Part 1: Using IPOR for Situational Awareness

Lisa Young: Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT Division is part of the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org. Show notes for today's conversation are available at the podcast website.

I'm Lisa Young. I'm a member of CERT's Cyber Risk and Resilience Management team. I'm pleased to welcome my colleague Doug Gray, also in the Cyber Risk and Resilience group. Today, we will be discussing Doug's take on IPOR, Intelligence Preparation for Operational Resilience. Today's conversation is based on a special report by the same name authored by Doug, and a blog post titled, "Leveraging Threat Intelligence to Support Resilience, Risk, and Project Management."

So, without further ado, welcome to the podcast series, Doug.

Doug Gray: Hi, Lisa. Thanks for having me.

Lisa Young: Well, I appreciate you being here to discuss this topic with our listeners. Can you start by sort of giving an overview or telling our listeners about intelligence, and what intelligence is, and how it might be useful?

Doug Gray: Well, essentially intelligence is--it's a term that we hear a lot in the national security arena, in military channels. But essentially, all intelligence is all of those inputs that go together to give us an awareness of our situation with regards to our environment, and as well as with our adversary because, let's face it, cybersecurity and operational resilience as a whole can be a rather adversarial proposition. Even if we're not talking about people or groups of people as an adversary, and adversary, or threat actor as we call them could be as simple as a hurricane, or a tornado.

So, essentially, what IPOR does is IPOR enables the organization, the manager, to break down the kinds of information that he or she needs in order to build situational awareness about their environment. It breaks down what kinds of information do I need? It also enables me to determine what kinds of information do I have on hand? What's the difference between what I need and what I have on hand? And it also enables me to determine how do I go out and get that additional information? And probably the most important part of this is it helps us to link that information into ways of acting upon that.

Lisa Young: Okay. Well, thank you. That's a great description. Now, can you tell us about this IPOR, Intelligence Preparation for Operational Resilience? How did you get the idea? And how did it come to be?

Doug Gray: Well, it actually came about from a conversation that I was having with a client. This particular client was a government organization. And I was remarking that they did a great job of identifying compliance requirements, things like OMB (Office of Management and Budget) memos, executive orders. And they had some pretty mature processes in terms of converting that into project management. But one of the observations I made to them was, "The one thing that I don't see you doing is taking into account what is the threat actor doing?" And so, the client pointedly asked me, "Well, how would I go about doing it?" And so, that gave me the idea to try to answer that question. And IPOR was the result of that.

So, one of the things that I looked at was I looked at my own experience as a cybersecurity manager and looking at all the different things, the open source news media and technical media information. I was on active duty with the Army. So, there was also classified intelligence. And I was looking at some of the challenges that I remembered having which is how do I separate the wheat from the chaff, and how do I determine the relevance and the context for this information, and what does it mean to me?

So, one of the frameworks that I took a look at to elucidate what would the IPOR look like is a framework that the Army and the Marine Corps use called Intelligence Preparation of the Battlefield (IPB). Any time that the military goes about doing any kind of operation, even ones that are not necessarily adversarial such as fighting forest fires or peace keeping, they analyze their mission. And part of that is this process called Intelligence Preparation of the Battlefield.

And it could be things such as the weather. It could be things such as the terrain. It could also be things such as civil- military conditions. And I thought, gee, isn't this something that we could, first of all, translate into a language that the layperson could understand? And second of all, isn't this something that we might be able to give a more definitive treatment to operational resilience in cybersecurity as a subset?

Lisa Young: Okay. Well, thanks for that description. And actually that was going to be my next question. How did you go about sort of translating this IBP to a non-military audience?

Doug Gray: Well, one of the things that I looked at was were schools of thought such as business process improvement. And one of the terms that stuck out to me was the voice of the customer. And it reminded me of a saying in military planning that regardless of whatever operation you're doing, regardless of how grandiose your plan is for conducting an operation, the enemy always gets a vote.

And so, what that means is that, despite everything you know about your own condition, about the environment, there are always things that your adversary and the environment can do to change that. And I said well, that's a voice. And that's a voice that goes into your planning. So, I used that idea of the voice of the customer to build out these other additional voices which help a cybersecurity planner, an operational resilience planner, to determine well, what are the inputs that I need to know in order to do my risk management and eventually do my project management?

Lisa Young: Okay. All right, thank you for that. That's really good. So, then it sounds like this not really about collecting intelligence. But it's really rather about using and being aware of things that a cybersecurity manager might need to know.

Doug Gray: That's exactly right. We wanted to stray away from intelligence collection. There's a rather large body of knowledge on collecting intelligence. It's very specialized. But what we find is that your line managers, your cyber security managers, your operational resilience managers may not be able to have a structured, pragmatic way of identifying well, how do I consume that intelligence, how do I build a relationship of trust, which is repeatable with an intelligence provider? And that's really what we're trying to achieve with the IPOR framework.

Part 2: Setting the Operational Context and Hearing the Voices

Lisa Young: Okay. So, then how would someone know if IPOR was a good technique for them to use in their organization?

Doug Gray: Probably the best thing to do is to look at how you're currently consuming intelligence today. A lot of us in the field, we may start our day looking at the blogs, looking at different trends or different sources. Krebs on Security is a great source, SANS, Dark Reading. And ask yourself if you are confident that you are consuming that intelligence in a way that is in the proper context. Ask yourself are you answering the so what in relationship to what it means to your organization? So, one of the ways to do that is to look at the special report and compare it to how you're looking at these inputs of information right now. And look at things, such as am I considering the business environment, am I considering the physical environment, even am I considering the legal environment? And ask yourself if that changes the way that you are consuming intelligence today.

Lisa Young: Okay. All right, so that's some good management considerations then. So, then thinking about sort of, as you mentioned, cybersecurity and all of the other frameworks and standards that are in use, how do you see this fitting in with other things that people are already doing?

Doug Gray: Well, that's a terrific question. Kenneth Olsen, the former CEO of Digital Corporation had a great saying where he said, "The great thing about standards is that we have so many to choose from," And that was exactly what we wanted to try to avoid with the IPOR. We didn't want to create yet another framework that we had to utilize in conjunction with all the other different frameworks that we might have been using.

We wanted to specifically fill the gap of making sense of your environment, making sense of your adversary. So, in building this framework, we built sort of connectors into three different risk management frameworks. There are a couple process areas for our own CERT Resilience Management Model (CERT_RMM). One is called Vulnerability Analysis and Resolution (VAR). Another one is called the Risk Management Process Area.

We also have our own OCTAVE Allegro Risk Management methodology. And of course those who do a lot of work with the government are familiar with the NIST Risk Management framework. So, we thought it was very important to be able to show how you can take the output from this and plug it into specific places in those frameworks in order to continue the process without replacing them.

Lisa Young: Well, sure. And if I understood you correctly, thinking about those other frameworks and standards, there's some pretty good things that you can do to fit some of these things together. And whether you do your threat collection or threat analysis in more of a formal way or an informal way, I think this might be actually useful in many different organizations.

Doug Gray: Exactly, and especially a number of organizations will generally have to change their way of expressing their risk management based upon who their customer might be. Today it might be ISO. Tomorrow it might be NIST. So, it's very important that your ability to collect, to build your situational awareness, be extensible and be flexible to adapt.

Lisa Young: Now, you mentioned something I think a few minutes ago about the building of trust with your intelligence provider. Can you talk a little bit more about that and the management considerations for that?

Doug Gray: Absolutely, one of the things that we should consider as managers is who-- do we have a regular place that we can go to get our information? Now, one possible recommendation-- one of the people that we talked to is an individual in the military who actually did IPB for a living. And one of the things that he recommended a manager considering is having an individual on staff for whom a concerted amount of their time is receiving and processing intelligence. Even if they're not an intelligence analyst, having a one stop place to consider this intelligence is very useful. So, this could be done in house. It could be done partly in house. Or, it could be outsourced.

But one of the things that having a regular routine and a trust-based relationship with an intelligence provider enables you to do is the intelligence provider gets to understand how you think, and what your priorities are, and what matters to you because it's going to be different based upon the organization.

The other thing it enables you to do is to get an insight into their judgment. There are going to be certain qualitative, intuitive things that your intelligence provider is going to be able to see and recognize that may not be apparent in, say, a report or just the data stream. And having that kind of relationship allows you to tap into that.

Lisa Young: Right. So, you get to tap into then the collective experience, judgment, sort of things that they're thinking about as they gather intelligence or information from different sources.

Doug Gray: Exactly. It's all about bridging that gap between intelligence and management.

Lisa Young: Oh, and then being able to put that in a context that does matter from a risk perspective. I like that approach actually a lot because there's so many things that we have to contend with, so many different threats, and so many different-- the risk landscape is constantly changing. Having that relationship and that constant, steady stream of information flow is a good way to sort of gauge how you're doing and where you are on the continuum of risk management, too.

Doug Gray: Exactly. And there are other frameworks that we talked about such as the goal question indicator metric (GQIM) framework that enables us to determine what's the question we want to ask. By understanding the strategic goals that you're trying to support and to develop questions that help you understand if you're meeting that goal, you can better ask questions of your intelligence provider, so that they can give you the information back which scratches your particular itch.

Lisa Young: Okay. All right, that's perfect. All right, so then let's decompose this IPOR a little bit more and talk about the different elements of IPOR, and describe them for our audience. So, let's start with-- I read your report, and I enjoyed it. But let's start with decomposing information. Can you say a little bit more about taking in the information and then the decomposing step?

Doug Gray: Well, and that's a very key point. I'm glad you brought that up. The saying we hear a lot is eating the elephant one bite at a time. And nowhere is that more important than trying to build your situational awareness in intelligence. You're going to have partial information at any given time, especially given the rapid change of the cybersecurity and the operational resilience environment.

So, one of the ways to keep from being overwhelmed and to build your situational awareness incrementally is to breakdown those elements into what we call voices. We talked a little bit about the voice of the customer earlier. Well, inside of IPOR, we break it down into three voices. The first one is called the voice of the environment. It's essentially neutral territory. It is the environment that both you and the threat actor has to participate in. And it can be things such as the social- political environment. It could also be a physical environment as well. Of course, things such as floods and forest fires, proximity to tectonic plates and the resulting earthquakes are all part of the environment.

The second part is the voice of the organization. And that breaks down into a couple of other voices. The first one is the voice of the mission. And the voice of the mission is essentially well what business are we in, what's our mission? What are our strategic objectives for the larger organization, and what services, things like HR, e- commerce, payroll, accounts payable, what services support those? And then we actually take a look at the assets that support those services, things such as servers and facilities, basically people, information, technology, and facilities, and how do they support those services.

And what that does is that enables us to tie it down to us, the organization, the assets that we're trying to defend. And it gives us context which is meaningful to us. And the last part is that whole idea of the enemy always gets a vote. And that is the voice of the threat actor. And Intel, for instance-- and we're not promoting any particular product.

But for instance, they had built a very neat taxonomy of threat actors called the threat agent library. It enables you to break down this wide plethora of different threat actors into definable categories. And inside those categories of threat actors, by understanding the voice of the environment, and understanding in the voice of the organization, we can build what we call threat actor use cases. Based upon all that information, what do we think that a particular threat actor might do? What are their capabilities, their intentions? And what kinds of attack patterns might they use to try to degrade the resilience of our particular assets?

PART 3: Getting Started With IPOR

Lisa Young: Okay. So-- well, I was just going to recap. So, voice of the environment, voice of the organization, voice of the threat actor, I like all of those concepts. And I like that notion the enemy always gets a vote. So, say a little bit more about those and sort of put them in context for what the user should-- how the user should view those in the context of IPOR.

Doug Gray: Well, one of the things that the user should remember is that you're going to build this incrementally. You collect the information that you have. And you may even have to make planning assumptions, as long as you identify those as assumptions and come back to them later. The voice of the environment, for instance, will include things such as legal statutes, but also legal precedents.

So, take for instance the Computer Fraud and Abuse Act (CFAA). That is, for cybersecurity defenders, that seems to be our big-- that's our big bullet for a recourse if somebody utilizes our assets in a way that we didn't authorize them to do. Well, court cases after the statutes are passed actually changes how those particular statutes can actually be enforced.

In the case of the Computer Fraud and Abuse Act several years ago-- and this may have changed since then. I have to say I'm not a lawyer, and I'm not trying to substitute for qualified legal opinion. But in the case of the Computer Fraud and Abuse Act, there actually were court cases where appellate courts ruled that act as unenforceable because they said it was too

vague. Having a-- in addition to your intelligence provider, having a routine relationship with legal counsel enables you to build that kind of situational awareness as well.

Lisa Young: Okay. All right, great. All right, anything else you want to tell us about IPOR, the different elements, before we go on to the next question I have for you?

Doug Gray: Just the thing I want to stress is-- and this is a saying that I try to say over and over again. And that is the formality of the process and the rigor of the process will depend on the time and resources available. Even when you're looking at the assets inside of your own organization, if you have a large organization, and if you're just starting out with IPOR, it may be an additive process of identifying the assets that support your critical services. And that's okay.

Build on it as you go and improve your situational awareness as you go. And update these three voices, the voice of the environment, the voice of the organization, and the voice of the threat actor as you go.

Lisa Young: Okay, all right, great. Well, then that brings me to can you tell us how you might get started using IPOR. Is there is a best place in the organization to maybe leverage what you're already doing?

Doug Gray: Well, the first thing to do is, obviously, shameless plug, is to download the special report and to take a look at some of the steps involved. The next thing to do is to actually take a look at your resources available and also take a look at your time constraints. An organization who may be under the gun, of course, may have shorter time constraints than ones that may not be under the gun.

So, take a look at what do you have financially, human resources-wise, and technology-wise in order to support this kind of framework. One of the things that we stayed away from was trying to dictate what kind of format this takes place in. So, my background is as a database guy. I see this and I see this as a database. But that could be my hammer making this look like a nail.

You have to take a look at how you process information to determine is this a routine report, maybe a presentation, maybe it is a database. Or maybe what you want to do is you want to start on a particular incident or set of incidents and then evaluate them in the context of the IPOR. So, that's definitely the second thing that you want to look at.

Lisa Young: So, then thinking about taking a look at incidents and taking a look at things you're already collecting information, can you say how IPOR might support that, or be an entry point to that, or put it in the context of that?

Doug Gray: Well, for instance, if we're doing cyber security, of course, we're-- our currency today seems to be incidents. And we want to be able to pull meaning out of an incident other than what just happened in a particular the incident itself. We want to try to determine is this a larger trend or is this an isolated environment.

So, one of the things we can do is we can take a look at that particular data set and create an anchor point, a start point. And if we want to start with our incident database, what we can do is we can use that GQIM method that we just talked about, goal, question, indicator, metric, and we can ask ourselves, "Well, what do we want to know about an incident or a set of incidents?"

And one of the great things about GQIM is it works both for us, in terms of the ones who are defending, and the threat actor as well. The threat actor has goals. And there are questions that we can ask to try to elucidate whether or not the threat actor is reaching his or her goals as well. So, probably the first thing to do is to create an anchor point and build out what questions that you want to answer. And then try to fill in the gaps with these three voices that we identified with the IPOR framework.

Lisa Young: So, that gives you much better, larger context for what's happening at your organization.

Doug Gray: Exactly. And another thing to keep in mind too is the information has to go to a particular stakeholder. So, while you're collecting this information, always keep an eye out for who it is that you're going to be advising or enabling with this information.

Somebody in the C suite, for instance, your chief information security officer (CISO), your chief risk manager (CRO), they're going to have one set of-- they're going to have one way of looking at the information. And they'll make decisions in one particular way. Whereas, a technician who might managing your firewalls or intrusion protection systems will have a different way of taking information, may have different needs. So, keep an eye out for that as you're developing this and try to think about who the stakeholder's going to be before you start.

Lisa Young: Okay. All right, that's good advice. So, then can you tell us where can our listeners learn more about IPOR?

Doug Gray: Well, the first place, of course, is the special report which is posted on the SEI website. We've also competed a webinar just recently. And the links for both of those sources of information are on the site for this particular podcast. And the blog entries that you'd mentioned previously, those links are also on this page for the podcast as well.

Lisa Young: Okay, perfect. So, for our listeners, all that information will be in the show notes for you. So, Doug, anything else you want to tell our listeners before we close for the day?

Doug Gray: The last point I'd like to make is this is a brand new framework. And one of the things that we would like is we would like feedback on this. It is a concept. But we'd like to hear how you implemented it. And we'd like to hear the challenges and the success stories that you had in implementing this so we can progress this to make it an even better model.

Lisa Young: Okay, great. All right, well thank you Doug. I appreciate your time. And thank you for being here today.

Doug Gray: Thank you, Lisa.