Intelligence Preparation for Operational Resilience (IPOR)

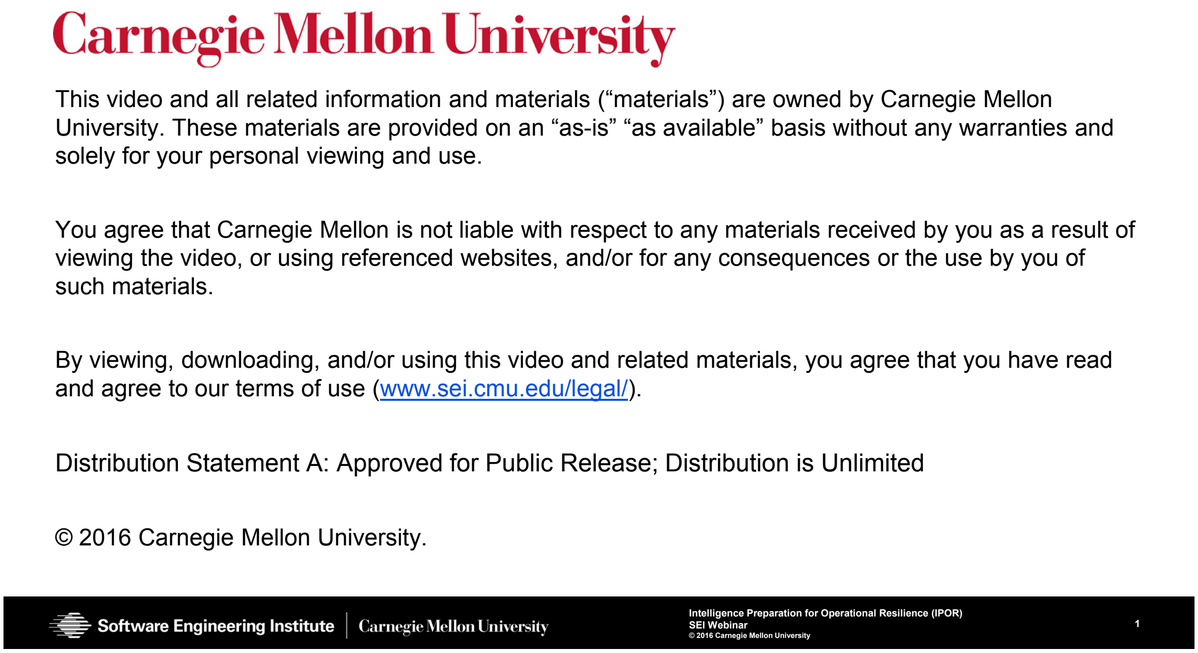
Table of Contents

SEI WEBINAR SERIES | Keeping you informed of the latest solutions

SEI WEBINAR SERIES | Keeping you informed of the latest solutions

#SEIwebinar

Carnegie Mellon University



Carnegie Mellon University

This video and all related information and materials ("materials") are owned by Carnegie Mellon University. These materials are provided on an "as-is" "as available" basis without any warranties and solely for your personal viewing and use.

You agree that Carnegie Mellon is not liable with respect to any materials received by you as a result of viewing the video, or using referenced websites, and/or for any consequences or the use by you of such materials.

By viewing, downloading, and/or using this video and related materials, you agree that you have read and agree to our terms of use (www.sei.cmu.edu/legal/).

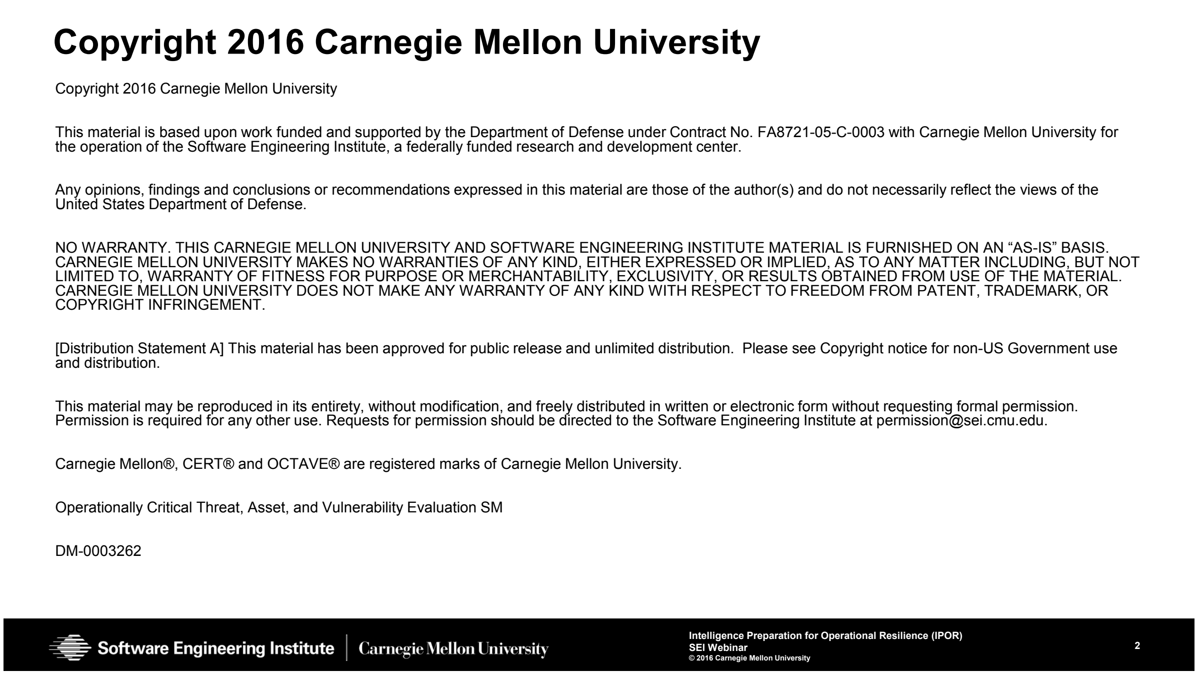
Distribution Statement A: Approved for Public Release; Distribution is Unlimited

Software Engineering Institute | Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

1

Copyright 2016 Carnegie Mellon University



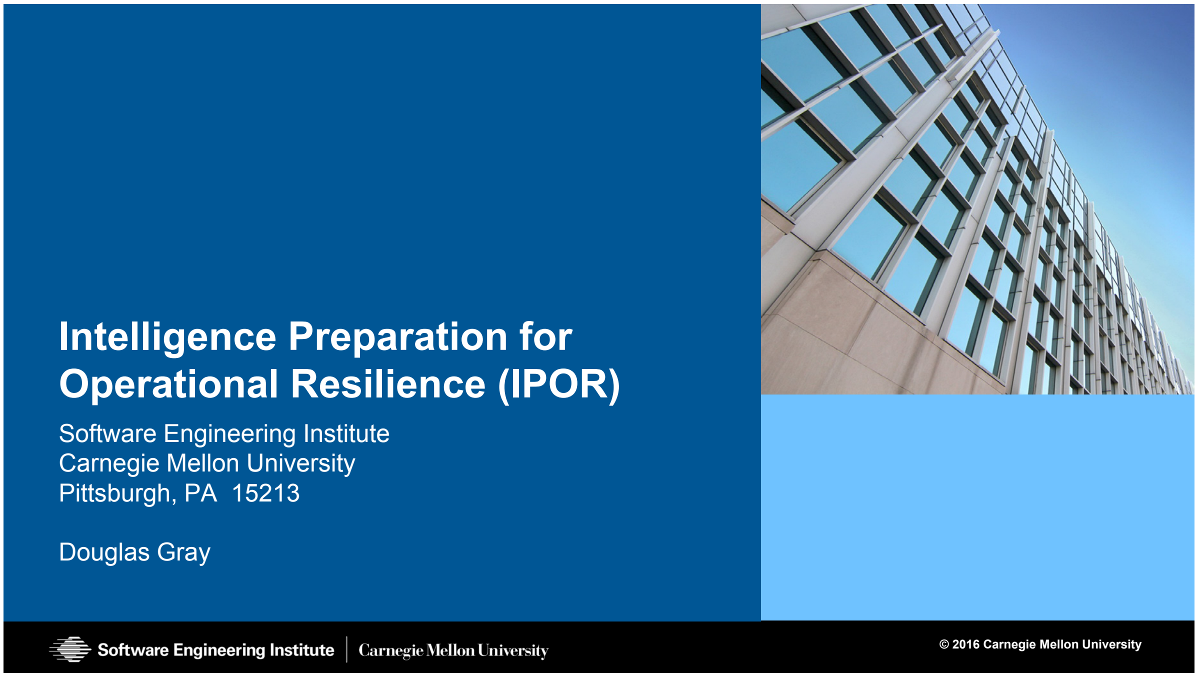
Copyright 2016 Carnegie Mellon University

Software Engineering Institute | Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

2

Intelligence Preparation for Operational Resilience (IPOR)



Intelligence Preparation for Operational Resilience (IPOR)

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Douglas Gray

Software Engineering Institute | Carnegie Mellon University

© 2016 Carnegie Mellon University

**003 Shane McGraw: And hello from the campus of Carnegie Mellon University, in Pittsburgh, Pennsylvania. We welcome you to the Software Engineering Institute's webinar series. Our presentation today is Intelligence Preparation for Operational Resilience, or IPOR. Depending on your location, we wish you a good morning, a good afternoon or good evening.

My name is Shane McGraw. I'll be your moderator for today's presentation, and I'd like to thank you for attending. We want to make today as interactive as possible, so we will address questions throughout the presentation and again at the end of the presentation. And you can submit your questions at any time to our event staff within the Q&A widget on your control panel. Just type in your question and click Send. We will also ask a few polling questions throughout the presentation. They will appear as a popup window on your screen. In fact, the first polling question I'm going to launch now is asking how you heard of today's event.

Another three tabs I'd like to point out are the Download Materials, Twitter and Survey tabs. The Download Materials tab has a PDF copy of the presentation slides there now, along with other cyberintelligence and resilience-related work from the CERT Division at the SEI. For those of you using Twitter, be sure to follow @SEInews and use the hashtag #SEIwebinar.

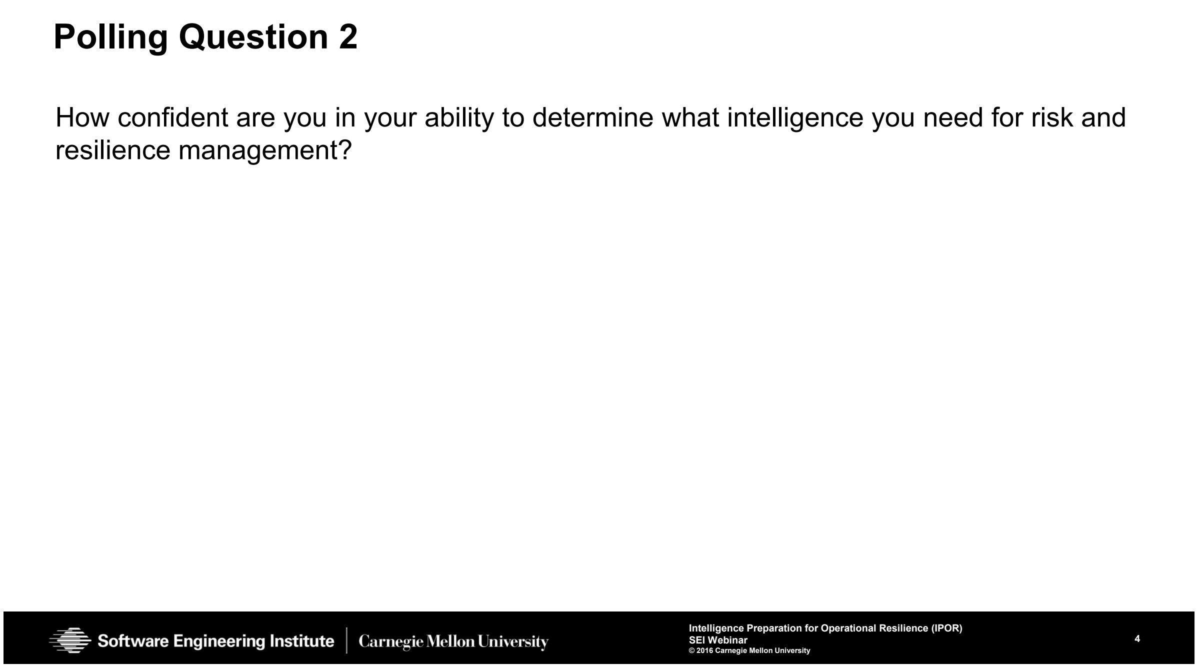
Now I'd like to introduce our presenter for today. Douglas Gray is an information security engineer within the CERT Division of the SEI, an expert in risk and resilience management. Doug is a former Army Senior Officer with 23 years of organizational leadership experience, 112 years in IT leadership, and 7 years in cybersecurity leadership. Doug has lead projects in data-driven cybersecurity governance, information security, continuous monitoring, mobile security, e-mail gateway security, and integration of intelligence into risk-resilience and project management.

In 2012, Doug led the U.S. Army Command and Control Support Agency to earn recognition as runner-up for the National Security Agency's prestigious Rowlett Award, which recognizes outstanding organizational excellence in the field of information systems security.

And now I'd like to turn it over to Douglas Gray. Doug, welcome. All yours.

Douglas Gray: Thank you, Shane. And welcome, everybody. So as Shane pointed out, we'd like to talk to you about a brand-new framework that we've developed here at the SEI called Intelligence Preparation for Operational Resilience, or IPOR. Now, this framework is geared towards operational resilience practitioners. People like chief information security officers, chief risk officers, risk managers, information system security officers, and authorizing officials. So what we're not going to be doing today is we're not going to be getting into the intelligence analysis and collection portion of this. We actually, there's some great work that we'd like to point out from our emerging tech center. Jay McAllister and their intel consortium has a lot of great information on that area. What we'd like to talk about is a framework that's intended to bridge the gap between all of the great work done in intelligence collection [and] analysis and the process of actually analyzing [and] mitigating risks and ensuring success at the point of execution.

Polling Question 2



Polling Question 2

How confident are you in your ability to determine what intelligence you need for risk and resilience management?

Software Engineering Institute | Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

4

**004 Shane McGraw: Okay. So we're going to launch another polling question here, folks. And we'd like to know, "How confident are you in your ability to determine what intelligence you need for risk and resilience management?" So we'll give you about 10 or 15 seconds to vote on that, and while we're doing that, Doug, I'd like to ask you just what's the genesis of this or where did the need come from that you ran into?

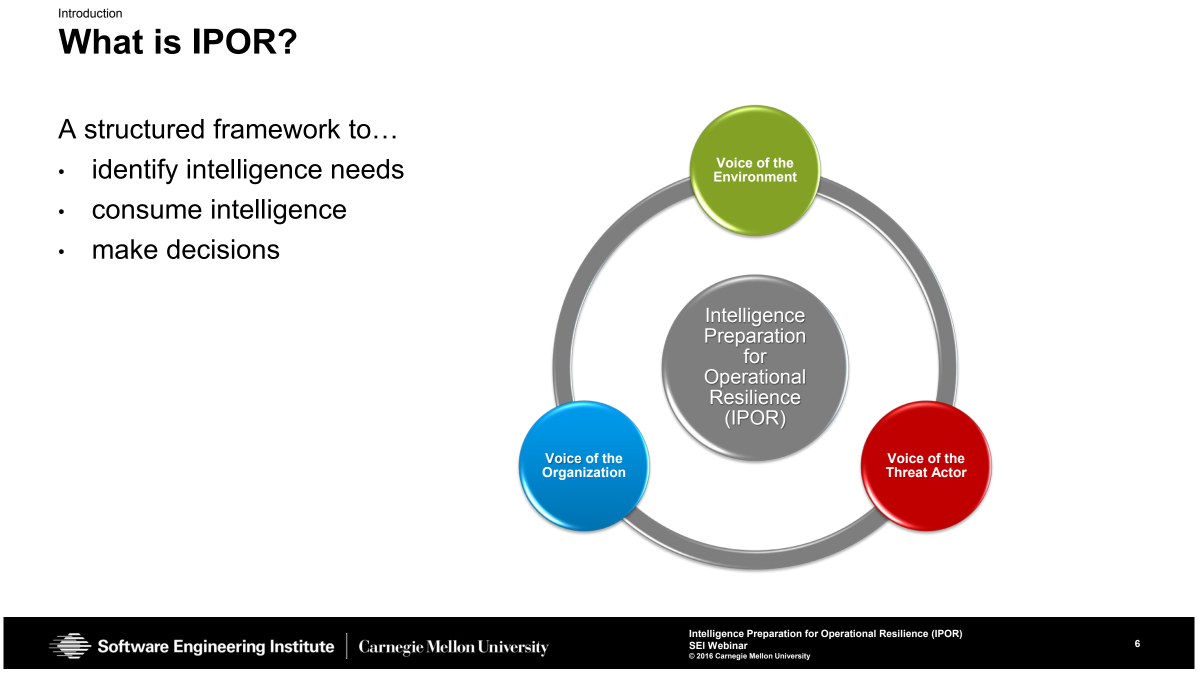
Douglas Gray: Well, that's a great question. The very specific genesis of this idea actually came from a conversation that I'd had with a government client of mine. I had made the observation that this client did an excellent job of identifying and executing off of compliance-related requirements: OMB memos, executive orders. They had very mature project management processes. They were, you know, they were very enthusiastic about implementing CMMI for services, for instance. But one of the observations I made to this particular client was, you know, "The one thing I don't hear involved in the conversation about what our priorities are is what is the threat actor doing?" And my client asked me point blank, "Okay, Doug. So how would we do that?" So it kind of set off a kind of a journey as to, "Well, how would we do that? How would we enable information system security managers, operational resilience practitioners, from all walks of life?" Not just those with an intelligence background, not just those with a national security background. What would enable them to be able to do this kind of analysis of, "Well, what intelligence do we need and how do we use it once we have it?"

Shane McGraw: Okay. Okay. So just to wrap up the polling question here, we had 10 percent with "Very confident," 65 percent with "Somewhat confident," and 25 percent with "Not at all." So I'm assuming you'll be able to speak to each audience here today.

Douglas Gray: Well, that's fantastic. Because one of the things that we tried to do with IPOR was we tried to make something which could be useful for organizations of all stripes: larger organizations, small organizations, ones with a very mature resilience management background and ones maybe trying to step up the ladder somewhat. So that's really great to hear.

Shane McGraw: Right.

What is IPOR



Introduction

What is IPOR?

A structured framework to…

- identify intelligence needs
- consume intelligence
- make decisions

Voice of the Environment

Intelligence Preparation for Operational Resilience (IPOR)

Voice of the Organization

Voice of the Threat Actor

Software Engineering Institute | Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

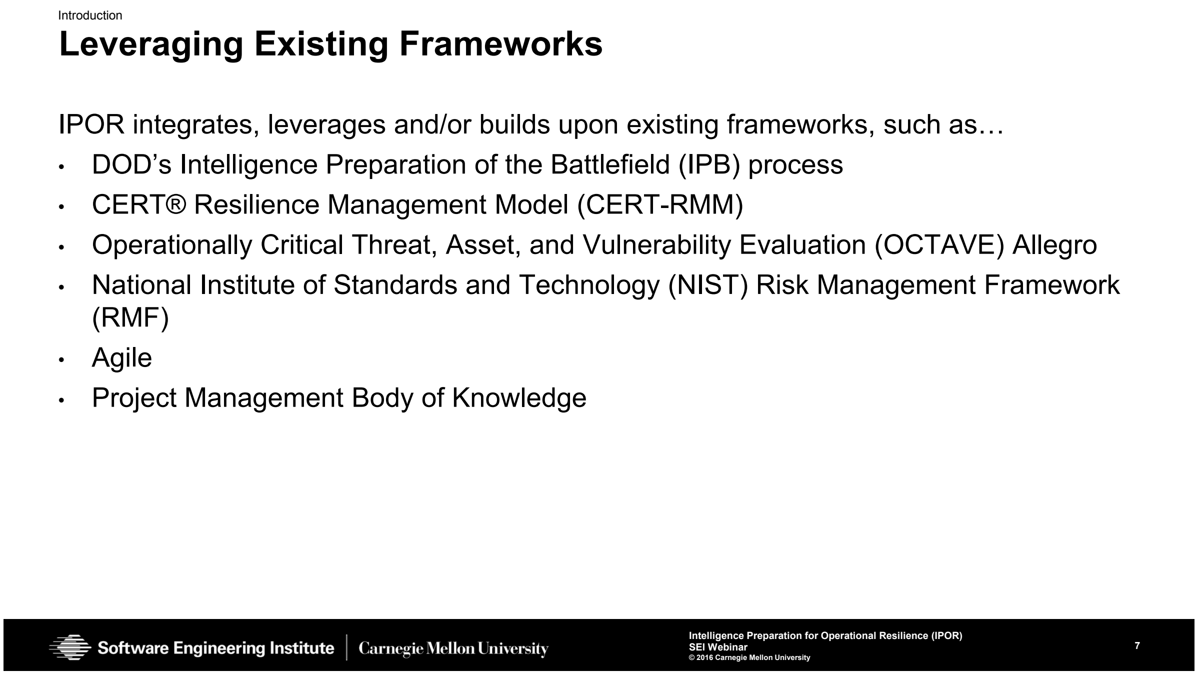
6

**006 Douglas Gray: So what is IPOR? Well, how we came about to IPOR, so one of the jumping off points to developing this idea of, "Well, how do we assess our needs for intelligence and how to we utilize it once we have it?" came from actually the military. There's a framework called Intelligence Preparation of the Battlefield or IPB, that the Army and Marine Corps specifically use as part of the Military Decision-Making Process. Any time they do any kind of operation, they do this IPB process. Even if there's not a defined expected adversary. Things like humanitarian operations, for instance, fire-fighting. They still do an IPB, because there are pieces of information like the terrain, like social, like civil-military considerations, weather. Things as esoteric as space weather. Charged particles in the atmosphere can have a negative effect on communication. That's all part of the IPB process. But one of the things that, in looking at IPB, a couple of the opportunities I saw was first of all [with] IPB, if you don't have a military planning background, it could be a little bit of a touch chew to try to be able to digest if you don't have that kind of background. It was initially designed for what's called "kinetic" operations. The military uses it for all kinds of operations to include cyber. But trying to make that translation for those without that background may be a little problematic.

Second of all, I thought that there was probably a great opportunity to really hone in and focus on operational resilience. So I started taking a look at some of the concepts and frameworks in the private sector. And one of the ones that struck out or stuck out was this concept of the voice of the customer, which is a concept in business process improvement. This idea of making sure that your customer has a voice in whatever it is that you're doing. And it reminded me of a saying in the military, which is, regardless of your military planning, the enemy always gets a vote. And so I took that idea of the voice of the customer and I extrapolated it out into what are the voices that we need to think about when we're trying to build situational awareness? And I came up with three. The first one is obviously, as we said, the enemy always gets a vote, the adversary always gets a vote. The Voice of the Threat Actor.

What are they doing? What do we need to know about the threat actor? Then there are also the environmental considerations that I alluded to in the discussion of the IPB. And I called that the Voice of the Environment. And lastly, we need to determine, well, what is it we're trying to defend? We need to kind of go on a journey of self-discovery and identify those things about our organization and the organizations that we're trying to defend and determine what pieces of information do we need to know about that? So I called that the Voice of the Organization.

Leveraging Existing Frameworks



Introduction

Leveraging Existing Frameworks

IPOR integrates, leverages and/or builds upon existing frameworks, such as…

- DOD's Intelligence Preparation of the Battlefield (IPB) process
- CERT® Resilience Management Model (CERT-RMM)
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Allegro
- National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)
- Agile
- Project Management Body of Knowledge

Software Engineering Institute | Carnegie Mellon University

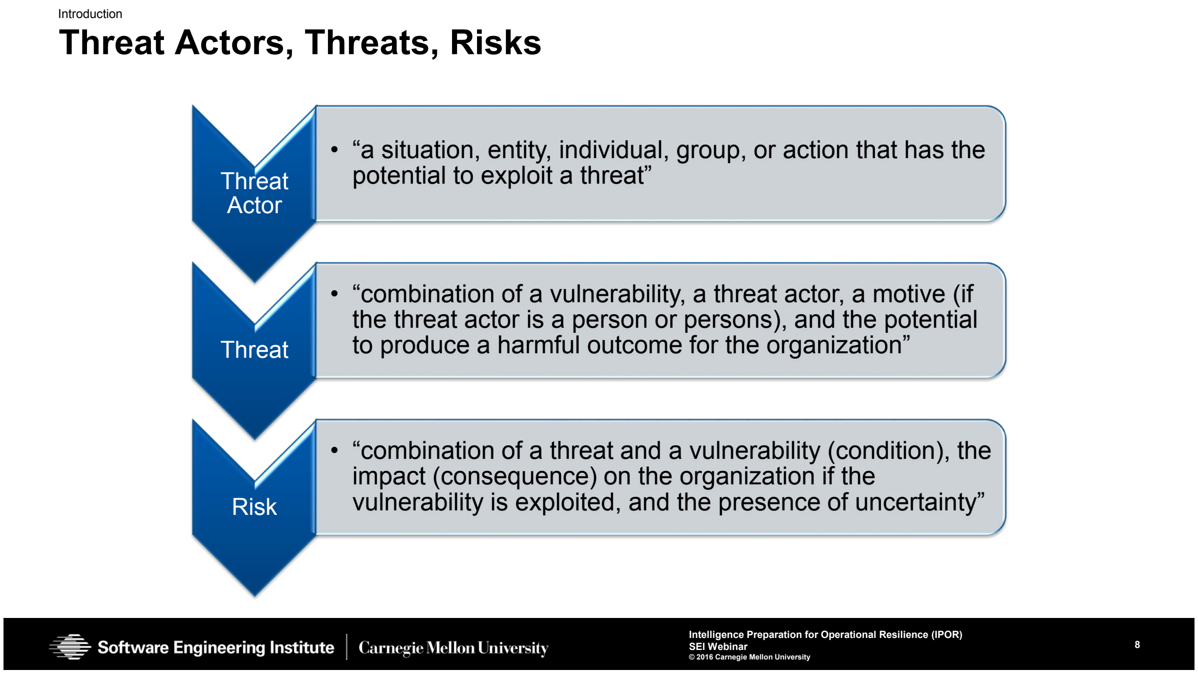
Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

7

**007 So we talked a bit about the role of IPB as inspiration. Another key piece of information is our own CERT(r) Resilience Management Model. As you'll see later on in this presentation, it's actually the primary driver for the Voice of the Organization. But moreso than that, we didn't want to create yet another framework. Information security professionals, cybersecurity professionals of all stripes, have to already deal with so many different frameworks out there. We wanted to create something that filled the need while not creating a competing framework that somebody had to use or make a choice to use between it and something else. We wanted it to work with other frameworks.

So what we did was we looked at some risk-management frameworks, and found places where this IPOR framework would plug in to be able to answer certain questions, certain information needs. So obviously as a start, CERT-RMM was, of course, near and dear to our hearts, but we also looked at OCTAVE Allegro, which is a risk management methodology also that we're custodians for. And of course, anybody who does any kind of business with the government at some point in time comes across the NIST Risk Management Framework, outlined by NIST Special Publications 800-37 and 800-39. We felt that it's very important to be able to take this kind of analysis and plug it into what has to be done in the NIST Risk Management Framework. And lastly, we saw the need to make sure that after all this analysis, after all this risk management, that we actually support success at the point of execution. So we looked at a couple of project-management methodologies, Agile and the Project Management Body of Knowledge, which is developed and run by the Project Management Institute. So we could take the output of risk management and show how you can achieve success at the point of execution through disciplined project management.

Threat Actors, Threats, Risks



Introduction

Threat Actors, Threats, Risks

Threat Actor

- "a situation, entity, individual, group, or action that has the potential to exploit a threat"

Threat

- "combination of a vulnerability, a threat actor, a motive (if the threat actor is a person or persons), and the potential to produce a harmful outcome for the organization"

Risk

- "combination of a threat and a vulnerability (condition), the impact (consequence) on the organization if the vulnerability is exploited, and the presence of uncertainty"

Software Engineering Institute | Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

8

**008 Shane McGraw: So what kind of background do you need for IPOR, for someone listening now? You know, what's the ideal background to work in this space?

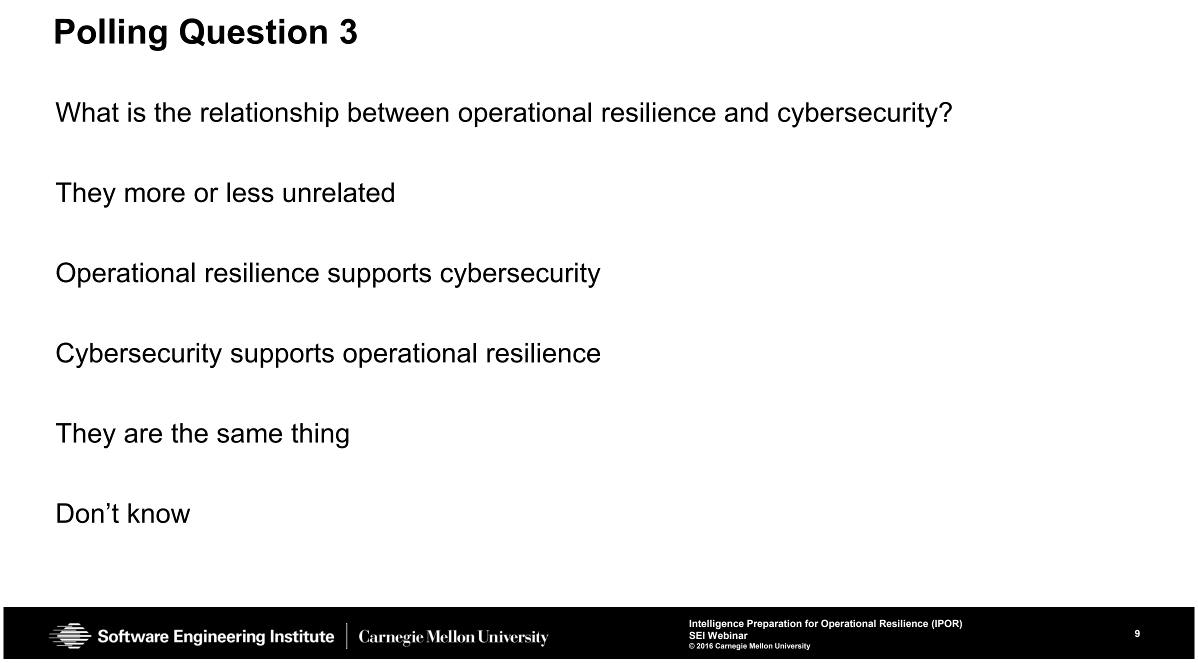
Douglas Gray: That's an excellent question. And the answer is you don't really need. The purpose of this is to not really have, you don't need to be, have, an intelligence background or a military background. You need to have a background in whatever it is that you're trying to boost the operational resilience for. That's what you need to have the background in. So as you go through the process of learning IPOR, you know, we talk a bit about, later on in the presentation, where you're building a relationship with your intelligence provider and sources. So the answer to that is if you have an intelligence analysis background, that's fantastic. But you don't need one. This is about being able to get the most out of your intelligence sources, your information sources, to build your situation awareness.

Shane McGraw: Great.

Douglas Gray: So before we go forward, so some definition-setting is probably in order. So there are obviously multiple different definitions of what is a threat, what is a vulnerability, what is a risk? And we offer these three definitions, not before we believe any of the other definitions are wrong, but simply these are the definitions that we work with here at the CERT(r) Division of the Software Engineering Institute. And they work kind of as a Russian doll. They kind of nest within each other. And the first concept is this idea of a threat actor. That's the active component of a risk. It could be a person or a group. It could also be a condition such as a hurricane or such as an earthquake or maybe even civil unrest.

When we take threat actor and then we add to it a vulnerability and a motive to that threat actor, then we get threat. So if you use the NIST paradigm, threat probably looks a lot like what NIST would define a risk to be. But we call that a threat. And we introduce the idea of the potential for a harmful outcome for the organization. And finally, we get into risk. And once we get into risk, we're adding actual consequence. The actual potential for a negative consequence on the organization and the presence of uncertainty. So essentially what we do is we start from threat actor, we add different components, working our way through threat to get to risk. Again, this doesn't mean that any other definitions are wrong. These are just the definitions that we're going to work with for the purposes of this conversation.

Polling Question 3



Polling Question 3

What is the relationship between operational resilience and cybersecurity?

They more or less unrelated

Operational resilience supports cybersecurity

Cybersecurity supports operational resilience

They are the same thing

Don’t know

Software Engineering Institute | Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

9

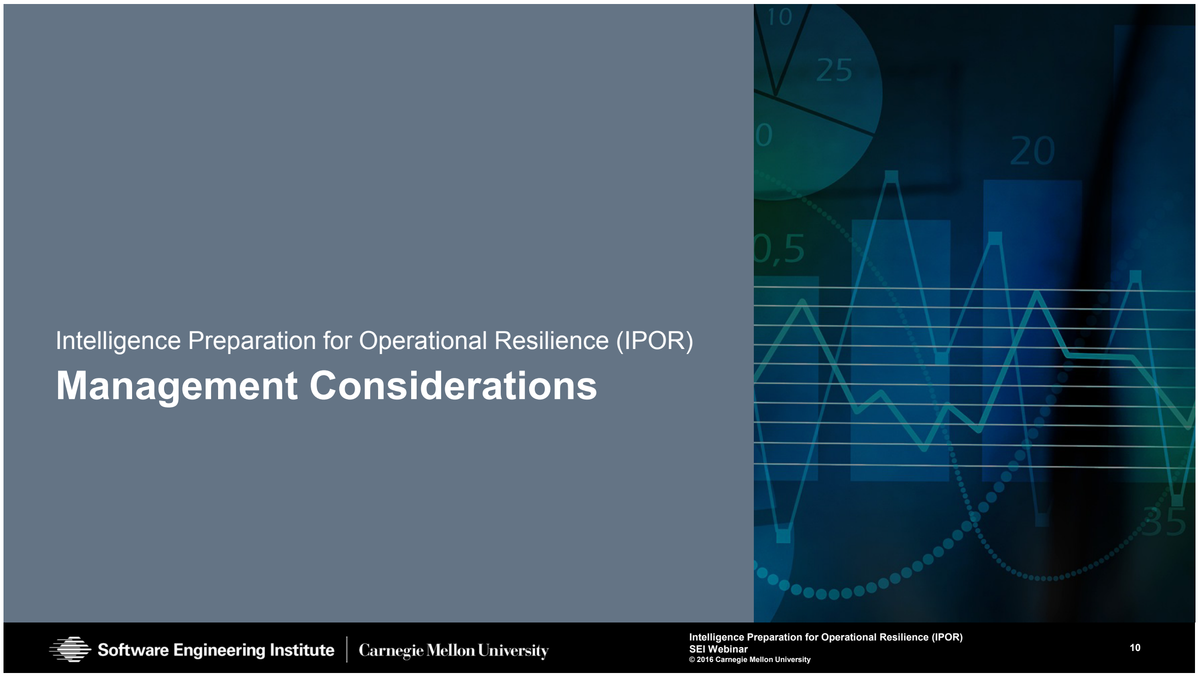
*009 Shane McGraw: Okay. So we're going to launch our third polling question here now. It should be on your screen now. We'd like to know, "What is the relationship between operational resilience and cybersecurity?" Do you consider them more or less unrelated, operational resilience supports cybersecurity, cybersecurity supports operational resilience? Option four, they have the same thing, or five, "Don't know." So we'll give you about another 10 seconds to vote here. And let's take a look at the results here now. Oops. Just pose it again. Let me hit Preview. Okay. So we got 26 percent says, "Operational resilience support cybersecurity;" 62 percent says, "Cybersecurity support operational resilience;" 5 percent saying they're the same thing; and 8 percent "Not sure."

Douglas Gray: Okay.

Shane McGraw: Any surprises there?

Douglas Gray: No. That's actually fantastic. And it's a bit of a trick question, because the boundaries between operational resilience and cybersecurity are rather squishy. So what we're going to deal with, although we're going to mention cybersecurity because that's near and dear to a lot of our hearts, obviously, but we're going to talk mainly about operational resilience--

IPOR Management Considerations



Intelligence Preparation for Operational Resilience (IPOR)

Management Considerations

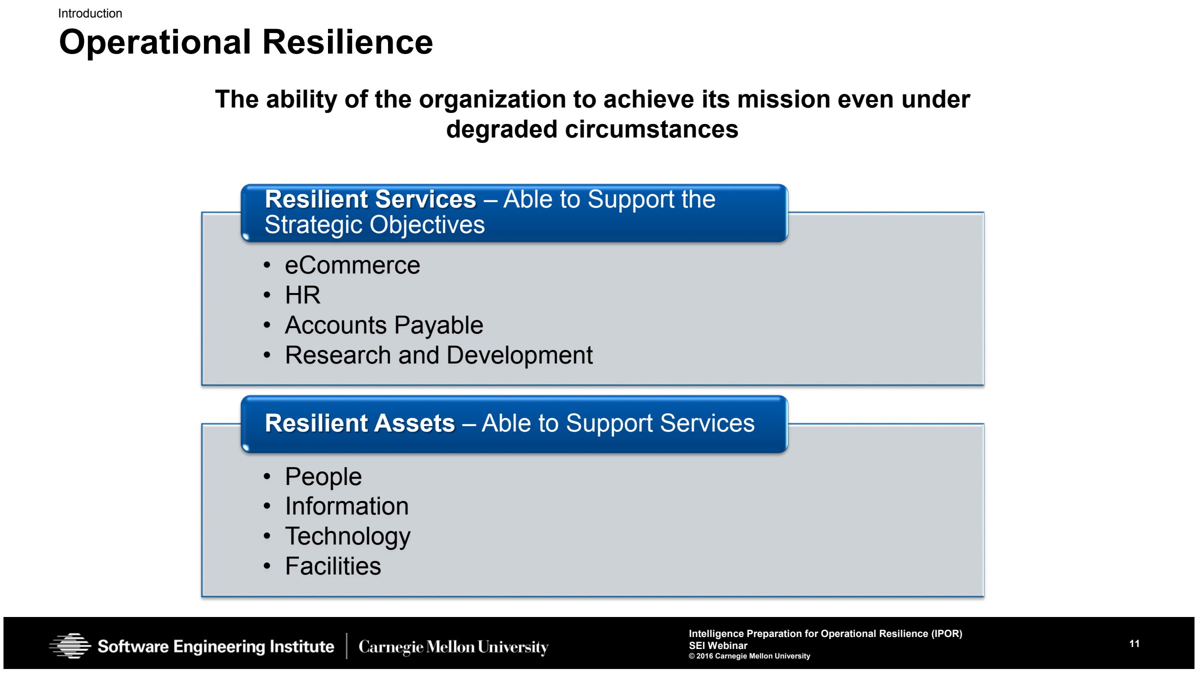
Software Engineering Institute | Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

10

**010 --for the remainder of this conversation. And operational resilience and the nature of it basically starts us off in our conversation about--

Operational Resilience



Introduction

Operational Resilience

The ability of the organization to achieve its mission even under degraded circumstances

Resilient Services – Able to Support the Strategic Objectives

- eCommerce
- HR
- Accounts Payable
- Research and Development

Resilient Assets – Able to Support Services

- People
- Information
- Technology
- Facilities

Software Engineering Institute | Carnegie Mellon University

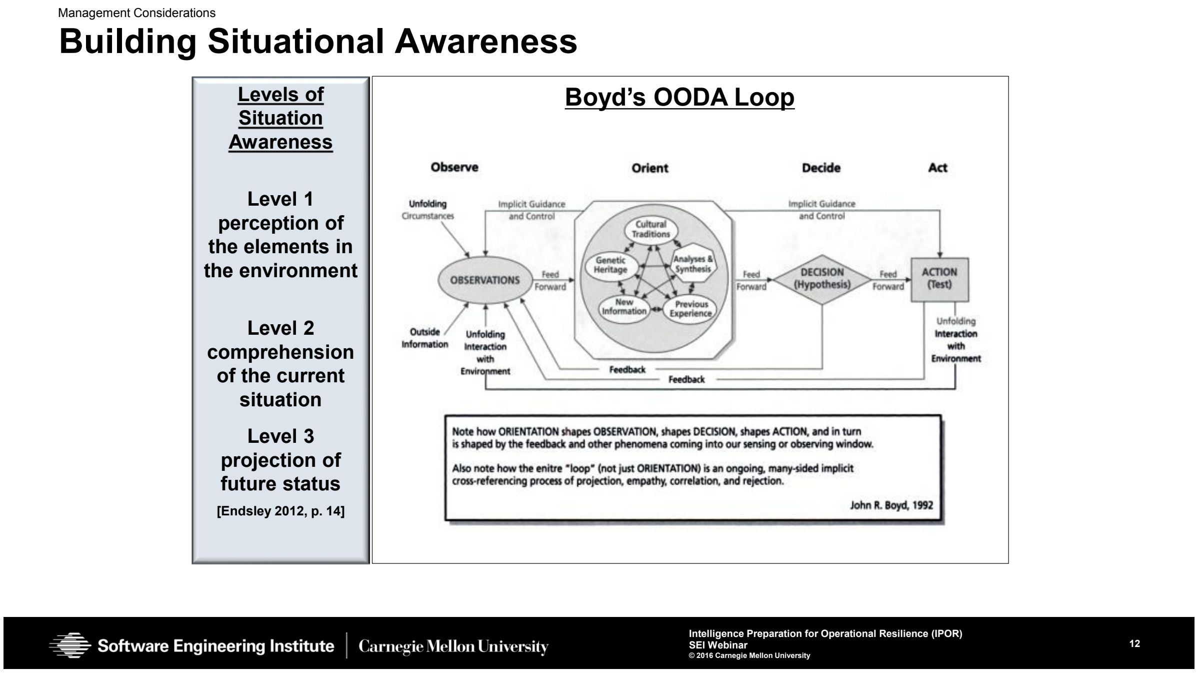
Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

11

**011 --management considerations for the IPOR. So let's talk a bit about what is operational resilience? Why do we care about it? Well, operational resilience is the ability of an organization to achieve its mission even under degraded circumstances or in times of stress. And let's face it, in today's day and age that's pretty much all of the time. Any given time we look at our circumstance as a potential time of stress, basically whether we know it or not. And the idea of resilience, we call it an "emergent property". And so we have a .edu at the end of our e-mail address, so we have to use phrases like "emergent property". Well, basically what we're saying is that resilience isn't something that you do, resilience is something that is a result of the things you do. It's like health. You don't do health; you do things to make yourself healthy. So by taking a look at this from the perspective of resilience, what we can do is we can tie our effort, all the hard work that we do, all the way back to the organization and its success or failure. And the first place we can do this is to itemize out, "Well, what are the services that our organization has to accomplish in order to achieve its mission?" And we have, you know, four examples here. But certainly the list of services are going to be custom to your organization. We do a lot of work with the federal government, wide array of different functions in the government, from law enforcement through agriculture. And each one of them has a service which is specific to them. And your organization probably has some surprises in there as well. But it's important to identify these services from a holistic perspective because it provides some connective tissue between the things that we're trying to defend and the actual success of the organization's ability to meet its strategic objectives.

So our services have to be resilient, and the services are supported by assets. And we break these down into four categories. So it's actually a definitive set of four categories of assets. And they break down into people, information, technology and facilities. Now, there's obviously overlap. People know things, they have information. Information systems will have information and they'll also have technology, but by being able to look at your assets, your people, information, technology and facilities and how they support these critical services, you're able to complete that ability to show how your defensive and your resilience building activities go back to achieve resilience for the organization as a whole.

Building Situational Awareness



Management Considerations

Building Situational Awareness

Levels of Situation Awareness

Level 1 perception of the elements in the environment

Level 2 comprehension of the current situation

Level 3 projection of future status

[Endsley 2012, p. 14]

Boyd's OODA Loop

Note how ORIENTATION shapes OBSERVATION, shapes DECISION, shapes ACTION, and in turn is shaped by the feedback and other phenomena coming into our sensing or observing window.

Also note how the enitre "loop" (not just ORIENTATION) is an ongoing, many-sided implicit cross-referencing process of projection, empathy, correlation, and rejection.

John R. Boyd, 1992

Software Engineering Institute | Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

12

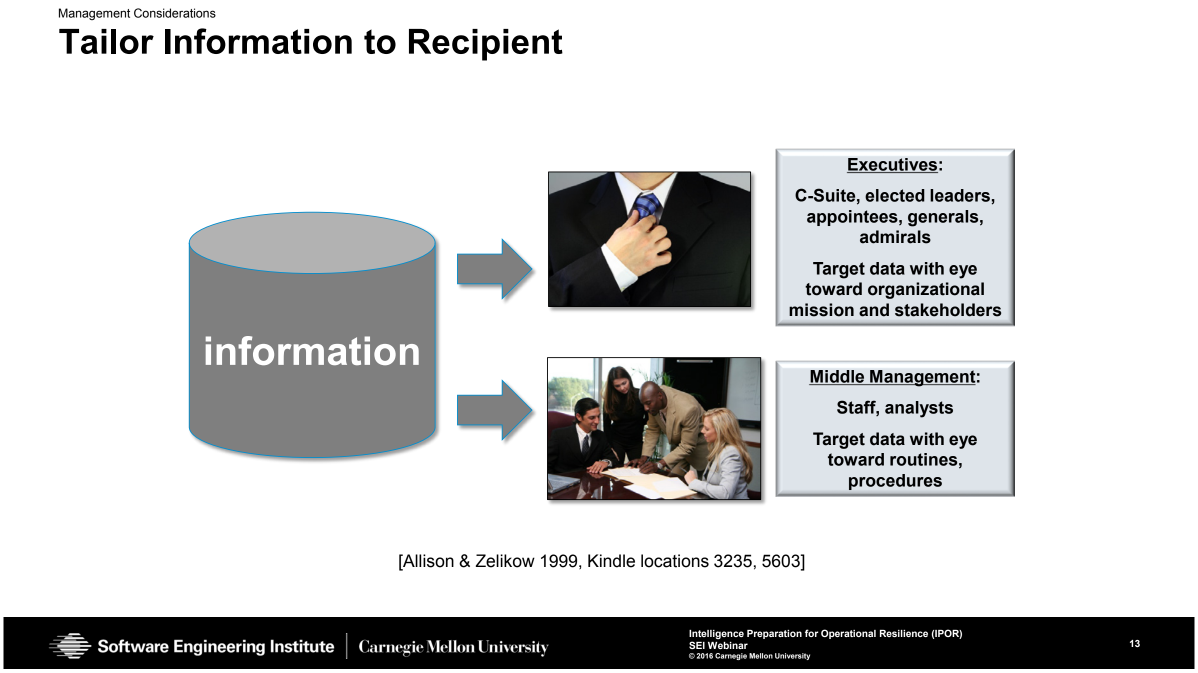
**012 So here's another piece of context that we'd like to put this in. So off to the left of your slide are some work that was done by a very famous writer in the area of situation awareness, Mica Endsley, and in situation awareness she basically categorizes three different levels of situation awareness. And these are very useful for looking at your organization, your processes, to see where you are in a given category in terms of these levels.

So Level 1 is a basic perception of your environment. I may have a chair that's sitting next to me here, and perceiving that would be a Level 1 of situation awareness. I may say I'm, you know, I'm tired and that chair is a recliner, it looks more comfortable than this chair that I'm sitting in. So my sitting in that might make me more comfortable. So that would be a Level 2. I'm actually comprehending, I'm putting it into context. In Level 3, now I'm actually thinking, "Well, if I go to this recliner next to me and sit down, I'm going to first of all step off camera," which won't make for a very good webinar. And you as the audience may consider me to be a little less than professional. So that's kind of taking the things that we know in our understanding of the situation and kind of projecting it into the future, which is really what we want to get to. We want to take the pieces of information we know today and to try to extrapolate, "Well, what does that mean for us next week, next month or next year?"

So another dimension to this is our process, is what's the lifecycle of building situation awareness? And a very good framework for this, a model for this, or basically my personal favorite, is the OODA Loop, the Observe, Orient, Decide, Act Loop. It was designed by an Air Force officer named Col. John Boyd in the '70s and '80s. He was tasked with the task, to be redundant, of trying to decide or figure out why were American fighter planes in

Korea more successful than their Chinese and North Korean counterparts? Especially since the Chinese and North Korean fighter aircraft of the day were far more capable, faster, better climb. And what he realized was that there were certain aspects of our aircraft which enabled the pilots to identify what was going on, make sense of what was going on, and then decide and act faster than their opponents. And it gave them a substantial edge even despite the differences in the aggregate capabilities of their aircraft. So he came up with this idea of this Observe, Orient, Decide and Act Loop. And as you can see from the diagram that we had up, although it's relatively sequential, there's a lot of feedback loops. Obviously how you orient has a large effect on how you observe, for instance. But it's very much focused on the idea of speed and effectiveness of your OODA Loop. And it's one of the reasons why it's actually kind of permeated outside of the military and is actually used in law school programs to help budding lawyers prepare for cases. It's about this idea of building a better OODA Loop than your adversary. So you can kind of see where that kind of fits into this idea of operation of resilience, being able to Observe, Orient, Decide and Act faster and more effectively than your adversary.

Tailor Information to Recipient



Management Considerations

Tailor Information to Recipient

information

Executives:

C-Suite, elected leaders, appointees, generals, admirals

Target data with eye toward organizational mission and stakeholders

Middle Management:

Staff, analysts

Target data with eye toward routines, procedures

[Allison & Zelikow 1999, Kindle locations 3235, 5603]

Software Engineering Institute | Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

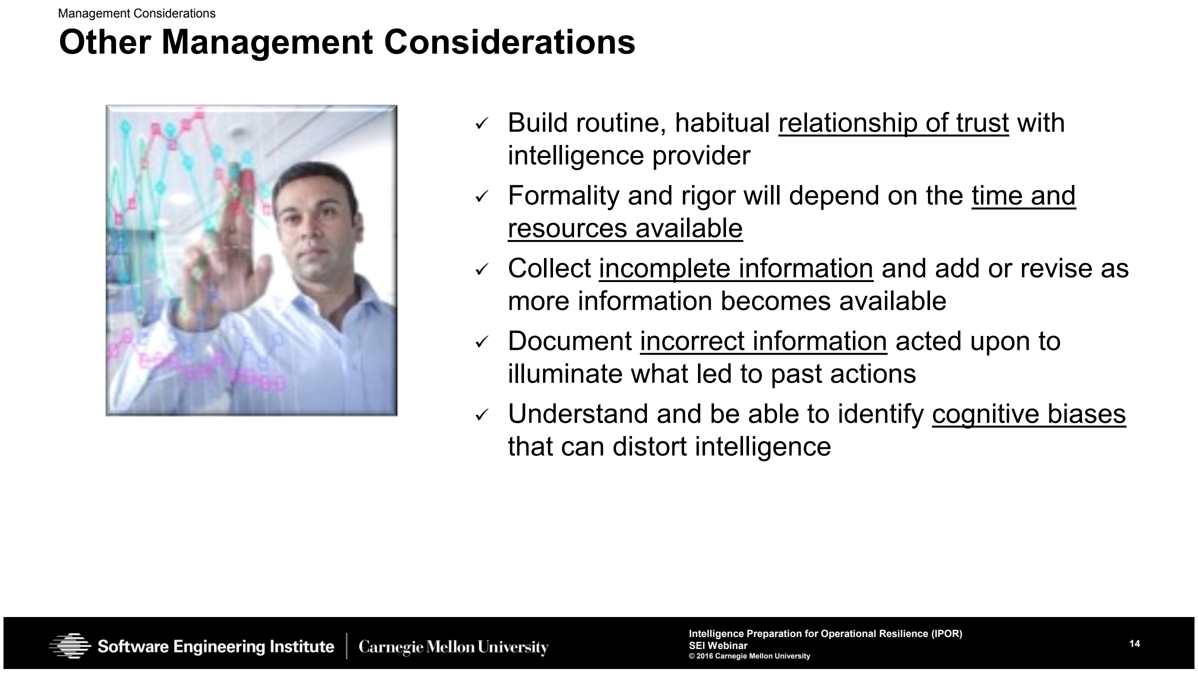
13

**013 So another kind of orthogonal piece of the IPOR framework is this idea of deciding early and throughout the process, keeping in mind, "Well, who are the recipients of this information? Who's going to be making use of it? Who will be making decisions? Who will be carrying the decisions out?" And a very descriptive source for analyzing this was a book written by writers Graham Allison and Philip Zelikow in 1999 entitled "The Essence of Decision: Explaining the Cuban Missile Crisis." And what they did was they looked at the decisions that Soviet Russia and the United States made in that conflict and tried to figure out, "Well, why did they make those decisions?" And what they realized was by looking through what we normally look at history through, the Rational Actor Model, this whole idea that groups and organizations and the individuals in them will act kind of in this kind of Borg-like, collective way is really quite not as accurate as it could be. So you take the idea of Russia putting missiles into Cuba and you may say, "Well, what were they trying to achieve? Look. They didn't even camouflage them, so obviously they were trying to provoke something with the United States." So what they did was they took a look at the actual actors and there were a couple of behavioral models that came out. And the first one was called the Governmental Politics Model.

They looked at the executives. And so for us this would be your C Suite, your elected leaders, your political appointees, your generals and admirals in the military. And what they determined was that your executives, your people who work at this, at this strata, generally tend to make their decisions based first on their mission but also based upon their constituencies. Who did they have to answer to? And so we take a look at Khrushchev and ask, "Well, why did he put missiles in Cuba in the first place?" And one of the things that Allison and Zelikow looked at was the fact that at the time Khrushchev was in hot water with his political base because he'd cut the size of the Red Army. Putting missiles in Cuba was a way of kind of retaining or building face with his political base. So then you look at, "Well, how do the rest of the organization, your middle management, your analysts, your technicians, so how do they make their decisions?" Well, let's take a look at this idea of, "Well, why didn't the Soviets camouflage the missiles when they put them into Cuba?" Well, the answer to it was that their standard operating procedures never called for it. The organization, the unit that put the missiles into Cuba, had always only set up missiles in Soviet Russia. There was no call to camouflage them.

So when they brought their procedures and processes to Cuba, they followed them. And so as a consequence, it wasn't a case where they wanted us to find them, it just wasn't in their SOP. And so in this other model called the Organizational Behavior Model, what he's saying is that those in middle management, technicians, tend to look at information and make decisions in the context of their SOPs. So your network engineer, for instance, will probably look at things in a decidedly TCP/IP kind of way and that's how they're going to approach things. If you understand the model within which people are going to take their information and make their decisions, it helps you to do better analysis up front.

Other Management Considerations



Management Considerations

Other Management Considerations

- ✓ Build routine, habitual relationship of trust with intelligence provider
- ✓ Formality and rigor will depend on the time and resources available
- ✓ Collect incomplete information and add or revise as more information becomes available
- ✓ Document incorrect information acted upon to illuminate what led to past actions
- ✓ Understand and be able to identify cognitive biases that can distort intelligence

Software Engineering Institute | Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

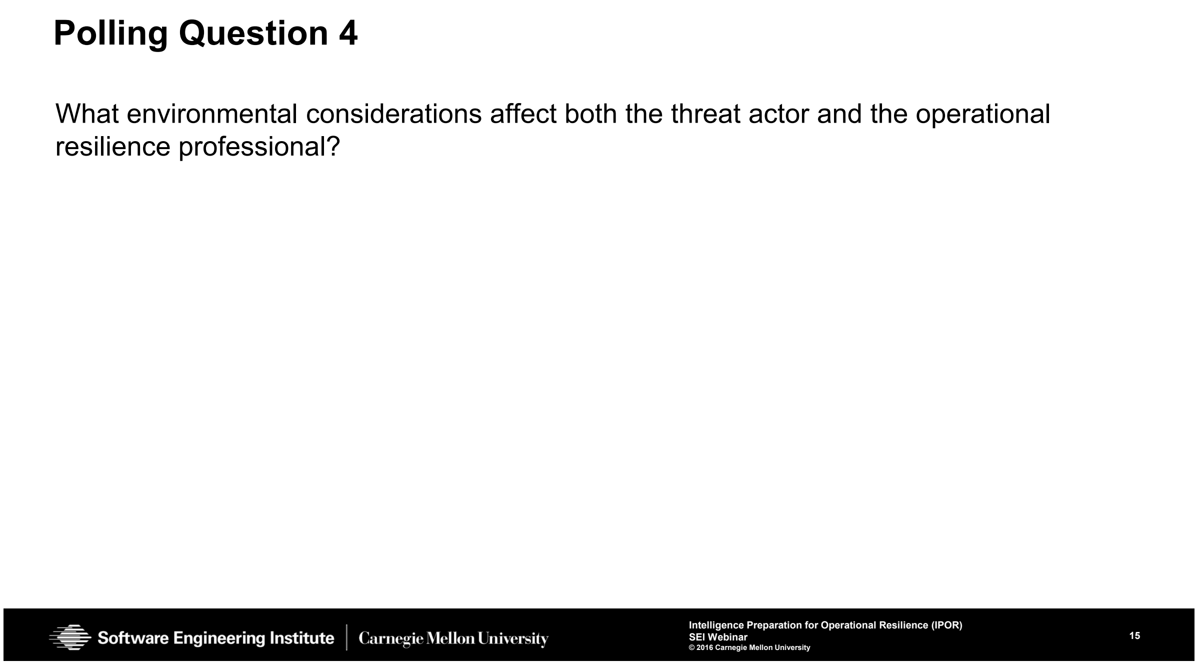
14

**014 So a few other management considerations. So we had talked with members of the intelligence community, and so one military professional who works specifically in doing IPB, stressed over and over again the need to build a routine and habitual relationship of trust with your intelligence provider. Now, as some of the polling questions have identified, there are organizations on this webinar who are large, who are small, that have a lot of resources, who have a little resources. So the idea's not so much that you have to go out and build this capability in-house. You may have it, you may not. What you want to do is you want to try to identify this source, get to know them, and find out ,how do they make their judgements, what are some of the intuitive things that's they've learned in dealing with this intelligence, and also get them to see how you make your decisions and what's important to you.

And the second bullet on this slide is very important and it's something to keep in mind throughout the entire process. And it's kind of key to this whole process. And that is the core to successful implementation of IPOR is eating the elephant one bite at a time. How formal and how rigorous you will implement this, if you decide to implement this, will be based on your time and resources available. The situation may not allow for a lot of analysis. It may be kind of a back-of-the-napkin kind of approach. And the original, so the original ancestor of this, the IPB, was actually developed to be used in time-constrained and in times when there was more, there were more time of, there was more time available to do those kinds of analysis. So don't feel that you have to do it all at once. Don't feel that you have to roll out the bright, shiny solution to do this. Do what fits to your organization.

Collecting complete information. As we show you this framework further on in the presentation, don't think that you have to have every single element of this framework filled out all at once. Collect what you have. Even if it's a planning assumption. Just annotate that it is a planning assumption and come back to it later, see if it's still valid or see if you have a fact that can replace that planning assumption. Even document incorrect information. There's a writer called Richard Hauer, who has a book on intelligence analysis. You can actually find it on the CIA website. Inside our report we actually, we reference it inside the report. And he talks about certain cognitive biases that can result in doing intelligence analysis. Well, they can also permeate in the use of intelligence as well. So if we take the incorrect information example, what he found was that even if a piece of information early on was found to be incorrect, it can actually color the decisions and analyses made further on down the road. So watch out for those cognitive biases.

Polling Question 4



Polling Question 4

What environmental considerations affect both the threat actor and the operational resilience professional?

Software Engineering Institute | Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

15

**015 Shane McGraw: Okay. We're going to launch our fourth polling question. You'll see it up on your screen now. And for this one we're just looking for you to type something into the Q&A box. It'll be within the text option there. There's no multiple choice answers. We're looking for your opinion here. "What environmental considerations affect both the threat actor and the operational resilience professional?" Well, while you're voting to that, we're going to jump into an audience question, Doug, if that's okay with you?

Douglas Gray: Absolutely.

Shane McGraw: And it's from Don asking, "On organization," back to earlier slide, "what is your working assumption on the capabilities of the integration engineering contractor charged with adopting operational resilience?"

Douglas Gray: So if I understand correctly, we're talking about integrating IPOR, and so if I understand the question correctly, and please forgive me if I'm misstating it, so the format for IPOR is whatever is best for your organization. So we're not necessarily saying it needs to be--so I'm a database guy as my background. So everything to me looks like a database, but that can be my hammer making everything look like a nail. If it works best for your organization to put it into a database, whether structured or unstructured, whatever works best for you. If it's best in maybe a regular PowerPoint slide, maybe a report, or maybe just looking at individual incidents, that's what's best for you. So however you determine to do that is important.

Just make sure that if you are having somebody integrate this into a system, make sure they understand what your needs are. And make sure they understand how you make your decisions and what's important to you. Process. So I have a saying, "Technology without good process supporting trained people is useless." It actually adds to your headaches.

Shane McGraw: Okay. So we're still waiting for some people to type in, you know, within the Q&A box, "What environmental considerations affect both the threat actor and the operations resilience professional?" so--but while we're waiting, one more question we can fit in from Steve.

Douglas Gray: That's fine.

Shane McGraw: Wanting to know, "Do you recommend organizations spend time and money in proactive efforts to deny or degrade threat actors' target system analysis efforts?

Douglas Gray: See, that's a really tough one. Because I--so I have my personal opinions. So if I understand correctly, we're basically talking about hack-back. There is a--so there's actually a point of IPOR later on in the presentation when we start getting into voice of the environment where we--and so I'm actually jumping ahead bit, where we start looking at the legal ramification, legal ramifications of what we're doing. And that's actually a piece of information that you'll need to collect. One of the things that I have found in my history of working cybersecurity is that one of the people who I find to be absolutely indispensable is the lawyer. And so my recommendation is if you're not talking with your lawyer on a regular basis, make sure that you're doing that. And even if your lawyer, your legal counsel, might not have a background in some of the cybersecurity law and case law, and when we're talking about hack-back and we're talking about degrading the threat actors' capability, we're definitely talking international law. We're talking treaties. Potentially we're talking jus ad bellum and jus in bello, which is basically the two components of law of war. If you're talking about a, you know--

Douglas Gray: Right.

Shane McGraw: --a government agency. But you definitely want to talk with your lawyer, because there are considerations that you will want to make sure that you have put into your thought process, your risk management, before doing that. Obviously nobody attacks your network, almost nobody attacks your network directly. There's usually collateral damage between you and them. So again, I hope it doesn't sound like I'm ducking the question, but I definitely have to say make sure you talk to your legal counsel and get all the ins and outs.

Shane McGraw: Great. And just to wrap up our polling question. So I'll just read off some of the answers. From Oni asking, or saying, "Environmental considerations include customer need for operational flexibility." From Joe, "Environmental considerations to us include and are not limited to the business process, or KDE that supports the business process, key data elements."

Douglas Gray: Yeah.

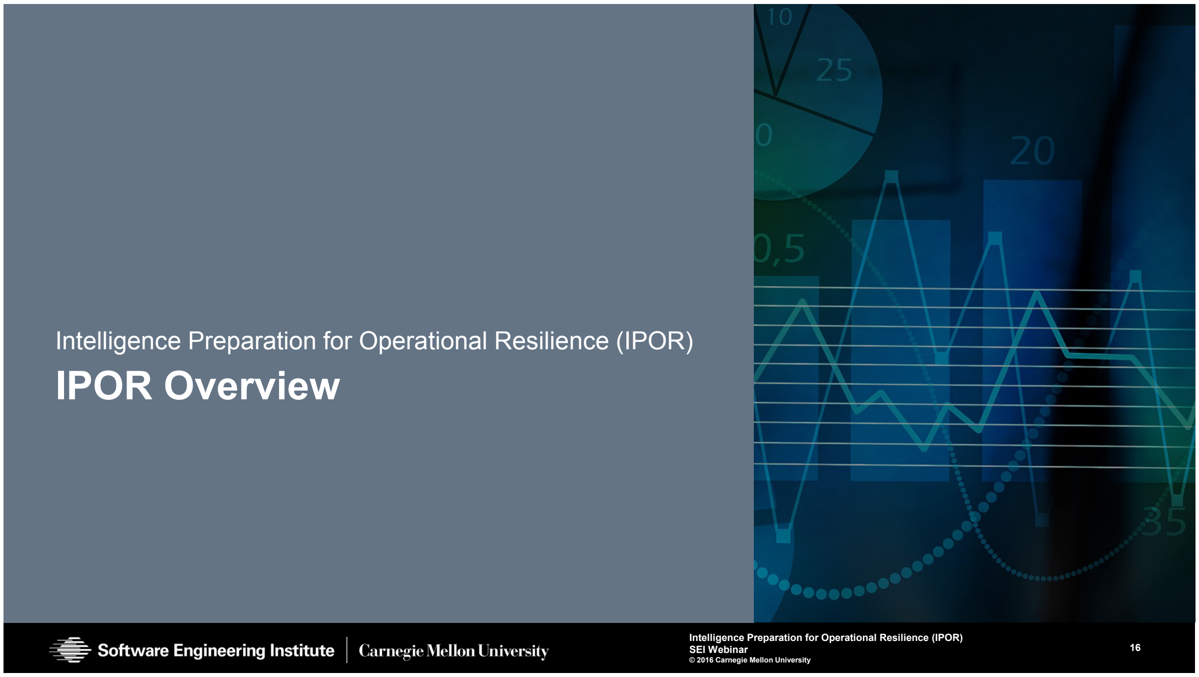
Shane McGraw: "The ability for the EEFI to be found on both sides. Or employee risk, social media, et cetera, and other similar areas." Jeffrey, "Weather." "Context and culture harmonization," from Don. Another one from another Don asking, "What is the nature of your threat surface? For example, university environment tends to be wide open verse a financial institution is more locked down." And then from James saying, "A level of personal experience, personnel experience information technology assets in use, access to intelligence." So those are good answers.

Douglas Gray: Great.

Shane McGraw: Yeah.

Douglas Gray: So those are great answers. I almost, so I almost feel like many of you actually have briefed a portion of this for me. So I appreciate you making my job easier for me. So let's go ahead--

IPOR Overview



Intelligence Preparation for Operational Resilience (IPOR)

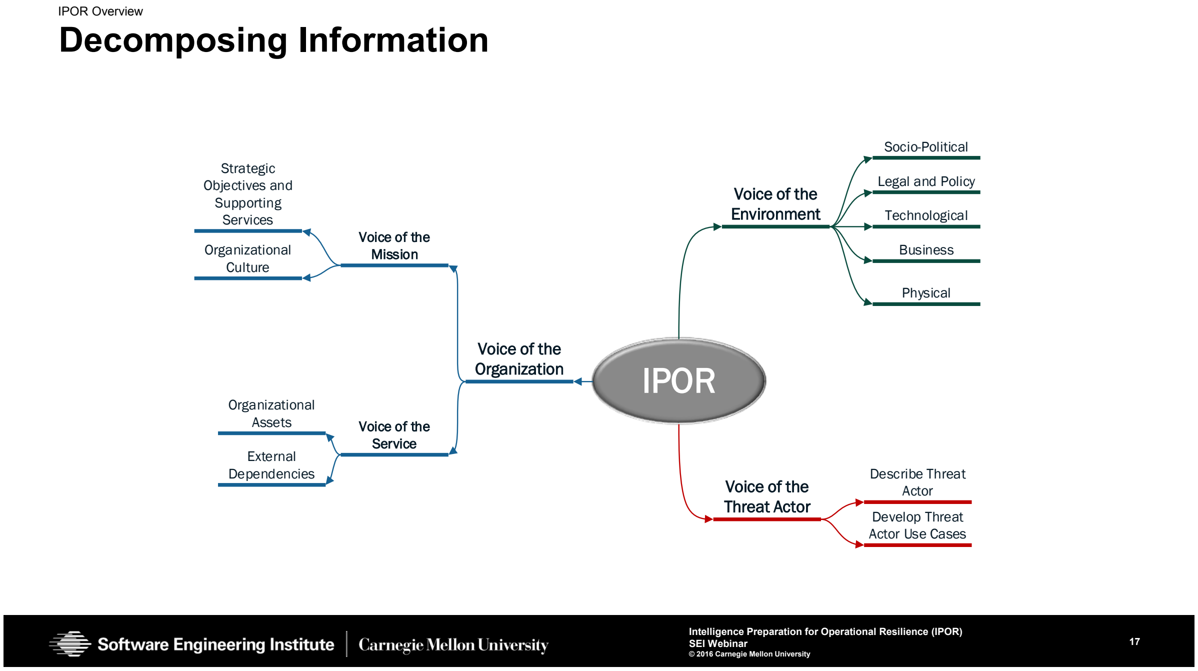
IPOR Overview

Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

16

**016 --and take a look at the
model itself.

Decomposing Information



IPOR Overview

Decomposing Information

IPOR

Voice of the Organization

Voice of the Mission

Strategic Objectives and Supporting Services

Organizational Culture

Voice of the Service

Organizational Assets

External Dependencies

Voice of the Environment

Socio-Political

Legal and Policy

Technological

Business

Physical

Voice of the Threat Actor

Describe Threat Actor

Develop Threat Actor Use Cases

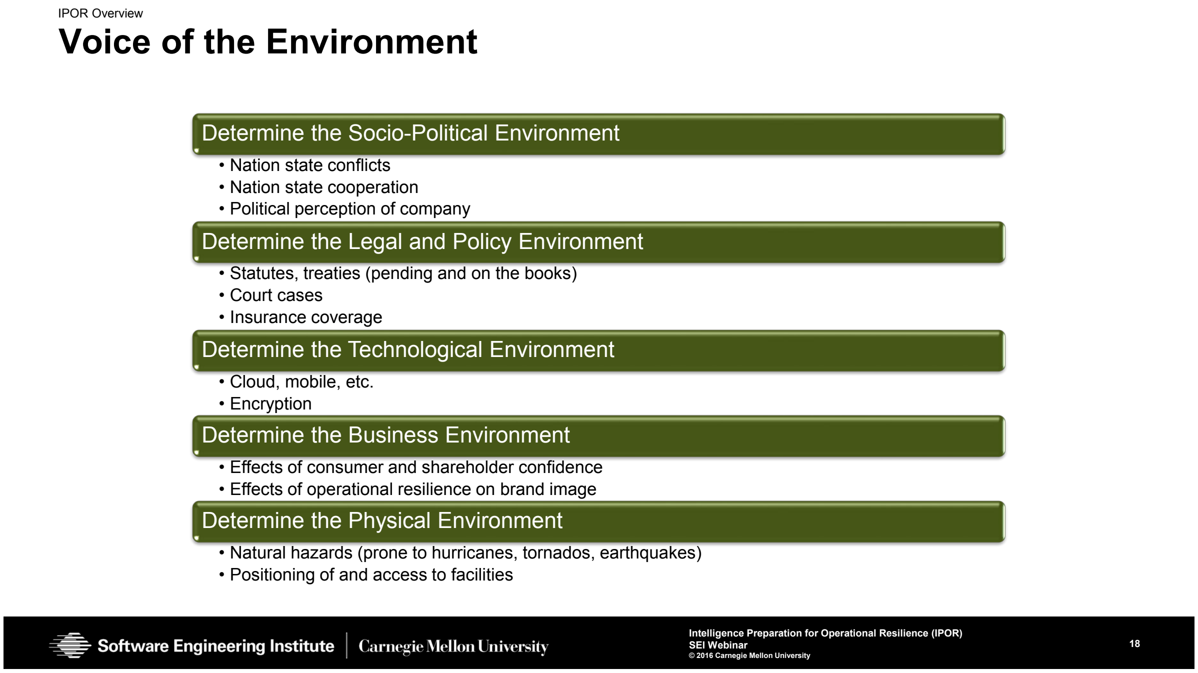
Software Engineering Institute | Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

17

**017 So here we are and we are at--so this is about the 10,000-foot level of the Intelligence Preparation for Operational Resilience Model. So remember we talked earlier about the voices. The Voice of the Environment, the Voice of the Threat Actor, and the Voice of the Organization. So what we've done is we've actually--so one of the things I'd like to point out, a question that I often get asked, if you can see this on the slide, is why are the arrows going out? Why aren't the arrows going in? Obviously they're all describing IPOR. And the answer for that is that we're talking about decomposing information. Again, you know, hitting up on that idea of eating the elephant one bite at a time. You want to take what we need to know and then decompose it into smaller bites that we can deal with more effectively. So we take things like the Voice of the Environment and we decompose them into other areas that we want to describe. If you notice, Voice of the Organization decomposes into two other subvoices that we'll get into further, a couple slides on. And then the Voice of the Threat Actor, we actually try to break down what it is that we need to know about the threat actor, and then come away with a piece of currency that we call the threat-actor use case that we're going to use for injection into risk management frameworks.

Voice of the Environment



IPOR Overview

Voice of the Environment

Determine the Socio-Political Environment

- Nation state conflicts
- Nation state cooperation
- Political perception of company

Determine the Legal and Policy Environment

- Statutes, treaties (pending and on the books)
- Court cases
- Insurance coverage

Determine the Technological Environment

- Cloud, mobile, etc.
- Encryption

Determine the Business Environment

- Effects of consumer and shareholder confidence
- Effects of operational resilience on brand image

Determine the Physical Environment

- Natural hazards (prone to hurricanes, tornados, earthquakes)
- Positioning of and access to facilities

Software Engineering Institute | Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

18

**018 So let's talk about the environment. And they were really fantastic questions, or very fantastic answers that came back from that last question. And that's why I say, you actually kind of briefed about half of about the next couple of slides.

So we're talking about the social political environment, for instance. So one example that I can point out from personal history, although I can't go into detail on it, is nation state conflicts. As we know, as two cyber-enabled nation states and more and more nation states are becoming cyber-enabled today, as conflict arises there's a cyber component to that. And we know that one of their preferred attack patterns is the distributed-denial-of-service attack. I want to take your presence off of the web. Well, what do we need for distributed denial of service attack? Well, most of the time we need a botnet. And what's a botnet but basically a large collection of latent or hidden malware on a network. And so we can actually find ourselves drawn into nation-state conflicts simply by having this latent malware on our network. We can actually become part of the attack. So keeping our eye out for what's going on in the world stage, especially between cyber-enabled actors, is helpful. We also know that certain nation states are more or less cooperative to dealing with threat actors, and that can affect the intentions and the capabilities and the willingness of threat actors. And those can change over time. Relationships with those nations can actually warm or they can degrade. And there's also the political perception of the company. The-- and again, this can change over time. We could have a fantastic political perception today. We may be a, you know, the darling of the not just regulators, but also potential threat Actors, and tomorrow a single event may happen and we may look a little less favorable to either component.

And again, we get to this idea of the legal and the policy environment. And I can't stress this enough. Statutes change, treaties change, but one are that I would like to call out is the case law. And this is why it's so important to have a routine relationship with your legal counsel. The United States and a lot of other nations, especially ones that were former British colonies work in a common-law system, which means that after the statute is put on the books, the court cases that come after become part of the body of jurisprudence.

So we'll take the Computer Frauds and Abuse Act, for instance. For cyber defenders, it is a great arrow in our quiver to be able to enforce proper use of our systems. If I--so by the letter of the CFAA, if I, say, elevate my permissions beyond what's authorized, I'm actually in violation of the CFAA. Well, here's an interesting twist. Some years ago, and again, I'm not a lawyer, and this doesn't replace advice from your legal counsel, but some years ago a couple of the federal appellate courts actually held that the CFAA was unenforceable because it was too vague. And so now things may have happened since then. So at the time, I believe this was a three-court panel of one of these jurisdictions that may have gone to the full appellate court.

I don't believe it went to the Supreme Court, but I could be wrong. But things change over time. Just because it's in the law doesn't mean that the courts are interpreting the way you think it's being interpreted. It's important to keep up relationships with your legal counsel. Also, insurance coverage is a big deal today in determining what our risk profile is. Not just how much that we are covered for but what we're covered for. What are the exceptions for that? There are a lot of--so if those of you follow Brian Krebs' column for "Krebs on Security," he does a lot of writing on banking by corporate customers in what the companies will cover, what they won't cover, what makes the, what basically makes the company's filing in the claim liable or not able to retrieve funds. So keeping up with not only what your insurance coverage is but how it's being interpreted in the courts is also important.

Technologically, the environment. So that's near and dear to a lot of our hearts. So things such as cloud, mobile, take center stage. We want to look at those from the perspective of our company or of our organization, but what we also want to do is we also want to look at the second and third-order effects of these technological conditions as well. Take cloud, for instance. We may be using cloud, we may not be using cloud. But another thing that's been written about in the security press has been that cloud has been offering, some cloud instances, not all of them, have been offering a great tool for threat actors. Why? What's cloud? It's scalable, it's on demand. So certain conditions that are out there, if we follow those trends, can allow us to see, "Well, how is our surface area changing?" And, of course, encryption algorithms. They're algorithms which were great yesterday and now they're, today, they're broken and they open us up to increased risk.

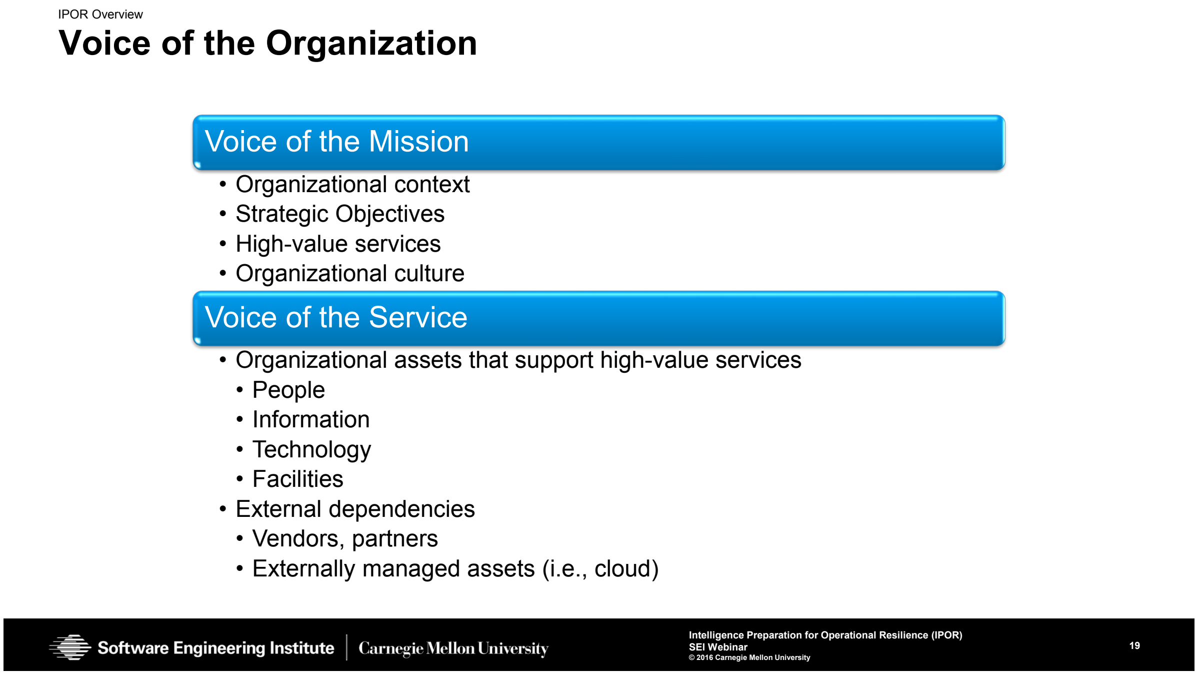
Somebody mentioned the business environment.

Shane McGray: Right.

Douglas Gray: Our customers, our stakeholders. Certainly looking at what happens to our competitors or colleagues when they have a compromise is definitely descriptive for our risk profile. And finally, the physical environment. We can't overlook the effects of weather, of civil unrest, earthquakes. So, you know, one of the examples I use is, let's say somebody, say that your company wants to build a data center in New Orleans and you may say, "Well, look at what happened in Hurricane Katrina." You know, "I won't--" you know, "Why would I do that?" Well, that's not what this framework in doing. This framework is actually about collecting information to make the risk management decisions. So in the case of that data center, you would look at, "Well, what were the risks that happened in Hurricane Katrina?"

It's a very documented use case. "What are the mitigations that have taken place since then? What are the conditions that made Katrina exceptional?" I mean, don't forget, New Orleans had had plenty of hurricanes prior to Katrina. Collect the information to make a useful risk management decision. Because after all, we have nor'easters in the Northeast, we have earthquakes in the West, we have tornadoes. Every place has their own physical threat actors. So collect your information to make a good risk management decision.

Voice of the Organization



IPOR Overview

Voice of the Organization

Voice of the Mission

- Organizational context
- Strategic Objectives
- High-value services
- Organizational culture

Voice of the Service

- Organizational assets that support high-value services
  - People
  - Information
  - Technology
  - Facilities
- External dependencies
  - Vendors, partners
  - Externally managed assets (i.e., cloud)

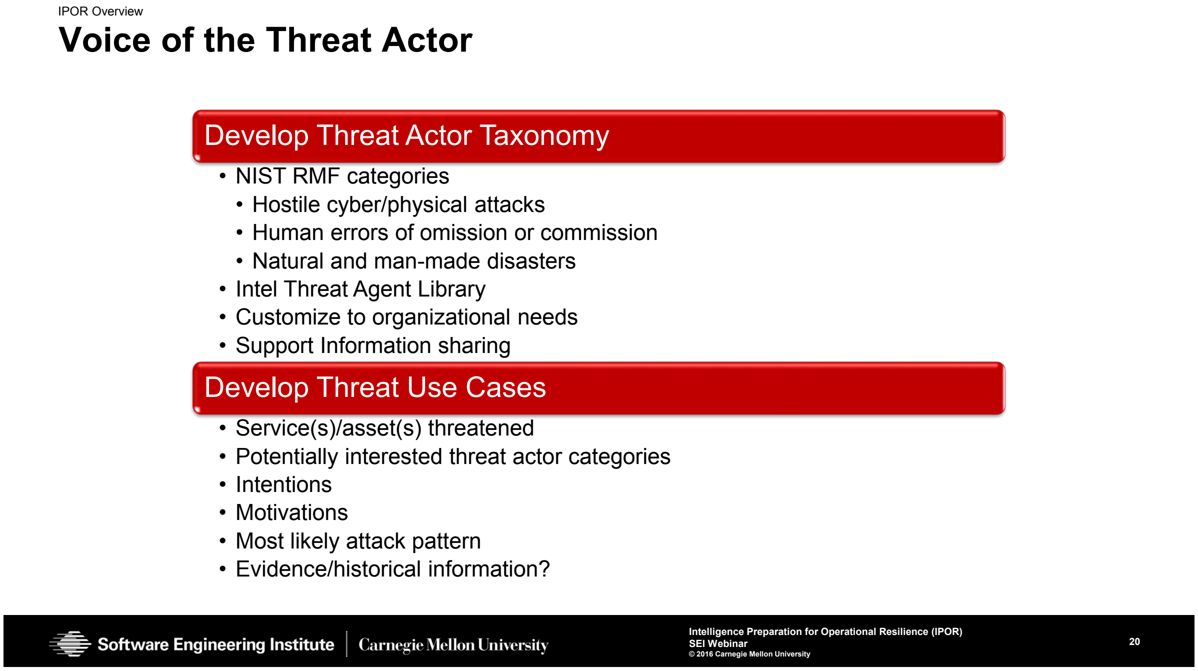
Software Engineering Institute | Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

19

**019 So now we get into that journey of discovery we're talking about, the voice of--so the Voice of the Organization. So for this I borrowed very heavily from the CERT(r) Resilience Management Model. So for those of you were looking at, who are using CERT-RMM, Voice of the Mission is very dependent upon or borrows very heavily from the Enterprise Focus process area. This is this whole idea of basically trying to decide, "Well, what are we trying to support for the company?" the strategic objectives and critical services that we're talking about before. And it also is talking about, "Well, what is our organizational culture?" Somebody mentioned that in talking about environmental factors earlier. And then in Voice of the Service we start talking about that idea of identifying those assets that we need to make resilient. That borrows very heavily from our acid definition and management process area. And finally, our external dependencies. Even if somebody else is managing it for you, you're still responsible for it. If you're a government organization, that's actually spelled out in the FISMA Act of 2014.

Voice of the Treat Actor



IPOR Overview

Voice of the Threat Actor

Develop Threat Actor Taxonomy

- NIST RMF categories
  - Hostile cyber/physical attacks
  - Human errors of omission or commission
  - Natural and man-made disasters
- Intel Threat Agent Library
- Customize to organizational needs
- Support Information sharing

Develop Threat Use Cases

- Service(s)/asset(s) threatened
- Potentially interested threat actor categories
- Intentions
- Motivations
- Most likely attack pattern
- Evidence/historical information?

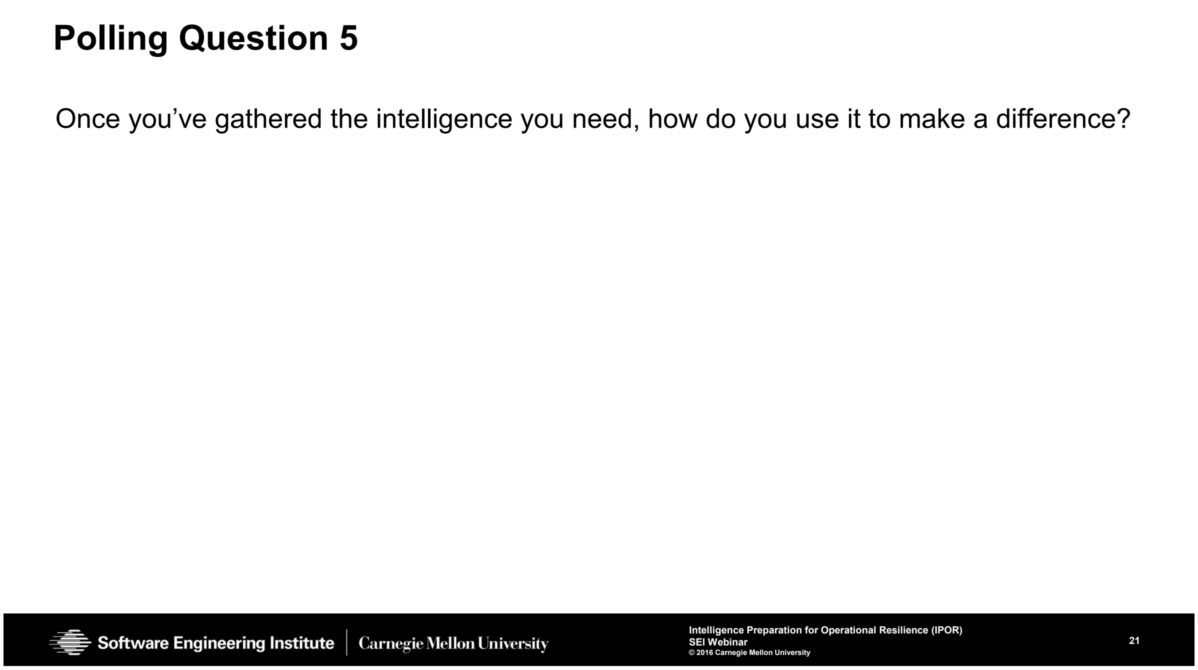
Software Engineering Institute | Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

20

**020 So now we get into the juicy, exciting part of this, which is the Voice of the Threat Actor. So the first thing we want to do is we want to take a look at--again, we want to eat the elephant one bite at a time. We want to develop a categorization for threat actors because we may not actually have intelligence that pinpoints a specific threat actor. We'd love to know it's Bob, but we--but in m any cases we're dealing with nation state actor. We may be dealing with Unit 12354 of the Krasnovian Army. Or we may actually have information on Bob. The point is, having a useful taxonomy is very important. So a couple of sources are, of course, the NIST Risk Management Framework. Intel has put out a Threat Agent Library, which offers a very good way to kind of categorize and kind of create a lexicon to help support information sharing by ensuring that if you say nation state actor I'm thinking of the same category. And finally, we want to put it all together into this commodity called the threat-actor use case. We want to tie together this, what kinds of services or assets the threat actor might be going after. The categories that we just discussed, possible intentions, motivations, prevailing attack patterns. We know what spearphishing is a big deal today, and we want to try to tie together if at all possible evidence or historical information. And this helps--

Polling Question 5



Polling Question 5

Once you've gathered the intelligence you need, how do you use it to make a difference?

Software Engineering Institute | Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

21

**021 --to facilitate information sharing.

Shane McGraw: Okay. That'll lead us to our fifth and final polling question today. And similar to the last one, we're looking for you just to type your answer into the Q&A box and we'll read them off as you're typing them in. That question is, "Once you've gathered the intelligence you need, how do you use it to make a difference?" So once again, type your question into the question and answer box. We'll read them off. The question is, "Once you've gathered the intelligence you need, how do you use it to make a difference?" And while you're doing that, just a reminder for everybody upon exiting today's webinar, we request that you fill out the survey, as your feedback is always greatly appreciated. And also a reminder, make sure you check out the Download Materials tab, where you could walk away with the report on IPOR, a copy of today's presentation slides, some other resources on cyber intelligence work from our emerging technology center, and other frameworks like the RMM and OCTAVE that Doug has mentioned throughout the webinar. So let's see what kind of responses we're getting.

So from Gary we got "mitigate risk." Let me hit a Refresh here. "Try to convince management that the security alerts are strong enough to warrant taking a device offline." "When I decompose a voice of the bad actor I get things like one, nation state; two, organization crime; three, insider threat; four, hacker." "Create TTPs to combat the possible threats." So anything else to add to that, or is that what you're looking for?

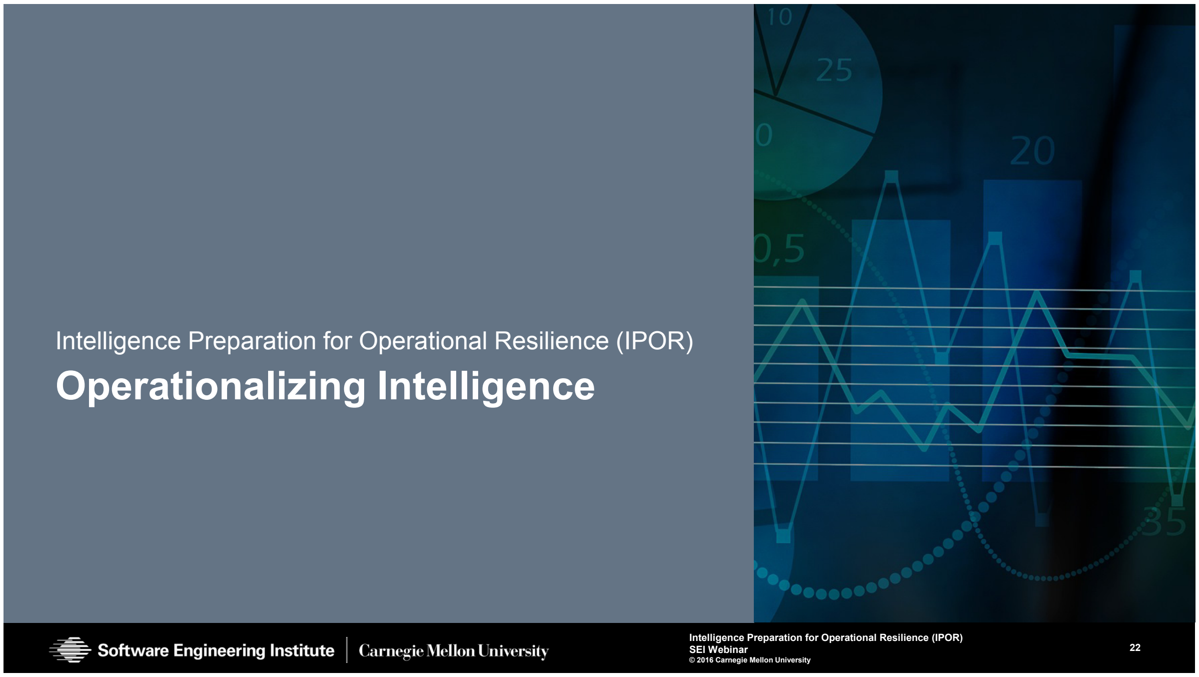
Douglas Gray: So that is fantastic. And again, it's gratifying that everybody is kind of thinking along the same lines of kind of what we're going for. So we're hoping that this is going to be very useful for you, and I'd like to take this time just to reiterate, this is a new framework. So what we're asking for is feedback. So as you're reading the report, as you're looking over the material, we'd like you to take a look at it and to tell us some areas where we may have left something out or maybe there's a way to utilize this in a--so there may be a way that the framework might be perfectly find, but there's a way to utilize it in a very specific way.
Shane McGraw: And Andrew made a good comment here of becoming a change agent for your organization. Yeah.

Douglas Gray: Absolutely.

Shane McGraw: Yeah.

Douglas Gray: Absolutely.

Operationalizing Intelligence



Intelligence Preparation for Operational Resilience (IPOR)

Operationalizing Intelligence

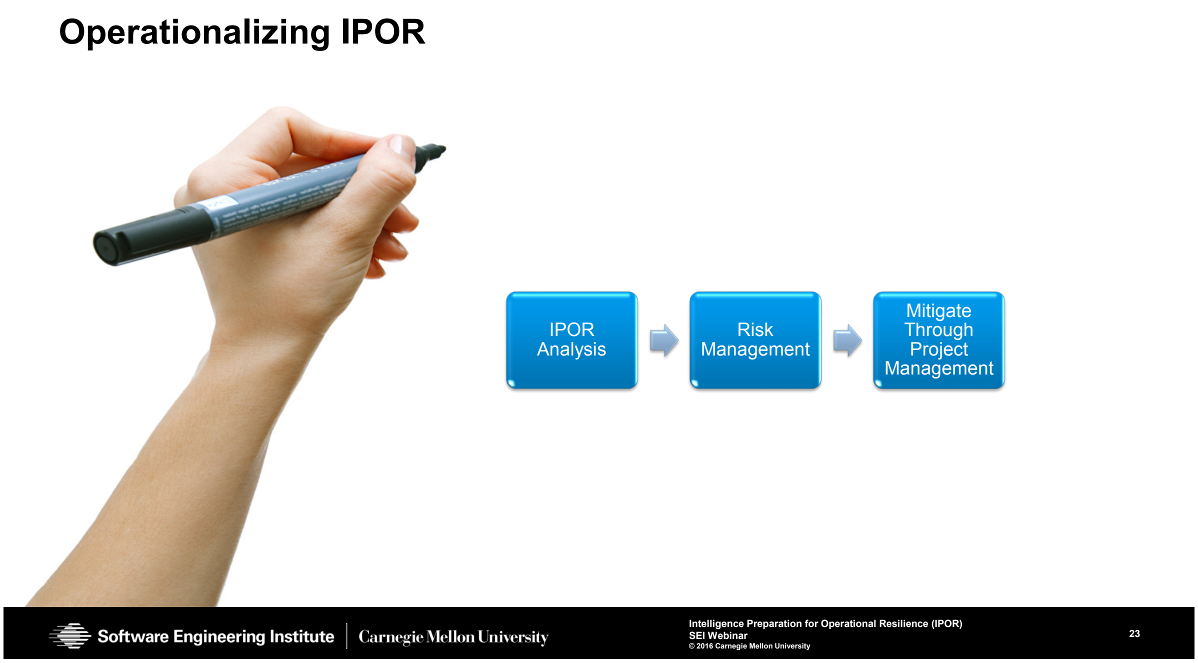
Software Engineering Institute | Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar

22

**022 And this is all about empowering you to do that. So we get to that point of the actual--go a gentleman mentioned mitigating risk. So let's talk about operationalizing--

Operationalizing IPOR



Operationalizing IPOR

IPOR Analysis → Risk Management → Mitigate Through Project Management

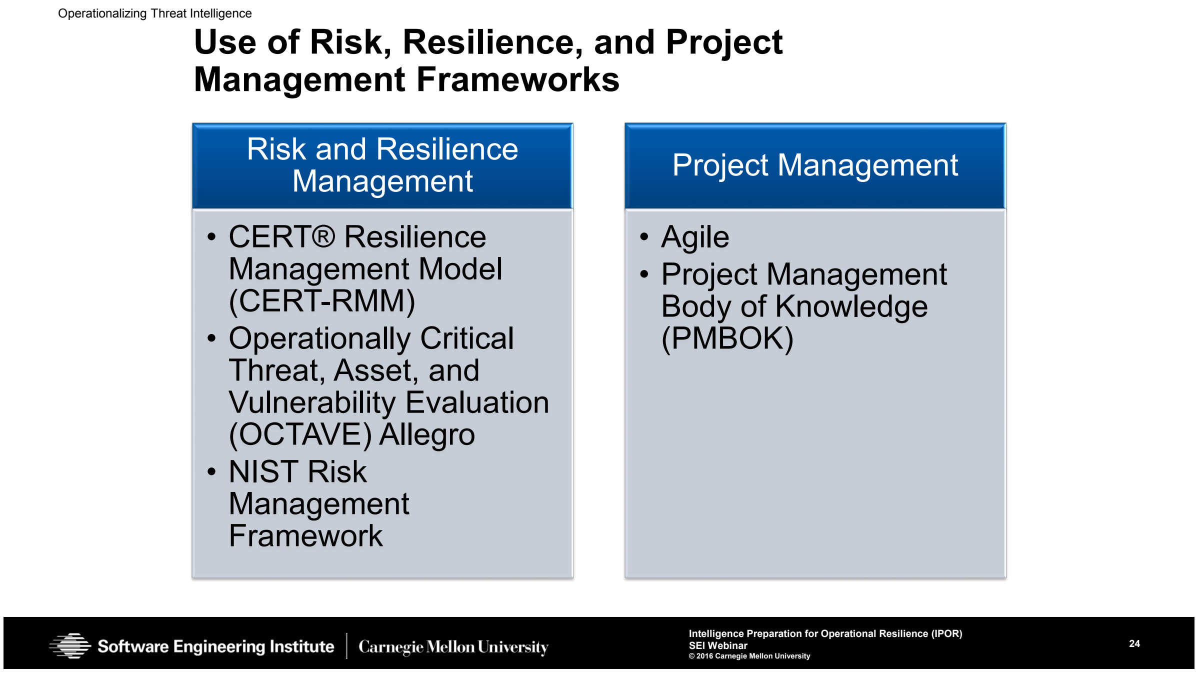
Software Engineering Institute | Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

23

**023 --intelligence. So we've collected our information and so now what we're going to do is we're going to talk about two steps. We're going to talk about risk management and then taking the output of risk management and we're actually going to mitigate that through discipline project management.

Use of Risk, Resilience, and Project Management Frameworks



Operationalizing Threat Intelligence

Use of Risk, Resilience, and Project Management Frameworks

Risk and Resilience Management

- CERT® Resilience Management Model (CERT-RMM)
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Allegro
- NIST Risk Management Framework

Project Management

- Agile
- Project Management Body of Knowledge (PMBOK)

Software Engineering Institute | Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

24

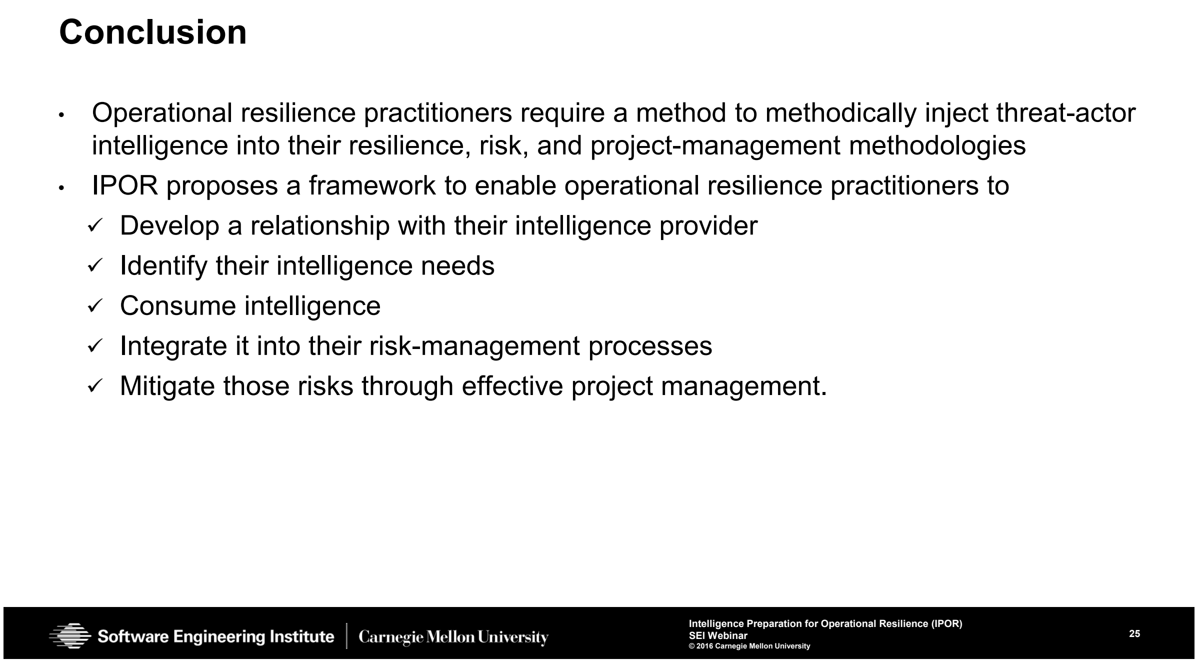
**024 So again, we pulled out three risk-management frameworks, so of course CERT-RMM is near and dear to our heart. And what we did in the special report was we actually, for those of you who use CERT-RMM or are thinking about it, we actually pulled out specific practices in a couple process areas that are actually germane to this area. So as the vulnerability analysis and resolution process area where you're taking a look at those vulnerable conditions in your organization. And there's also, of course, the risk management process area where we're categorizing risk, we're describing the risk and we're creating a disposition for those risks. We're prioritizing them. So OCTAVE is a little bit more of a regimented, risk-management methodology. It's kind of checklist and worksheet oriented. There is a very specific or there's a particular worksheet called the information asset. The Information Asset Risk Worksheet. If you look at it, it looks actually very much like the threat-actor use case that we just were talking about in the voice of the threat actor. So this is very good place to kind of inject this. Finally for risk management, the NIST Risk Management Framework, if you do work for the federal government and you're working with systems, you're probably very familiar with the process but the one thing I'd like to emphasize is, you know, there's kind of this perception that the RMF is just a way to kind of get your system certified and accredited. It's a controls management framework. It's not. It's not. It's a risk-management framework.

So a couple of different areas in the NIST Risk Management Framework, where this helps you, is first of all when you've selected your controls you then have to tailor them and you tailor them based upon a risk assessment. So although that's kind of an optional step, you know, a lot of people, they grab their baseline controls and they kind of run with them, you really should be looking at how do I take these controls and how do I make them useful for the thing I'm trying to defend and the people who are trying to undefend them, for lack of a better phrase?

So then we want to ensure success at the point of execution. And one area that we're really excited about in terms of looking at for ensuring success in these operational resilience and cybersecurity domains is the Agile methodology. So the whole idea of Agile, and I know I'm going to butcher this. There's a lot of Agile purists on the line. So I ask for your forgiveness up front. But basically the idea behind Agile is we basically chop up our work into bite-sized morsels called user stories. And we take those user stories and that becomes our unit of work. We put it into a backlog and then we, through a planning process, we assign those user stories to a sprint. Usually about one to four weeks. The sprint team can be multi-functional, but it's, they're, usually dedicated to resolving those work products in that one to four-week sprint.

Well, risk management is ever-changing. The inputs are ever-changing. How we weight those criteria are ever-changing. So having a project-management methodology which actually welcomes changes is a really exciting thing to consider. So we've talked a little bit about that in the special report and we certainly recommend if you're not just for this but for anybody looking to mitigate risks, either emanating from this or information security continuous monitoring is another framework. We certainly recommend taking a look at that. So the project management body of knowledge is a, that is a body of knowledge which was developed by the Project Management Institute. For those of you who have studied for or have taken the Project Management Professional certification, that is the basis for that. And provides a framework for managing projects. Now, mind you, Agile and PMBOK go well together, go very well together, but PMBOK is a very nice way of making sure that you've kind of covered all the bases for your project management. One point of inject, out of your risk management, your IPOR-enabled risk management, is the project charter. In the project charter, you're identifying your business case. So here in Process 4.1 of the PMBOK, an IPOR-enabled risk-management process helps you to build a better use case. You're actually able to show intelligence that's actually behind why you think this project should be taken on. In Process 5.1, we're determining the scope. And if we understand what the intentions, capabilities and prevailing attack patterns are of the threat actor if we understand the environment and our defendables, that helps us to define the scope for the project. And finally, in Process 5.2, well, we have requirements development. So what this very defined, structured way of developing situation awareness enables us to do is it helps us to add context, kind of color and flavoring to those requirements. So it's not just a requirement statement, it's a requirement statement that really has some kind of teeth behind it and we can actually craft it to actually achieve a risk management outcome.

Conclusion



Conclusion

- Operational resilience practitioners require a method to methodically inject threat-actor intelligence into their resilience, risk, and project-management methodologies
- IPOR proposes a framework to enable operational resilience practitioners to
  - ✓ Develop a relationship with their intelligence provider
  - ✓ Identify their intelligence needs
  - ✓ Consume intelligence
  - ✓ Integrate it into their risk-management processes
  - ✓ Mitigate those risks through effective project management.

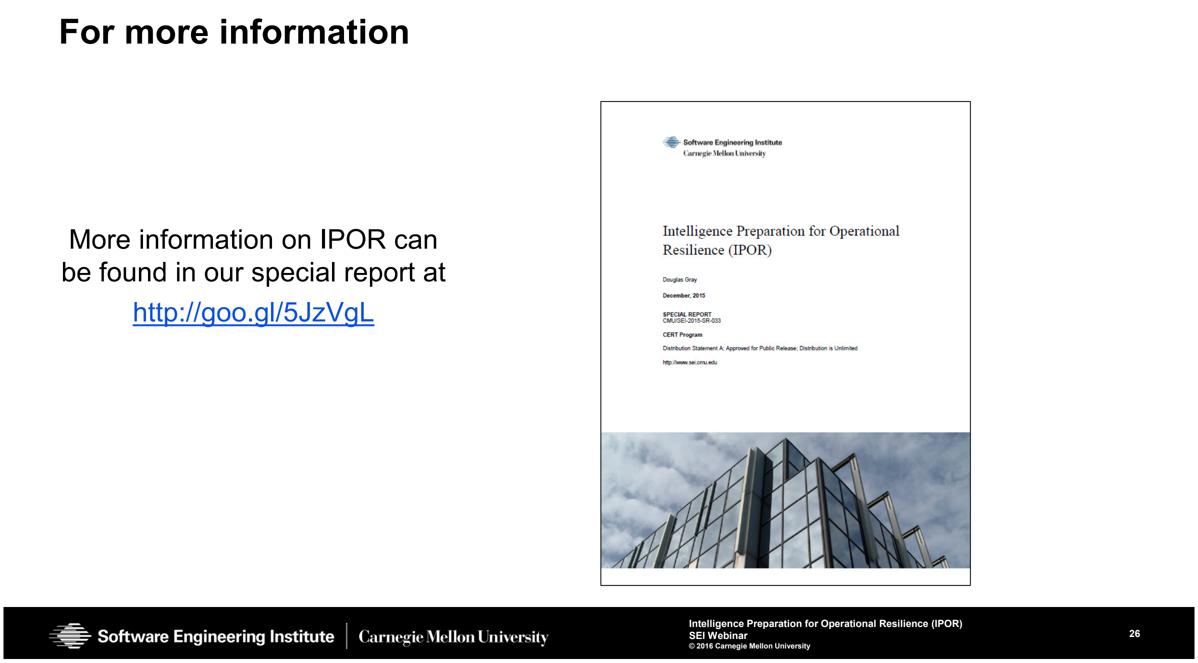
Software Engineering Institute | Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

25

**025 So in conclusion, so we've gone over the IPOR framework, Intelligence Preparation for Operational Resilience. It's a framework built, or inspired, by the IPB process from the military. Designed to help us determine what kind of intelligence we need, have, still need to get, and how do we get after that, how do we get that intelligence? And how do we inject it into the risk management frameworks and agile--and I'm sorry--and project management frameworks that we're already using?

For more information



For more information

More information on IPOR can be found in our special report at http://goo.gl/5JzVgL

Software Engineering Institute
Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)

Douglas Gray

December, 2015

SPECIAL REPORT
CMU/SEI-2015-SR-033

CERT Program

Distribution Statement A: Approved for Public Release; Distribution is Unlimited

http://www.sei.cmu.edu

Software Engineering Institute | Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

26

**026 So again, this is a brand-new framework. So we very much invite you to check out the special report on our website. It's also in the Additional Resources.

Shane McGraw: In the downloadable section. Yes.

Douglas Gray: Absolutely. And we're looking, we're definitely looking for feedback. And if you'd like to work with us directly on it, we'd like to hear from you, as well.

Shane McGraw: Okay.

Q&A

Software Engineering Institute | Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)
SEI Webinar
© 2016 Carnegie Mellon University

27

**027 We got about a minute left here with Doug, so we're going to work in one more question, if you don't mind, and then we'll--

Douglas Gray: Absolutely.

Shane McGraw: --wrap it up and get people out of here at two thirty. So from Tim asking, "How do we uniformly and objectively describe the threat actors? Most schemas are very terrorism focused, which is not a big problem for us."

Douglas Gray: So there's another body of work that we've done. I think it's--I think I may have put it into the special report. And it's a framework that we use to kind of describe yourself. It's called the GQIM framework, Goal, Question, Indicator, Metric. And so we've done a lot of work on basically taking what your mission is and building goals around it, developing questions that help you determine whether or not you're getting your, you're meeting your goal. Indicators of pieces of information that help you to answer the question. The metric is how you put it together. So there's--so one of the things that I found in looking at this is that the GQIM method, although it's great for answering our own questions, it also applies to the bad guy as well. So it's kind of a structured way. And again, it can be as formal or informal as you want, but it's a great way of looking at the category of the threat actor and asking, "Well, what are the goals?" And trying to get some information as to, "Well, what's my evidence?" You know, like one question's, "What's the evidence that this goal actually exists?" What are the pieces of information that helps me to answer that question? And how do I know that they're achieving their goals? How do I divide X by Y? If at all possible. Sometimes this is going to be subjective and qualitative to try to answer that. Above all, always go back and reevaluate the assessments that you made before. In the military we called it murder boarding.

Shane McGraw: Very good. Folks, that's all the time we have for today. Just a reminder, upon exiting the webinar, please make sure you download those materials, fill out our survey, and as a last reminder, our next webinar will be next Thursday, March 10th, and the topic will be "What makes a good software architect?"

So we'll have a lively discussion there and we hope you can attend. Have a great rest of your day.

SEI WEBINAR SERIES | Keeping you informed of the latest solutions

SEI WEBINAR SERIES | Keeping you informed of the latest solutions

#SEIwebinar