Information Sharing and Analysis Organization (ISAO)
Standards Organization (SO) Public Meeting
LMI Headquarters

7940 Jones Branch Drive, Tysons, VA 22102
November 9th 2015, 7:30 a.m. – 5:00 p.m.

Perspectives from the Front Line

HEIDI GRAHAM: Our next speaker is Mr. Brian Engle. He is the Executive Director of the Retail Cyber Intelligence Sharing Center. Prior to his service as Executive Director, Mr. Engle has served in information security roles in the past for the state of Texas and in the private sector. Ladies and gentlemen, please welcome Mr. Brian Engle.

[Applause.]

BRIAN ENGLE: Thank you. Good morning. I did not get to preface the "brief" part, but she's bright, she's sharp, and she picks up on that and I'm glad that she kept that very brief. As was mentioned, I am the Executive Director of the Retail Cyber Intelligence Sharing Center, or R-CISC, and that is a pretty newly formed ISAC. It positions us with a degree of perspective, but today I wanted to just sort of share and reemphasize why the perspectives of each of you are so important by just giving a few examples of the perspective that the R-CISC and myself bring to bear on this project.

Very briefly, the R-CISC was formed in April of 2014 through incorporation, but became operationally capable, essentially, in February of this year. In that time frame, we've grown pretty rapidly, but what we're seeing is that our growth is in a space that is not as defined as critical infrastructure sectors might wish that to have. So in that, we have a bit of a perspective on how an ecosystem and a business-oriented approach to information sharing create some of these nuances that I think will be very, very important to consider when we start to consider what ISAOs can do.

But at the same time, when we think of retail as a sub-sector component of a critical infrastructure sector, it's critical. It's critical to our lifestyle, it's critical to our economic viability and structure across the Nation and the world. Beyond that, most of my perspective then comes from being a CISO more than trying to head up an information sharing organization.

In that, one of the things I've come to realize is that information sharing is more important across so many different levels than intelligence and tactical intel. Its formative need is really well rendered in what we're doing even with the forming of a ISAO standards organization. The input at the beginning, the ability to come together and share information at the start of something is so critical and it's one of the types of things that many organizations are faced with is how to share information in the forming stages rather than in an evolving state. This sharing includes strategic decision-type things as well as tactical indications of attack and otherwise. So, that bias that I have comes from not just being part of an ISAC but also coming from the place where, as a CISO, there are many questions that you need answered along the way of the formation of a security program.

My passion, much like Mike Echols', is that I think that this is critical. The ability for us to be able to share information to enable security programs to be capable of protecting themselves is just absolutely critical and essential. And the types of things that are needed are the areas of benchmarking, the types of things that are needed to get programs evolved and to mature and to get to the place where the force multiplication factors that enable us to protect at a rapid rate are essential.

Speaking of essential. . . . So, one of the things that I think has become sort of a mindset of many organizations is that they will build information sharing in once they are capable. So they'll develop and get to the place that they will have a story to tell and information to share rather than building it in at the beginning. I would compare this to the sort of age-old principle of, "You build something and then you secure it at the tail end". I think it needs to be flipped around and absolutely has to include information sharing at the onset and the concepts of how to share that information at the building stages. So, the fundamental and essential steps should not be an evolution or a maturity or the type of thing that occurs over time. If you think of a sort of Maslow's Hierarchy of Needs, where you would reach a capable state and then be in a give-back and sharing state. We need to pull that down into the fundamental and essential level of building programs. If you think of that, and you think of the types of organizations that are out there, at all varying degrees of maturity at their start. How do you get information sharing into a capable state at the beginning? And that's going to be our challenge. That's where these perspectives, I think, are so important to be able to look at the history of how some of the ISACs were formed and how they got to the place where they were able to share at the rate that they are now, means that we have to be able to give that capability to organizations that may not be able to deal with tactical intel on Day One. That means helping to build their capabilities at the onset. These standards need to be inclusive of organizations of many different types, many different sizes, many different levels of maturity. We would like to see them grow through capabilities. We want those to be a stair-step approach—that organizations entering at the onset are building towards that very highly tactical and capable level.

We know that the hurdles are significant and many of these obstacles are based upon the types of things where we've seen sharing struggles occur in the past. So we have a rare opportunity to really break down some of those obstacles and do so in a short period of time and make this an effort that is capable of supporting organizations today. I think that's important because sharing is occurring and it's occurring all over the place and there are many organizations that are building and trying to get capable. So, our ability to bring in standards that help develop that capability to the end goal is just super important.

One of the things that I think that we have to be cognizant of is that we cannot just simply hand the tools that we've used for the places that we're at (or that we've gotten to) carte blanche. We just can't give the toolbox to an organization that is trying to develop. We have to enable them to get to that place of being able to use the various different tools that we have in place.

One of the things that we find is the aspect of actionable intelligence. Building a capability of being able to do something means resources. It means applying skills and a lot of those skills are in short supply and high demand. So, we have to consider how to enable those types of sharing capabilities into organizations that are going to have varying opinions on what they consider to be actionable.

The story of context is one of the greatest things that we have to try to do in the building of sharing of intelligence. The quality of intelligence is really highly subjective based upon your capabilities, and a highly capable organization is always going to be able to look at even raw data and say 'I can do something with this'. An organization that has a lot less capability needs to have a lot more of that story built around it before it is handed over. Those are some of the struggles we've seen with information sharing.

So we have to think about not just standards of how the organizations will look at varying different tiers, but I think we have a really good opportunity to assemble the types of things to help rapidly enable capability. And those are some of the things that the R-CISC is trying to do internally, and we've become a very good laboratory for the types of things that these standards organization will develop over time. So, we realize that there aren't magic wands and that these things don't happen overnight. And while we're trying to move at a rapid pace, it means that we're really going to have to leverage things that have worked in the past, and perhaps take that same set of tools and modify them or where we need to create new ones, do so. And those types of templates and things are going to be extremely important.

One of the things that I think I've learned is (or I'll say "observed"): we consider the concept of "lessons learned" and oftentimes we don't truly learn those lessons—we just observe. The things that we observe are just as important to share because those are the types of things that will avoid pitfalls for others. When we look at a lesson that we learn, I think that we have some of those to share and we have others that are just too new (in the sense of, "We haven't gotten to the bottom of what those lessons will be.") The key, again, I see as we look across all of the varying types of organizations that are contributing at the onset and will continue throughout this project are just going to be super critical.

So I'm just going to summarize, briefly, to say that if we can step outside of our goldfish bowl and look at things a little bit differently, and look at the outcome that we're trying to achieve, we can start with certain perspectives and if we consider that those perspectives can be shaped, developed, and evolved to meet the needs of the sharing organizations that are coming to play today and that will come along the way throughout this new world of sharing. It's just going to be critical for us to work together and to cultivate those sharing standards. I told Rick I'd make up the time here. I want to thank each of you for your efforts getting us to this place, because many of you have been, basically, in the front line a lot longer than many of the rest of us. We look to you, we look to your experience, and we thank you for your contribution and look forward to working with you going forward. Back on schedule, sir.

[Applause.]