martinwolf

Executive Perspective®

Unique Viewpoints from Industry Leaders

April 2018

Ben Eazzetta

CEO, ARES Security Corporation

***Editor's Note:** To celebrate the 50th issue of Executive Perspective, we've invited back Ben Eazzetta, our very first interviewee, to discuss the developments in his career and his thoughts on the IT industry. After leaving his position as President of Rolta International, Ben served as Interim CEO of Confluence Security Group and currently serves as CEO of ARES Security Corporation, where he has been leading for the past five years. In addition to delivering its proprietary AVERT solution to government clients, ASC provides advanced situational awareness solutions to ports, transportation, and corporate security and delivers solutions against homeland security and business continuity threats.*

We first talked to you in the second quarter of 2012. Before we talk about how the IT industry has grown and evolved during that time, how has Ben Eazzetta grown and evolved?

I went back and worked on a startup, which I hadn't done in a number of years. I always found startups are particularly challenging. This one is in an interesting space: physical security assessment. Basically, we do virtual models of high-end facilities and model them against terrorist threats. We have another product line that does situational awareness.

It has been a lot of fun because I got back into a market I really enjoyed, public safety and security. But starting a business and being able to grow it from basically zero market share is always a challenge.

I've learned a lot from that perspective and am now getting exposed to more about artificial intelligence, which is the direction we're taking the company. We are working on "Advanced Security and Combat Analytics" using AI.

Let's talk a bit more about your role at ARES. In light of the physical security market, what does a typical engagement look like for you?

We have about 65 percent market share in the North American commercial nuclear market. Our primary clients right now are nuclear facilities, and they use our products to assess their security

to make sure it's adequate as well as to look at how they can reduce security cost, add capital or do things of that nature.
We also are now doing work in transportation, doing more work for two of the largest transit authorities in the US. We're also starting to do work in critical infrastructure, or corporate security. We are looking to be able to quickly assess active shooter, like how the incident in Las Vegas could have been modeled ahead of time to improve security and hopefully prevent this terrible act.

Clearly, what we're finding is a lot of people are increasing security in the venues themselves, like at a stadium or a concert. But they're not looking at the holistic approach of what security should be. For instance, in the bombings in Birmingham, they went into a concert. The concert had metal detectors and were searching bags, so the bomber took his vest in an area that was a connection between the underground transit system and the venue for the concert. There are plenty of people who go into the concert from there. Security wasn't from a holistic approach, seeing all the flow of people or things of that nature. So that's what our tool does; it allows for that broader assessment.

"They are not looking at the holistic approach of what security should be."

Compared to the past, would you say we need more security today?

From a physical security threat standpoint, I think people haven't really understood how to protect themselves against even the most basic threats, especially in our country. We have an open infrastructure. An active shooter could walk into any shopping mall, hotel, or corporate building and have his way. There have been over 750 active shooter deaths in the past year.

I think what we're going to see in the next few years are people getting more serious about protecting against this. We're going to see mobile-born improvised explosive devices and personal devices being used more often. People are going to get more savvy about how they're going to deal with these kinds of threats. Overall, I think there will be a lot more happening in the physical security space.

As for cybersecurity, the threats are continuing to grow. We're having a lot of folks out there now doing ransomware. There was a recent attack on the city of Atlanta that cost several million dollars. They had to get it all off and recover all their data. Even high tech companies are being attacked because there's a desire to download IP, steal designs or try to hold their capabilities or database as hostage.

I think even on the high-end facilities, although a lot of them are regulated and they protect against a "regulated design-based threat," many of them know true attacks on infrastructure will be preceded by a cyber attack. Our software can assess the impact of a positive cyber attack, so we can assess scenarios like cameras being spoofed, partial system shutdowns, doors being locked open and doors lock closed. We can model all of these.

Is your software fully transitioning to SaaS from on-prem?

We do both on-prem and SaaS. For nuclear facilities, because they're all in a highly secure environment, they have to have their own server. In fact, the server fits in a safe. The data that's on that server is what they call SGI; it's very secure data. It's not quite top secret, but it's like that kind of information. So all of that information sits in separate systems.

"Cybersecurity for critical infrastructure is going to be more of a topic."

But as we're also dealing with customers that have 30+ office locations, new building and venue design and are not in the nuclear space or regulated by the federal government, we are offering the tool in a SaaS environment.

We are working on a project now to offer our situational awareness product as a SaaS offering in all the ports in the state of Florida. We won that project in January and are implementing that now across all Florida ports.

I believe you're going to see more security as a service.

Let's detour back to where we started in the IT industry. Six years ago, we asked you what you thought were the three biggest trends affecting IT. You mentioned business development, big data and software/cloud services. What would you say are the three biggest trends today?

What I would say is, cybersecurity for critical infrastructure is going to be more of a topic. I think that's going to be a trend. It's a big trend already, but it's going to become even bigger because there are a lot of very large governments around the world that are doing some bad things. I don't see that stopping. I think cybersecurity will become a bigger component and find itself with more regulations, especially in the critical infrastructure space to protect our infrastructure.

I also think cloud computing will continue.

Big data, in my view, will see development of AI or deep learning applications. Now we're going to take that big data and begin to do deep learning. And I think that's going to be something that will be more prominent in the next five to seven years. We'll begin to see more applications that are getting access to vast amounts of data that were created and will continue to be created. We will be able to do fantastic and interesting things with that data.

Let's talk specifically about the rise of cloud. Is it fair to say it has even more potential than previously realized?

I think so. We're seeing companies like Alibaba growing at 100 percent year-over-year in their datacenters or their cloud computing capabiliites. It's already a $700 million business, and it was nothing two years ago. It has become very expansive. I think you're going to see more things moving to the cloud.

In the absence of a highly secure environment, I think you'll continue to see that the cloud aspects are continuing to grow.

"I think there's going to be a wave of innovation around the efficiency of datacenters."

Looking at the cloud landscape today, are there lower barriers to entry? Or do you think it has solidified certain giants, like Amazon or Microsoft, in their market dominance?

I'm not saying there's no room for anybody else. From what I've been exposed to, I think there's going to be a wave of innovation around the efficiency of datacenters. They consume a lot of power and I think you're going to begin to see companies that come up offering a lot of the infrastructure for cloud that are very efficient. Perhaps somebody else, a startup, will challenge some of these other companies because of their efficiency. I think a lot of the original datacenters are not as efficient as the newer ones or the modular ones built in the locations they were in.

Another thing I think we'll see is, if you look at a map of the US and where the bandwidth is, a lot of the bandwidth is in key areas. I think you're going to begin to see a growth in rural cloud capability and datacenters. You're going to begin to see remote datacenters pop up in areas where the connectivity tends to be at the end of the line. Quite literally, you can see a lot of these rural areas have smaller modular datacenters. Maybe local businessmen or local utilities make complete sense to tie into a transmission substation or into some other type of facility. So overall, I think you'll see more rural datacenters, not just in the big urban areas.

How do you weigh the increasing role of big data against the invasion of privacy for consumers?

There's a definite conflict. It's going to become worse and more invasive. People are going to be very surprised at the amount of data that these applications have access to. Some of these voice activated systems can be used to collect a very significant amount of personal data about people that they didn't use it for. The goal could be for commerce but it can have many other applications.

I think what happened to Facebook you'll find more in other places, but also it provides the unique opportunity in the policing area too. Perhaps there will be a good way to track some of the bad people too. We can mine some of those trends across multiple networks and see things today, especially some potential AI deep learning applications that will see trends we were never able to find before. It can add a lot of safety in some areas, but privacy is going to become more of an issue. Facebook is not the last one.

“Privacy is going to become more of an issue.”

How would you rate the economy today vis-à-vis market opportunity for IT companies?

To me, it seems the economy is good. There’s a lot of investment happening and more competition in certain places. A number of years ago, business analytics was just getting started. Even in cloud computing, there was a lot on hardware that were opportunities. There’s already a good amount of competition in IT areas, but as economies are continung to expand and people are spending money, there are great opportunities for IT. As we begin to push more of IT into the whole, it will spur more IT growth in the application area, such as various applications from Amazon or Apple.

What would you say about the ERP space today?

I think it's going to be in the cloud, whether it's private cloud or public. A company is large enough to have its own, but most of the applications are going to run in to the cloud. I think it opens up a lot of markets because there were a lot of mid-size and small companies in the ERP system.

Will there always be a role for on-prem software or do you see the shift to cloud as permanent?

I think there are certain applications, like security for the Department of Defense or the Department of Energy, that are highly secure. If they move to cloud it will be very secure. I think you'll find that there will always be some on-prem, but there will be more SaaS-based applications and more software operating in ways that people can buy to allow them to revenue share that make more sense. People starting platform companies now have to be a lot more innovative than they were 20 years ago when everything was either seed-based or licensed by the machine.

Is M&A more or less significant in securing growth today?

I think M&A is always going to be critical. In a good economy, it's probably even more critical. When the economy is down, people look at consolidation but are not actively looking to grow. But now, people want to grow and there are a lot of new areas, like deep learning and data analytics, that companies will begin to pick up capablility in. They will find they need them. Maybe the install dates are ready but they don't have that expertise, so they will look to M&A. I think we'll see the M&A trends continue, and if the results are good, it will be a bigger component.

"Don't be afraid to take a bigger risk."

What advice would you share with six-years-younger Ben Eazzetta?

I would say, "Don't be afraid to take a bigger risk." I think that the path of growth is often not one that is safe. You're not going to find a safe path sometimes. You're going to have take chances, reach out to your community and customers you're serving, and you'll find some people that are willing to take risks with you. I learned that you can grow a company, work with a client base and find new growth initiatives, but take a risk don't look back. Just go forward. That's what I would say.