Information Sharing and Analysis Organization (ISAO) Standards Organization (SO) 3rd Public Meeting

Public Comment And Debate: Standards Working Group 3

Speaker: Kent Landfield and Mike Darling, Co-Chairs, SWG3

Kent Landfield, SWG3: Just to set the tone, you probably heard so far both previous discussions of the work in progress have been focused on trying to make sure we state this is truly voluntary. Nothing that is listed in any of the efforts here is prescriptive and that's absolutely a fundamental tenant of what we are trying to accomplish here. The question just a minute ago about sort of directing an ISAO to the next step in maturity is not something that should be up to a group like this; it should be up to the members deciding what they need and taking that to their board of the ISAO to actually get those kinds enhanced services or growth within the organization to provide more value. That's not something that, from our perspective, we are trying to do, to be prescriptive. In working group 3 we sort of have the interesting task of trying to pinpoint useful exchanges of information; where those points are within the process of defending our networks or it's useful for us to get our information or it's useful for us to share information and in what format. This working group has been going through a process of trying to identify what we would consider framework understanding because part of the work we are trying to accomplish here is not just directed at the ISAOs. Information sharing from a lot of the organizations today is a nice hype word, but the reality is you have to have a value for sharing. There has to be a real reason you want to share. What do you get out of that kind of exchange of information between two parties or many, many different parties? The intention here was to try to put together something that not only informed the new ISAOs that we are talking about but to inform those members who may want to join or even consider at some point coming into partnership and doing something for themselves. We see a lot of relationships that exist today that can be very beneficial as an ISAO. From our perspective, we wanted to try to establish conceptual framework that allowed us to go through this process of describing what it is that we are trying to accomplish [Reference to screen]. What we've come up with initially is a context for information sharing. There are really two aspects to this. There is the situation awareness decision making and action process that an organization or an ISAO would want to go through and try to determine whether the information was actually useful and valuable. What the processes are and what they might want to accomplish. Really because we are trying to pinpoint where information is exchanged and the types of things that could be available, it was important to also create the construct levels. The three information construct levels on the right side [Reference to screen] that really describe an immediacy issue. You have a strategic, which is very long range. You have a tactical, which is shorter range, more of applied focus as well as an immediate "I have to respond now, there's something going on". All three of those levels have different points of sharing, different information needs, and they need to be understood by the ISAO as well as the members as to how they could potentially get value out of that and where those sharing points could be. You want to state anything there?

Mike Darling, SWG3: Yeah, I would just say that the example you used yesterday and when digging through immediate, tactical, and strategic and understand that there are a lot of connotations that come with those words depending on what you're background is. The immediate is, often times, you've got a SOC [Security Operations Center] analyst, information is coming in, and you're making decisions whether to block something or that sort of thing. The tactical would be more on a daily basis. We are seeing a lot more activity on an internal application server than we are on the web servers so we are going to move resources to help support that. The strategic would be [that] we see deficiencies in our architectures and we need to think about additional resources to address those based off of the information that we are getting that is informing us about this dynamically evolving environment. Those are really the concepts behind those words and we recognize those words it may not necessarily be the right one but we want to think about how we refine that concept.

Kent Landfield, SWG3: We tied a lot of this together [Reference to screen] from the standpoint of an ISAO action, a member action, trying to, again, identify where the exchange of information is, what occurred, what the value is, and mirroring that with the real focus of that point in time. Next slide. We also came up with a conceptual use model [Reference to screen]. Again, this is to inform so we are using this as a basis to fill out the actual words to describe what it is that an ISAO would have to do in various situations, or have the choice to do, and where information itself may be applied appropriately. What we've come up with here is a conceptual approach to information uses and where that would fit into the same strategic, tactical, and immediate kind of focus. From our perspective, the working group itself has made a lot of progress in trying to develop what it was that, coming from ground zero, we really had no idea how to do this, we definitely had a lot of very qualified people working which is a positive and thank you to the people in the room who are participating in my working group, you are really doing a great job and I really appreciate it. The real focus here is that we need to describe the what, when and where kind of approach to information sharing. We have some overlaps with other working groups. We definitely have an overlap with working group 4 and working group 1. I think in a lot of respects we are just understanding the service offering aspects and that will also be an overlap area and we need to do some additional work with. One of the things that I think we are very focused on trying to accomplish is to create a core. That will allow us to be able to use that across the document and across the other working groups as well so that we can come to that common lexicon of being able to explain this in a consistent, and at least reasonably simple approach to understanding a very complex space.

Mike Darling, SWG3: I think the one thing we want to keep in mind through all of this is that, going back to what Kent said at the beginning, we don't do information sharing just to share information, we do information sharing for a purpose. And that is to improve cyber security organization and inform risk management and that type of thing. With that goal in mind, think about the data, think about how you run it through. We are pretty far down the road, but I think this is a point where getting it right and the refinement of the big colors we have in place right now is very important.

Kent Landfield, SWG3: [Reference to screen] So, I'm going to try to do something a little different. I have some requests of you, before we open it up for questions of us. One of the issues we have been sort of struggling with is to what level do we document certain aspects and one of those is documenting the automated cyber threat intelligence sharing. How much do we go down the path of documenting the various means of doing that and I'd like to ask the audience what you think from the standpoint of where we should be drawing a line. Should we be doing something at a very reasonably high level and pointing references out or should we be doing something where we'd actually be describing capabilities that could be put in place for automated sharing and its various aspects. Not all automated sharing needs STIX and TAXII. That's definitely from a cyber perspective. That's one more thing I didn't want to mention. I'm going to digress just one minute. One of the things that we wanted to make sure that we make clear is that while the EO [Executive Order] was focused on cyber threat intelligence sharing, the reality is information sharing is not only about cyber when it comes to today. We're starting to see a real emergence of cyber physical systems and we believe that in the long run we have to be able to support those in an information sharing aspect because new types of devices are going to be affecting our daily lives. Home automation is already having issues, we are seeing the whole movement toward driverless cars, I would definitely want to know if there are threats towards the highways I'm about to get on and if there is something I can do especially if I'm a manufacture, auto manufacturer or some sort of infrastructure manufacturer that supports the automotive industry. So, there's different types of sharing that's going to have to occur and while we're talking about cyber threat intelligence today, we are at planning and a subsequent phase, not in the first phase, but a subsequent phase, to address the cyber physical aspects of the emerging devices. Getting back to the question. To what level do we want to start talking about some of these kind of capabilities? We can get very deep in the minutia from an education perspective without creating a spec [specification] because we don't really want to do that. So are people more comfortable with a high level description of something that describes the automated sharing, or do they want to hear about specific means today to actually accomplish that, still at a reasonably high level, but a description of those types of mechanisms?

Q/A

Q. **Matt Gardner, CTC:** You said, "Where" in there. Could you go back a couple of slides? Back to a point Doug made in his analysis, there's lots of questions in there. We have members that are fortune 100 types that have their own core analysis capability, but that are coexisting that might be for example, auto manufacturers and industrial manufacturers that do not and so the 'where' the analysis occurs is an interesting question that our members have had, to a degree, some of them not expecting the ISAO to invest in the staff to do any deeper analysis, so have you had any sort of conversation about sub-groups of members that might have conducted some of that analysis as subcommittees or working groups.

A. **Kent Landfield, SWG3:** We have had very cursory discussions. Analysis is definitely one area we have not focused on so much, but the conversations are, to your point, that easily sub-groups within the organization that have the resource to do that kind of analysis, could be spun up within an ISAO to do that exchange. Personally, analysis is one area I am struggling with because there's a lot of different ways you can approach it and our mechanisms, we do not want to be prescriptive. We want to show the value of what we are doing, the value of the information, how it's going to be a part of the system and used but at the same time, it is something that has to be called out, has to be discussed. It's really creating value out of the data that we are sharing and that's, to be honest, I don't have a good answer, not yet.

Mike Darling, SWG3: So, I have a couple of thoughts on that actually. One of the things that I think is really important is when you look at the approach we are taking, start with the data. And when I say data I mean the analysis as well, because analysis is also a piece of information you are using to make yourself do something to make yourself more secure. I think your question is more of an organizational one than it is a data one, right? Because, could an ISAO have a strong, kind of centralized, analytical function? Absolutely. Or, could it have a distributed one, a more cloud sourced one? Absolutely. I think both of those have different pros and cons. But the important thing is that the product of that analysis that gets you toward your goal of being more secure is shared. There's a number of reasons for it. I always use an example. If you have an ISAO of 10 members, let's use malware analysis, and just assume that there's a 50% overlap of what each individual company is analyzing and that's probably fairly low. If you just shared your base malware analysis between those 10 companies with the 50%, you freed up 5 people. There's an operation advantage there because you have freed up 5 people to do higher level analysis and start getting more towards that goal. There's also a business case there that you are using resources more effectively. So, I think, a lot of times, these are very complex issues and one of the challenges is to parts them out. That's my paradigm; start with the data, think about what you are trying to do, think about the organizational pieces, think about the pros and cons, then make decisions and execute.

A. **Kent Landfield, SWG3:** The other aspect to that too is that, what we are laying today is the foundational piece for innovated types of information sharing, at least that's the hope, to emerge. And those innovative types of information sharing will take many different form. One of those forms could actually be, and I hope we see it, because it's probably going to be very beneficial. Not every ISAO needs to have every capability, and if you try to go down that path you may struggle a lot more than you'd expect, but at the same time there may be organizations who form only to do trending and analysis and sell that as a for profit capability to other ISAOs so that information is actually a mesh kind of information sharing mechanisms so you have that central point that on a prescription basis that when you share with them, they share with you. We have the opportunity here to create some very unique and innovative approaches. To these types of hard problems of how do you do analytics in an effective manor if we have 5000 ISAOs and 5000 ISAOs are trying to do analytics, we are really missing the boat. Thank you good question, good comment.

Q: **Frank Grimmelmann, SWG1:** I wanted to comment that the framework I particularly like because I think it lays out the capabilities or services that are there and it does not prioritize or become prescriptive in any way as you just emphasized, but I really wanted to encourage the other work groups and the other ISAOs and SO itself to consider this type of framework which simply lays out where you fit on a matrix, not its hierarchical order in order to achieve success. I just wanted to compliment you on a very well presented schematics that describes exactly what the context we hope for is.

A: **Kent Landfield, SWG3:** It's a lot of work from some really good people so, thank you. Alright, one of the things I guess I just got my answer to the second question we wanted to make sure my situational awareness decision making action paradigm really made sense to people. If you are trying to determine value you really do need to think about, organizationally, what you are trying to do and situational awareness is something you want to have enhanced at all points. It's the situational awareness and the information you get during that mechanism you start to make decisions around and those decisions are going to actually require you to, at some point, take action. We used this as a way to walk us through; what those points of needs were from a conceptual framework perspective.

And then the other question that we are still struggling with. Where work group 4 and work group 3 are going to have to sit down and have a discussion. What are the other PII sensitive data issues that we need to be addressing and considering? That's one area that you… it's potentially a rabbit hole at the same time, I think there are a few things we are not doing a good job of, today, considering. If you have any ideas of non-PII related sensitivity issues I'd love to hear them. The other question, I think is probably a little too broad, but what information do ISAOs need to improve the cyber security of their members? As you go through these documents, especially in ours, you'll see things that we need input on and that's one of the areas, I think, we have a start, but that start if far from a finished product. I would encourage all to take a good look at our documents, all the documents actually, and try to see where it is that you feel that there's just something missing. We have already had a lot of good input from folks who have taken that same approach and I'd like to see that more.

Greg White, ISAO SO: You asked a question about what are the non-PII sensitive data issues. One comment that we talked about earlier is the difference between privacy and confidentially, privacy being the PII side but the confidentiality being the business side. That is one thing that I think either your group or group 4, I think that's something we need to keep in mind, both the personal privacy and then the business confidentiality.

Q: **Rick Lipsey, ISAO SO:** Thanks again to both of you for the leadership you're providing and it's very exciting to watch your group in action. You got a great group of folks working there. There's been a good dialogue that's been circulating among a number of the members involved in the process about the importance of trust. And that is foundational to the information sharing that's going to occur. My question is, to what extent do you plan to address trust and

how to achieve it and how to sustain it as part of what you're developing and to what extent are you looking for other groups to tackle that issue?

A: **Mike Darling, SWG3:** You often hear that trust is based off of relationships and I think that's true to a certain extent, but one of the things that you get from a personal relationship is that I understand what we are talking about is that I understand what you care about and [you understand] what I care about and we have a mutual respectful relationship about those things. We don't have it explicitly in our documents right now, but I think the place where we build off of that is when we talk about these frameworks when we talk about the data models. What information are we actually talking about? Instead of having this conversation that is theoretical. "Well it could be this, or it could be this." You move that down and you create a foundation of mutual understanding and I think that mutual understanding is the first piece of a trusted relationship and that's the first piece of being able to scale it out. As an aside, I think it's broader than the information sharing group, I do think of the ISAO concepts, ISACs included in there, there's a little bit of trust brokers, as well. So if you have robust sharing amongst ISACs and ISAOs, if I am a company I don't have to gain from the information all of these other organizations have, I only have to trust my ISAO. I don't necessarily have to trust 100 different organizations. I do think there's a broader opportunity there in that concept of trust broker.

Kent Landfield, SWG3: From the standpoint of trust, there is the trust between humans and there's the trust we have to establish between machines and organizations and we really haven't gone down the path too much from the standpoint of machine trust. That's something yet that is still academic research and in progress, I mean pure, real, trust. From the standpoint of organizational trust it is not that hard to get. Trust in an organization, NDAs, contracts, the like, end up creating those kind of trust situations. It's a matter of how we look at it from an SO perspective. Because there are those three really different types of trust we have to address. We have human to human, organizational to organizational and machine to machine.

Q. **Rick Lipsey, ISAO SO:** There's a nuance I want to tease out of this. I have heard comments from some that would lend one to believe that there's an approach that is being considered that views trust as binary. I trust you or I don't. I trust your organization or I don't. I trust data stream or I don't. My sense is that there's probably a graduation with that and there's a degree of trust that is established that says, when I get this bit stream in am I simply going to act on it or do I need to do some review and analysis, and betting on it first before I pass it on to another group, or what have you, and as it pertains to the information sharing models that you're looking at developing, whether they are automated or non-automated, how does that binary or multiple layers of trust of data or individuals or organizations play into that?

A. **Kent Landfield, SWG3:** The binary nature doesn't. There's no such thing as I trust you completely. Well, maybe between a parent and a child but from the standpoint of that trust I never seen an organization trust another organization totally, explicitly. There's always some buffers, some protections, and some mechanism that's there to do that. I think in a lot of respects it's not binary, it's actually a matter of confidence because if you have data sources

coming from 15 different places, some sources have a better level of quality that you are going to get on a daily basis. Some have a really poor level of quality and when you rank those I can easily see an automated environment where those types of feeds are actually scored base on usefulness to the organization so those that have a higher level of confidence because you trust the quality for what's occurring data wise, again back to the data, then you can actually look at trusting that information source better than another information source. You do it today and you don't even know it. You read the newspaper and you read a newspaper or 5 newspapers and there's one that's always your favorite because you get better information or it's more comfortable for you, or whatever the reason. It's not all that different from here from an automation perspective when we start talking about sharing and trusting.

Q: **Roger Callahan, FS-ISAC:** I think when people talk about trust we all understand, "I'm going to keep your information confidential". I think one of the other issues though, around trust, is that trust is build up as a result of performance over time. Trust is not a data point, it's really a destination, so if you are an ISAO and you are really performing, your members trust. You become a trusted source. Then as that trust is created, it's a momentum thing. If you create more trust and more trust, that's been our experience. What they really want to see is that performance because you can put all the mechanisms in the world for trust, but if you can't perform, trust breaks down. I would put performance as an element of trust.

A: **Kent Landfield, SWG3:** I do like that point that trust is an information point in itself and needs to be identified.

Frank Grimmelmann, SWG1: I wanted to make a comment, Roger, I'm wondering if we could use the word for what you just described which is incredibly important, as 'confidence' as opposed to 'trust' because I always viewed trust as between people you can have trusted electronic relationships as well, but I think that what you described is essentially confidence in the data and the value proposition.

Scott Algiers, IT-ISAC: It's not just organization to organization trust, It's whether members of an ISAO trust other members of the ISAO to use and protect the information properly.

Chris Blask, ICS-ISAC: Trust can well be binary if you don't trust a sources last destination no information should cross that gap. If you did, and the trust was betrayed it's unlikely to be recreated. Kent's comment on quality is really what we are talking about when we are talking about trust.

Mike Vermilye, JHUAPL: On the automated indicators sharing effort, we've been refining a brokering concept between trust communities to where members of one trust community who are members of another and exchanging information between them, put in the capabilities where they can respect the constraints on dissemination and use, put on by a provider of information when it transits between to trust communities. We've been working on that, working on papers, and I actually have a set of slides that, I'll just need to check the sponsor, it

was presented at TTX [Table-Top Exercise] for federal personnel that kind of laid out that whole concept of what's involved in a couple use cases. That might be something.

ISAO SO Note: This transcript contains edits from the original recording for presentation in written format.