ceocfointerviews.com

Issue: November 29, 2021

AIT Engineering – providing Cybersecurity Services to the Department of Defense in support of Training Systems

Jason Eddy
President

AIT Engineering
https://www.aitengineering.com/

Contact:
Jason Eddy
407-601-7148
Jason.Eddy@AITEngineering.com

Interview conducted by:
Lynn Fosse, Senior Editor, CEOCFO Magazine

CEOCFO: ***Mr. Eddy, what is AIT Engineering?***
Mr. Eddy: AIT Engineering is an engineering services company primarily focused on the cybersecurity services for the Department of Defense and everything related to cybersecurity. These unique services include information technology, software engineering, logistics, and everything required to support to DOD training systems.

CEOCFO: ***Was it a deliberate intention to work so heavily with the DOD or was it more opportunistic?***
Mr. Eddy: A little of both. Prior to AIT, I had a decade of supporting the DOD, so it's where I was comfortable. I used my experience and expertise to look for opportunities that I felt comfortable taking on. I think naturally the intersection between my background and industry needs aligned in the DOD space.

CEOCFO: ***What types of projects might you work on typically?***
Mr. Eddy: Typically, we are handling the cybersecurity for Department of Defense systems where we basically do all the things ranging from system hardening to monitoring and security compliance where we make sure to keep the bad guys out.

CEOCFO: ***Are there different segments of the department that are your clients?***
Mr. Eddy: We typically work mostly with the Army and a little bit with the Navy and Marine Corp. In most cases we are supporting the training systems sectors.

CEOCFO: ***What do you understand about cybersecurity that less experienced people do not recognize is important?***
Mr. Eddy: Our approach for cybersecurity is all about risk management. Lots of folks in the cybersecurity space tend to want to have an all-or-nothing approach. This approach is typically successful on the cybersecurity side of things, but at the detriment of systems functionality and performance.

Our role is to come in and help find the balance between just enough security to keep the bad guys out yet allows the systems to continue to perform and conduct the mission. Finding that sweet spot between totally security compliant and remaining completely functional is what we do.

CEOCFO: ***Would you give us an example of where the give and take would be and where you might say we can do a little bit more or less depending on the risk?***
Mr. Eddy: A good example is, in a traditional training system we often put layers of network defense between the training systems and where any of the adversaries could access the systems. This gives us a little more leeway when it comes to things like frequency of security patches. In a modern directly connected internet system, we are applying security updates sometimes hourly as the as the threats are divulged. In the case of our training systems, we can't really do that in the middle of an exercise.

So instead of applying updates on the hourly or daily basis, we spend time to build extra network protections or firewalls so that we can safely extend the cycle out to a monthly or quarterly basis, yet still not create attack factors for any of our adversaries.

CEOCFO: ***Do you typically setup a project for one-time or continue on an ongoing basis on the various projects?***
Mr. Eddy: It depends on the project. Some projects we are there from the inception where we design it, we procure and build it, and then make it operational. At this point, we typically transition the sustainment to another organization to keep it running. However, in the past couple of years we are seeing a trend where customers are asking us to maintain control and monitor the systems continuously on a 24/7 basis throughout its lifecycle, sometimes years.

"We can never fully prevent anything, but in our world, they key is how we minimize the exposure when it happens. We assume bad things are going to happen so we focus on how we can make the impact as small as possible." Jason Eddy

CEOCFO: ***I see on your site a little section about security engineering and that it is a specialized field of engineering, do most people even know that or do people find when they see that is the way you are going, that it makes a difference?***
Mr. Eddy: I think anyone that is in the DOD space knows that it's a critical specialty to make sure that when a system is built, the design takes into account the end state and sustainment needs of the system to keep it securely operational. Doing this security engineering early in the process makes sure that we do not build a system and make it operational only to realize that it cannot maintain proper security hygiene and then have to go back and redesign the system.

These are the kind of costly mistakes that organizations would typically only make once, so including security engineering up front is where we come in and not wait till the end when it's too late.

CEOCFO: ***What about threats that seem to be constant and ever-changing and ever more powerful? How do you stay on top of what is going on and as you are constructing a solution what do you do about unforeseen circumstances coming down the pike?***
Mr. Eddy: There is the science and regulatory part of our jobs that we have to do, but knowing what's coming next, that is the art and kind of where some of our special sauce is. We never truly know what is coming next, but what we do know is how to contain them. We use some trusted principles such as the term least privileged in our world. It simply means only granting a user the minimum access rights they need so that if something were to be compromised the exposure is as minimal as possible.

In addition to limiting exposure, we also make sure that we have alerts and audits to notify us as soon as something happens in order to contain it as quickly as possible. We can never fully prevent anything, but in our world, they key is how we minimize the exposure when it happens. We assume bad things are going to happen so we focus on how we can make the impact as small as possible.

CEOCFO: ***Do people at the DOD understand on a deeper level than perhaps the average person, that they need to be careful and pay attention to phishing and rid of credentials when someone leaves the organization?***

Mr. Eddy: I would say that over the past five years there has been a drastic improvement in awareness within the DOD, commercial and medical sectors. We are seeing a lot more awareness campaigns from our clients, so I believe that most people know what phishing is now.

Most companies require annual training to at least create some awareness and maybe make people take pause for just a few seconds before they click on that link that says they have an ancestor that left them something or they have an Amazon order that is pending asking them to enter their social security number and credit card number to verify.

Even if it makes people pause for a second or two, that is usually enough to prevent that intuitive click that oftentimes is too late after they click.

CEOCFO: ***One of the things I see on your site is that you provide low-cost, common sense based approaches. How are you able to keep your cost in-check?***
Mr. Eddy: A lot of it is that there are thousands of companies out there selling security solutions with what they call turnkey security protection. A lot of organizations believe these are the silver bullet that can solve all their problems. In reality, they are very expensive and complicated, and more importantly once they are fully immersed, they realize they have a complicated set of very expensive things to maintain. We approach customer engagements a little bit differently where we do not immediately go to those shiny objects with the products and the companies, we take a step back and ask ourselves what the system needs.

In cases where large organizations say they need multifactor authentication with complex systems to maintain, our approach is to ask them what are we trying to protect and can we just maybe limit number of people that have access or can we place these assets on a network segment that is not accessible to the bad guys. Oftentimes using these type of approaches allows us to not need to incur all the costs with the latest state-of-the-art cybersecurity systems. We like the low-tech solutions because there is nothing more secure than just not giving someone access. We tend to take this approach instead of a fancy new proactive technology that oftentimes still creates an attack factor that we would prefer just to eliminate.

CEOCFO: ***What types of projects do you go after; is there something about a particular project that makes it appealing to you?***
Mr. Eddy: We go after two types of projects. One is what we have a great reputation for with a history of proven solutions and successful methodologies. We always go after those in our strength zone as what our reputation is built on. At the same time, we have a bunch of very smart and talented engineers that can get a little stagnant and bored.

For every two of our standards systems that we go after, we try to go after a new and emerging area to keep our people fresh, relevant, and excited about new technologies. It is a two-thirds split, we take two-thirds in our power zone and about one-third to diversify the portfolio and create some tangent markets to keep our engineers excited about coming to work.

CEOCFO: ***What has changed in your approach over time and what have you learned as AIT Engineering has grown and evolved?***
Mr. Eddy: What we have learned over time is that past precedent tends to be the most significant indication of success in the cybersecurity regulatory space. What I mean by that is there is a mountain of regulations and requirements that are written to define what right looks like. What works for one system's interpretation of policy, might not work well from a compliance posture for the next system.

What we learned was to take all of the requirements and regulations as written, then really look back at what worked last month or week and see how we can leverage that proven combination of policies and technologies to make up good cybersecurity. We use that pattern for new systems and is our guiding principle of basically the concept of do not reinvent the wheel.

CEOCFO: ***What have you learned from your military experience about how to run a business and perhaps how not to run a business?***

Mr. Eddy: From how to run a business, probably the biggest thing that I picked up in the military is about culture. Just like the military, we built AIT into a company with groups of like-minded folks having a common goal. We have tried to assemble teams that work together with lots of comradery and the same team-building experiences. We try to bring the team together and make them trust one another to build an organization much like the military here. It is one of the things we get constant feedback that AIT feels like a family and everyone trusts each other to accomplish the mission.

CEOCFO: ***With so many companies to look at, why choose AIT Engineering?***

Mr. Eddy: First is our people. Our engineers are absolutely the best at what they do and we would not be here without them. I think our secret sauce is about creating communication. Our automation frameworks allow all of these smart people to share their recipes for success with their peers within the company so we can reuse all the successes across the teams.

It is not very often that the smartest guy in the room does not want to continue to be the smartest guy. Why we are a little different is that we try to convince the smart guys to bring everyone else up to their level and share all of that knowledge to create an organization where the sum of our parts gets something greater than the whole.