume any power, connect to anything, or otherwise create a hazard. We simply set them up behind us and sat in front of them. It's sort of like setting up your brief case with a sign on it.

Don't push your luck

We had made plans for different things on the next 2 days. One day we were going to give away a chrome-book for one lucky winner who had their badge scanned. Another day were were going to go with chocolates. This to see how badge scanning related to exchanges. But we decided not to try the next day after the show folks were so polite and pleasant to us, and of course, we indicated we would stop, and didn't want to go back on our word. We advise others to always be polite and nice in such things, as in our experience it works better.

The remainder of the show was spent actually trying to get business done, asking about ridiculous claims made by booth marketing, and occasionally learning something new (although not about security). I do think that everyone who attends such a show should spend a few hours manning a booth... it's good for you.

Other observations

We did observe some other things along the way, and I thought they might be worth sharing.

- **Scanning and numbers:** A booth can scan from 10 to 300 badges in a day. More scans come from give-aways, as does apparent booth presence. On the other hand, more scans may not lead to more customers. But still, more scans means more opportunities for follow-up.
- **Scanning away from the booth:** On days 2 and 3, we used the badge scanner to scan anyone who wanted to scan us, and to scan friends as we chatted – just for fun. We also used it to scan the FBI agent at the FBI booth, where they weren't scanning anyone. Some of the FBI folks didn't want to be scanned – interesting. In any case, folks were surprised but not offended by the notion that scanning me meant scanning them.
- **Booth folks need nice people to chat with:** People who work in booths are all kinds of folks with all kinds of knowledge and backgrounds. I met a “booth babe” (female, good looking, dressed provocatively, hired to look nice in the booth and bring people over to the sales staff) who has a BS in Electrical Engineering and decided to go into film. She works in a booth for a few days a week for the money, is very nice, and very smart. I met a woman who works for a large consumer company who was exhausted and looked very unhappy, but after we chatted, she perked up and was on about her day. I met a “booth boy” (like a booth babe but male) who was very knowledgeable about issues but not allowed to represent the company for sales purposes. All in all, forgetting that they are there to sell you something and spending a few minutes with them, these are nice folks and good to get to know.
- **Folks at a show are stressed:** Whether happy, sad, tired, or mad, folks at the RSA are stressed. There is too much information hitting them, too much noise, to many crowds, and not enough easy quiet time. While lots of deals are made or started, by Thursday they should have stretchers for the people working there. And in many cases, a few kind words makes them far happier and less stressed. I think the show should hire professional therapists just to chat with folks and be nice to them for a few minutes when they look out of sorts, add more couches and chairs so folks can sit for a bit, and reduce sound levels across the board. But then what do I know?

I presume that these are not surprises, but they are observations. There is something brutal about the sales process, and make no mistake about it, the RSA conference is a sales venue. Very little new information is passed along, but you do get to see old friends and make new ones in the industry. The themes are formulated to find new ways to sell to people, the entertainment is pretty interesting, there are plenty of parties of all sorts to go to, there are many speakers who know a lot even though they tend to reject many excellent speakers and ask others to speak twice (something about their company sponsoring the events – pay to play), and like I said, it is a sales venue. Money talks.

They added a whole new floor of booths this year, likely doubling the income from the show, and still sold out the booths during last years' show, just as they sold out the booths for next year before the show ended this year. It's about selling security, and that's what they do and why so many vendors come.

Some other items

The folks at RSA have been more or less friendly over the years in terms of so-called security. This year they were far more reasonable than they have been. For example, wireless access no longer required going to a booth and requesting a user ID and password by showing a government ID along with your badge, which already required a government ID. You simply had to enter a name and check the browser box agreeing to whatever terms they had. It worked better and the good will was worth whatever perceived security difference it made.

The folks at entries were polite in their refusals to allow entry, and they decided that mandatory scanning of badges was no longer to be enforced. This meant that we didn't fee like cattle when entering venues, and frankly, this was a big plus. I think it has to do with the push back by society against surveillance. But in any case, they were nicer about the whole thing, and that is a good thing. And nothing happened that would cause me to believe that this produced any losses or other enhancement of threats, loss of revenue, or anything else negative.

I'm sure folks could have tailgated in through some entrances, and in San Francisco, that means a free meal or two for street people. But if you don't look the part, you won't likely get through, even though plenty of RSA attendees still come in jeans. And that means that however many may have done it or tried and failed, there was no substantial effect.

The show has a lot of workers. There are 3 or so per talk just to welcome (screen) guests, and there are 20 or so simultaneous activities at most all times. The workers I encountered were all polite and friendly, and this is an improvement over past years in my experience.

The invited speakers includes Bill Shatner (a surprise to open the show) and Steven Colbert (who closed the show). They were both great – people who both know how to laugh at themselves and how to be serious when called for. They were funny and fun, and most of all entertaining. Like I said – it was a show, and a very good one at the end of the day.

If the RSA keeps this up, they will perhaps even go back to their roots and start adding some meaningful technical content. It seems unlikely that they will host controversy, but what can you expect from a company that has gone ultra-conservative after its founders started out by ending up in the Supreme court over their cryptographic system being exported. On the other hand, maybe they will decide to also be the best technical conference, which they could succeed at, if they tried. But don't hold your breath. There was nothing new at RSA this year from a security standpoint, other than an improvement in their friendliness perspective.

Summary

Being nice about “security” issues is better. And the RSA did better this year than they have in the past. Whether it is because of media fears, push back from attendees, or a realization that they were just being oppressive, they were nicer, and they deserve some positive feedback from this.

While there is still a long way to go, the move toward Reasonable Security Again is a good thing in my view, and they should keep on going. Whatever is lost, more is gained by being reasonable, polite, nice, and friendly. Keep up that part of it RSA.

“Come and see the show...”[2]

2 ELP... I.b.i.d.

