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

Public Comment And Debate: Standards Working Group 4

Speakers: Rick Howard, David Turetsky, Co-Chairs, SWG4

Rick Howard, SWG4: Hello everyone, my name is Rick Howard. I'm the Chief Security Officer for Palo Alto Networks. I am Co-Chair of SWG 4 and this is my partner David Turetsky. This is not a competition between the committees, but how many other committees were smart enough during their meeting over the Pirates of the Caribbean ride yesterday? Just as a note we had a very raucous debate yesterday in leadership meeting and just some advice we got form Pirates of the Caribbean ride, if you want to tamper down that debate, dead men tell no tales.

The Security and Privacy committee is made up of about 15 core members and about 40 general members and the difference between the two in our committee is the general members can go to every meeting and kibitz about what we are doing, but the core people are the people I get to assign tasks to. We are looking for more people to be core committee members so, as I get an opportunity to talk to this group and everybody on the webinar, I'm looking for other people to come, join in and actually contribute to the group. There is a lot of work yet to be done; we've made a lot of progress, I think David would agree, but still more to follow. One of the things before I tell you about specifics, I want to bring up something Mike Echols said yesterday in the leadership meeting. This is a standards group and I know we are very careful of not trying to say, "You have to do 'X'" or "You have to do 'Y'". We don't want to make anybody angry, but the reasons we have standards is to make it easy to do what we are trying to do and I think we have to establish things that we all agree [on]. Maybe you don't have to do it internal to your own sharing organizations, but if you want to be a part of the community, here's some things you're going to have to do together and we all agree on it. Yes, that means we have to make some really, really hard choices about how we think these groups are going to go forth and do things.

The Security and Privacy committee. This thing is unique because out of all 6 committees, this kind of standard is what everyone does in every organization in the world, every business outfit, every government outfit, any kind of group that gets together thinks about how you secure your environment and thinks about how you protect the privacy of their members and their data, it's an interesting distinction between this group and others. Because what we really don't want to do is provide a lot of details of how to do just security or how to do privacy. What we're looking for, is what makes it unique in an ISAO, what security things are unique in an ISAO and what privacy things are unique in an ISAO that we want to highlight to brand new folks forming their own organizations and maybe we can advise existing organizations to think about because maybe they didn't think about it upfront. I'm a big believer in first principles. Last summer I read [the] Elon Musk biography, and he doesn't tackle small problems. Right? He tackles big giant hairy problems that none of us think that are possible and the way he does it is he doesn't take what other people have done. He reinvents everything from scratch just to learn how the problem domain is. This is our opportunity to do that for the information sharing organization. Right? So, we need to strive to go higher in our standards not just try to document what we already have. Did you want to talk about anything specific about privacy?

David Turetsky, SWG4: Why don't I just sort of hit a couple of the highlights of the privacy paper that we look forward to getting input on and we've already had some discussion about some areas of potential revision in our working group meeting before part of it adjourned to the Disneyland where we invested further efforts in creating a new reality. Anyway, the gist of it is that the importance of privacy to this process, I think to some extent, the ISACs we have out there have largely been successful and privacy has not been a hot button issue. It was in the debate over CISA, but not so much in the actual operations so far, which I think is a great thing. Privacy is a sensitive issue though and there is frankly, if it's not something that's considered carefully and addressed, it is a threat, in some sense, I think to the category of ISAOs and ISACs because if we ended up with a group of sharing organizations that didn't respect privacy it would be something that could potentially effect the credibility of more organizations than would fairly be impugned, if you will. Anyway, I think that there is certainly no reason that privacy needs to be challenged in the information sharing process and so the sensitivity we've been trying to address is to give some guidance to ISAOs about what the sensitivities are in privacy and different ways they might deal with it. For instance, that means that, in terms of an ISAO membership, and ISAO would want to provide some guidance to its members about what kind of information should be shared or not shared so that it isn't in a position where it may have invited the sharing of information that is private. We have been fortunate to be able to draft, to some extent, off the guidance that was put out by the Department of Homeland Security and the US Department of Justice interim guidance on privacy and civil liberties, other guidance that is out there for non-federal entity sharing that we heard about this morning from a DHS representative and going forward we know that there are additional documents, which we heard this morning, are going to be revised and updated to not only talk about the privacy in the context of ISAOs or ISACs sharing with government, but ISAOs and ISACs of course don't need to share with government that's a choice they can make, but CISA potentially applies to them even when there is private to private sharing. We'll be addressing some of that and the CISA standard is that companies have liability protection or ISAOs have liability protection when they are sharing and don't know at the time of sharing that there's some kind of PII, private information identifiable to an individual, that's part of what they are sharing. We intend to address considerations that ISAOs may want to undertake to be careful about privacy once they receive information, options for them to address with their members what should or shouldn't be provided and the like. That, I think, is probably the overview of what we're talking about. Questions that have come are; what should an ISAO do if it finds out either because it's been notified by a member that they mistakenly shared something that they shouldn't, what kind of process or function should they have to address that? What should they be doing, any kinds of scrubs on their own or not, is that an option? If members want CISA protection, what do they need to do and the like, and of course there's a whole, strange in some ways, body of law and guidance out there about what constitutes PII that is not necessarily intuitive. That's important to understand and to the extent that an ISAO may also get involved in sharing internationally, potentially with companies that are global and may be including in the shared information,

information on data subjects abroad or on events that involve data from people based abroad. There's the possibility that the laws of other countries may also come into play on privacy for some of that. We are trying to address this whole panoply of issues. In some ways the paper I think was a little more prescriptive in the draft than it ultimately will be. We want to provide options, choices, identify issues that should potentially be considered and the like, as a way of providing a road map for ISAOs on privacy issues that they should consider and evaluate how to approach.

Q. **Rick Howard, SWG4:** I want to ask a specific question to everyone here since we have this group of smart people, I would like one specific thing that's about security and privacy that is unique to ISAO?

A. **Mike Darling, SWG3:** I would probably say the ability of interim segregate and protect individual member information the way that you normally do in a normal enterprise.

Rick Howard, SWG4: That's a great point because in a normal organization they will have to do that and like in my company we don't have to segregate from people specifically but we definitely don't want group a or group b if they didn't get together; that's a great point for security or privacy, any others?

A: **Mike Echols, DHS:** So, a yet unanswered question related to vetting, of either members or the IASOs itself and then the information of how its disseminated and who gets it and why do they get it?

Rick Howard, SWG4: A question about how do you vet new members coming in or existing members of an organization. That's a great question that we haven't even talked about.

A: **Frank Grimmelmann, SWG1**: I think one level of complexity that differs with ISAOs form our experience is the fact that the levels of trust are not synonymous across different groups we share with so I would urge you to either comment on or evaluate how you are able to determine the level of security and privacy required depending on whom you are sharing with and in what format.

Rick Howard, SWG4: The question I have for you, is that confidence or trust?

A. **Frank Grimmelmann, SWG1:** Trust, in terms of whether I trust you to know who I am or not. Example, let's say that I am sharing among my members who are vetted and trusted with full attribution as to victim as to whom they are, yet they may not have that same level of trust in sharing with government, law enforcement or intelligence. Therefore, we have to have mechanisms, somehow built-in, to address that.

Rick Howard, SWG4: We do cover a little bit of that, but it needs more detail in the current document on labeling and policy for who gets to have that kind of data, but what you said is a lot for granular than what we even touched in our first draft. That's a good one though.

Q. **Brad Howard, ISAO SO:** This may trail a little bit on what frank had asked, so information is shared. You've got the privacy and security covered on it. As it moves around perhaps even from ISAO to ISAO, is there an ownership issue of how that information is going to be used and therefore privacy and security concerns applied to it?

A. **Rick Howard, SWG4:** That's a good question**.** When we talked about that part of it, the labeling piece, I don't think we even mentioned an ownership deal and who has the authority to say it can go further than your own ISAO or it needs to be deleted at a certain amount of time. I'll put that into the next standards.

Q. **Dan Strachan, AFPM:** Yesterday morning when you were having your leadership meeting I had a chance to watch the summit committee on homeland security and governmental affairs hearing on assessing the security of Critical Infrastructure. One of the witnesses there was Ted Coppell and in his closing remarks he brought up the whole thing of privacy. He said privacy is thrown down as almost a gauntlet to slow cyber security down and implementation. Coming from somebody in the media, that was very surprising. What are your thoughts on that because he is not the first person I've heard that from? I know when we were dealing with CISA last year on the hill that was brought up a few times.

A. **David Turetsky, SWG4**: I don't want to comment specifically on Ted Coppell because I didn't hear what he said, but what CISA did, for example, was it focused on ways to remove obstacles to the rapid sharing of information. I'm a lawyer and I say to my clients sometimes, this is general council's clients, that that law was addressed to you. To the extent that you are balancing the possibility of making an error and inadvertently including some PII in something that you share because you don't have time because you are moving rapidly, to assure 100% that you have screened it out, this law is made to encourage that sharing and to protect you because unless you knew at the time of sharing that you were including PII, you're protected even if you did inadvertently include PII. CISA, I think, was focused on trying to, if I understood your description of Mr. Coppell's testimony was, was meant to try to speed up information sharing in balance appropriately privacy and information sharing. Because at the end of the day, improved cyber security is the protector of privacy, not at odds, because if we don't protect our data we will be all over the place. We need cyber security, we need a balance.

A: **Rick Howard, SWG4:** Mr. Coppell wrote a book last year. Okay? He talked about the electrical grid security. He didn't talk to any security practitioners. He talked to… he kind of outlined the problem and then he went to Utah and talked to a bunch of government leaders. That was all he said. So, that book is not a very good depiction of the issue. That specific question. This is typical of what I get, I've been a cyber security practitioner for 30 years now, if you put security at the beginning of a process, it slows nothing down. If you try to bolt it on at the end once you've got everything established, that's when you start to hinder the process. So this discussion of ISAO SO products that we are developing, we are at the beginning of it and we can put security at the beginning and it won't slow anything down, it becomes a lot less onerous if we figure out how to do it first instead of after.

Mike Darling, SWG3: I'd like to pile on to that, more specifically privacy versus security. I want to point out if you think about what he was talking about earlier on the way CISA was implemented, I think this is a model going forward, privacy and security I reject out of hand are fundamentally a zero sum game, that you can have more security if you have less privacy and vice versa. If you think about how DHS is doing their CISA program where they have defined a discreet set of data elements and then they went through each elements and said this one has privacy implications and we can either do a technical mitigation or a human review on that to make sure it doesn't work. There may be the slowing of the process but by doing that, like Rick said, they baked into the beginning the security piece, they baked in the privacy piece and are actually achieving what they are trying to do in a way that wouldn't happen if it was the past debates where a very abstract, "well, we can't share information", "what if" to death and that type of thing. When you get to the granular pieces and I'm going to harp them back to the data, and this is why it is so important to be clear what the data is, you can make those decision of privacy versus security because they are not mutually exclusive.

David Turetsky, SWG4: The guidance that has come out of DHS and DOJ is very specific on what kind of information that in some context might be considered PII is and is not a part of a threat indicator and would be able to share under CISA for instance. IP addresses are normally not, but to the extent where a DDOS attack is coming from and other alike parts of that, well then an IP address would be potentially part of the threat indicator, but there is no, I don't think, fundamental opposition, not the way ISACs have for the most part conducted themselves so far and the way I would anticipate with some guidance, ISAOs would conduct themselves because as I say, my data is from my time as a government employee, is just all over the place and from companies as well. Unless we improve cyber security we are certainly not going to be protecting privacy.

Q. **Mike Vermilye, JHUAPL:** Two points from previous discussion was the ability to inforce constraints on dissemination and use, I would argue upfront, right now everyone is using TLP. TLP is, not totally useless, but it's pretty darn close for enforcing things further down the road because what it says is if it is TLP red it stops here. What's all up with that? There needs to be, I'm not saying a fully detailed like we worked on with enhanced shared situational awareness where its detailed tagging regime but there definitely needs to be a look at 'Son of TLP' or 'TLP 2.0' and there is some work moving in that direction, but there has to be a way to, at a more granular level, tag the constraint, the originator of the information wants carried with that information as it flows through the sharing and the big thing there is then you don't have to go back to the originator to say, "Hey, I know you said it's TLP yellow and I need you to make it TLP green for the following reasons" and start a whole discussion about [it]. That's something that needs to be looked at. A nuance of PII that was eluded to is, PII is necessary to understand the threat. In cases, you have to share the PII to give context of what you are sharing and again, I guess CISA will protect sharing PII and you could make the case this is necessary to understand the threat. I would just like comments on that.

A. **Rick Howard, SWG4:** I'll start on the first one. TLP was designed for one organization so you're right, I think it would be something this group should take on, what's version 2.0? The question was, shouldn't there be a better version of TLP? We are trying to make sure ISAOs can go there, TLP doesn't really match, we would have to bend it and you said somebody is working on that. How far along are they?

Mike Vermilye, JHUAPL: They are on their first draft.

Kent Landfield SWG3: I do want to say that I think TLP is, today, not as useful in this kind of situation as it could be. I hope the work inside at first is useful but I do encourage you to take a look at that, I do encourage you to take a look at the real problem from an ISAO sharing perspective because if were really going to get to a mesh environment, a mesh network of sharing information, where everyone seems to want to get to, that's going to require a lot more control over our corporate data that's being passed around and yes you can anonymize but every time you do you strip out context that valuable for trending and analysis. So, I think we have to, as the SO working groups, really look at the applicability of what exists today and where it doesn't exist, we either have to encourage that to change or we have to do it ourselves.

Rick Howard, SWG4: That's exactly right. Right now, TLP kind of puts barriers up if you want to share anything that's kind of [audio difficulty]. We need to build whatever we have so it encourages people to share. Given the choice they don't have to, but we need to make sure we encourage them to do as much as they possibly can.

Q. **Roger Callahan, FS-ISAC:** was there any discussion of 'derived data' as far as PII? What I mean by that, if I may, the analogy to the classified world, in the sense you can have lots of aggregated unclassified that eventually gives you classified information. Right? So, in the PII world there's going to be a lot of data, and we all know from even un-PII data, you can derive PII data. I don't know if there was any discussion of that.

A. **Rick Howard, SWG4:** Yeah, there was none about that so, I'll put it on my list. One point I want to make though is, maybe this is obvious to everyone here, but ISAOs are intelligence organization so, the language we are using to describe it like [audio difficulty] levels and derived classifications, all of that applies to these folks and maybe we should bring that to the front and kind of say what it is.

David Turetsky, SWG4: Actually, we have kind of talked about it a little in the context of privacy because there are different definitions of PIIs and we heard from Jeff this morning about the different regulatory agencies and some of them, including his, have a proposal now with an incredibly broad definition of PII and that's going to be an issue that potentially impacts ISAOs because if they do engage in protected sharing under CISA, it's one thing, if ISACs or ISAOs don't do that, but share PII and depending on what kind or sensitivity, it does raise legal issues about what happens to them and so that's just a whole other overlay. For instance, if there was a piece of protected health information that was a part of it and somebody knew that was being shared and it ends up in the ISAO, it's not just a level of protection you give it to and how many people you share it with, there's another underlying legal question of whether you can do that in the first place and whether it has to be reported somewhere.

Q. **Rick Lipsey, ISAO SO:** Although this entire effort was started under the aegis of an Executive Order, we know that our constituency includes multinational corporations and others with multinational interest so, my question to you is, to what extent is the work that you are developing applicable universally and to what extent is it dependent on US law?

A. **David Turetsky, SWG4:** So far, in the first draft, we have flagged the special issue of sharing information on what you might refer to as 'data subjects', PII, from people from abroad. We've flagged as a consideration that there may be definitions of PII and obligations in connection with the transfer of information that raise issues that need to be considered. We haven't really gone beyond identifying that there is such an issue. We don't think we want to provide a legal compendium of law of Germany and all the rest. I think what we want to do for ISAOs is flag that and I think what ISAOs will probably, in turn want to do, is flag that perhaps in some of their terms of use or representations with members to tell, to suggest, members ought to be to the extent of sharing information if it involves any PII from abroad, they should comply with all of those laws and I have a feeling that is where ISAOs and ISACs will go with that.

Rick Howard, SWG4: Going back to that vetting argument someone was making, from last question how do you vet somebody. If I'm going to share with an organization from Germany that's the first question. Here is the list of things we share, is that going to violate your laws?

Rick Lipsey, ISAO SO: Part of the reason I asked the question is that there was a suggestion that has been made that we ought to consider pulling those things that are truly US government specific or US law specific out or identify them as a separate document or separate annex or what not and so what I'm pondering is how feasible that is for the work you are doing or to what extent is the privacy considerations you are developing are truly universal and to what extent are they really rooted in United States law?

A. **David Turetsky, SWG4:** I think some of it is rooted in United States law to the extent we are going to talk about CISA, for instance, that wasn't even in the US law until December 2015 so that's an important consideration because members are going to be thinking about that and ISAOs will have to think about whether they want to comply with that and provide that protection and be protected in that way. So, I think there are some core elements of what we are writing about that are US but the international law principle that I mentioned a moment ago, that would apply to a global company that has a US presence and is a sharing member of and ISAO or ISAC so, some of that is probably immediately relevant.

A: **Norma Krayem, HKLaw:** I wanted to [audio difficulty] a lot about the international piece. I would just suggest since we have so many companies who are multinational and global that it would be very confusing to try and write a document that is domestic versus international. The other option is that we look at each of these components and if we notice if there are key differences

that we need to suggest, or make sure people are aware of, we can document those accordingly, but I do think that if you were to write a section that was domestic US only and now chapter 3 is international only, for a lot of companies who are doing this now, they're not going to find that very helpful and probably more confusing.

A: **David Turetsky, SWG4:** Rick and I would be remiss if we didn't thank the lead authors of the portions of our report, Norma Krayem, thank you for being the lead author on security and Carl Anderson who was on the phone for being the lead author on privacy and Chris Boyer who contributed in major ways to all pieces and to the rest.

Kent Landfield, SWG3: To address Rick's comment or question. I think in some respects there are things that have to be put into the base document that explain the concepts and the like. It's just a matter of the level of detail you want to go into specifically in one section that could be put somewhere else. That way, to Norma's response, multinational companies have multinational issues so this isn't just one countries issues and somehow we are going to have to figure that out because cyber security is not restricted to that national boundary.

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