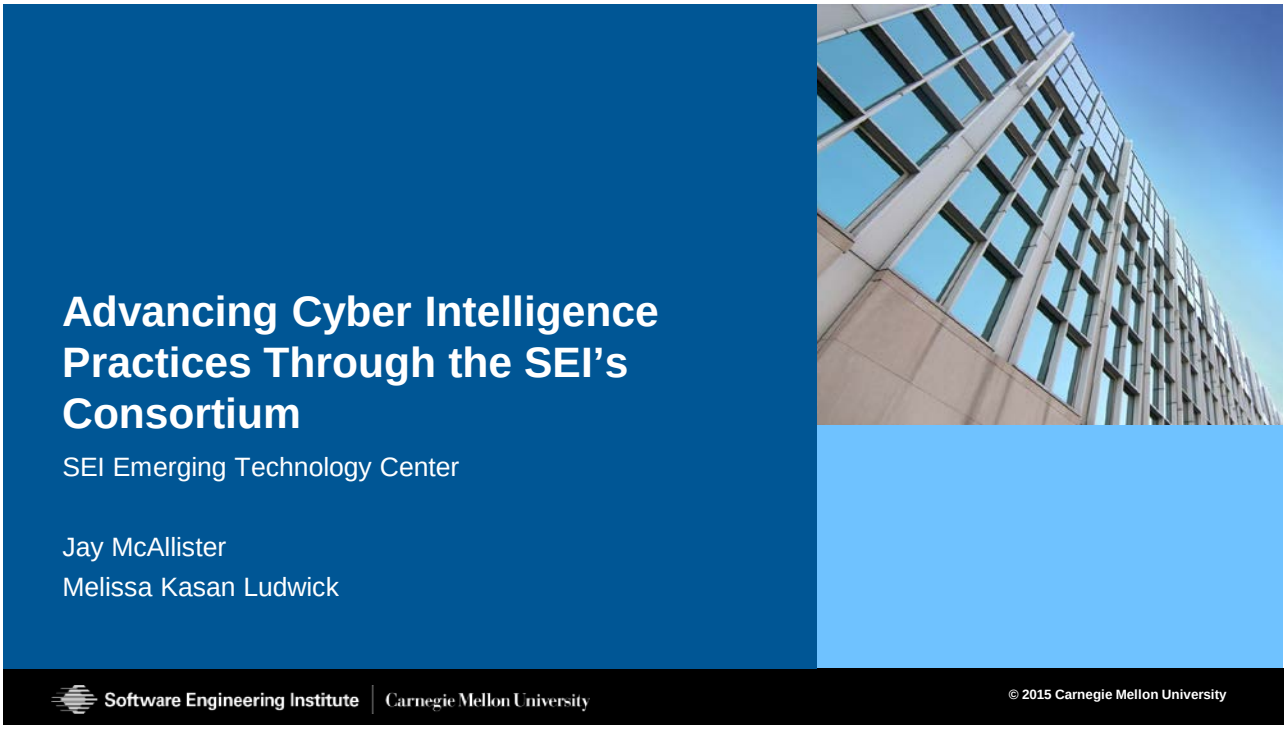
Advancing Cyber Intelligence Practices through the SEI's Consortium

Table of Contents

Carnegie Mellon University Notice

Carnegie Mellon University

**001 (Music)



**002 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 Advancing Cyber Intelligence Practices through the SEI's Consortium. Depending on your location, we wish you a good morning, a good afternoon, or good evening.

My name is Shane McGraw, your moderator for today. 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. To log a question, simply go to the Q and A tab on your

event console and type in your question and click send. We will also ask a few polling questions throughout the presentation. They will appear as a pop-up window on your screen. The first question we want to ask today is how did you hear about today's event?

Another three tabs I'd like to point out are the files, Twitter, and survey tabs. The survey, we ask that you fill out upon completion of the webinar as your feedback is always greatly appreciated. The files tab has a PDF copy of the presentation slides there now along with other work in cyber intelligence from the SEI. For those of you using Twitter, be sure to follow @SEInews and use the hashtag SEI cyber.

Now, I'd like to introduce our presenters for today. Jay McAllister leads research and development efforts that provide technical solutions in analytical acumen to cyber intelligence practitioners from government, industry, and academia. Prior to joining the SEI, Jay served as a counter-intelligence, and counter-terrorism analyst for the Naval Criminal Investigative Service. He holds a master's degree in strategic intelligence from the National Intelligence University, and a bachelor's degree in economics from the University of Notre Dame.

Melissa Kasan Ludwick is a technical analyst for the SEI's emerging technology center. In this role she focuses on matching state of the art

software research with critical government and private sector needs. Ludwick is currently concentrating on research and prototyping efforts aimed at developing and refining cyber intelligence methodologies, technologies, and processes.

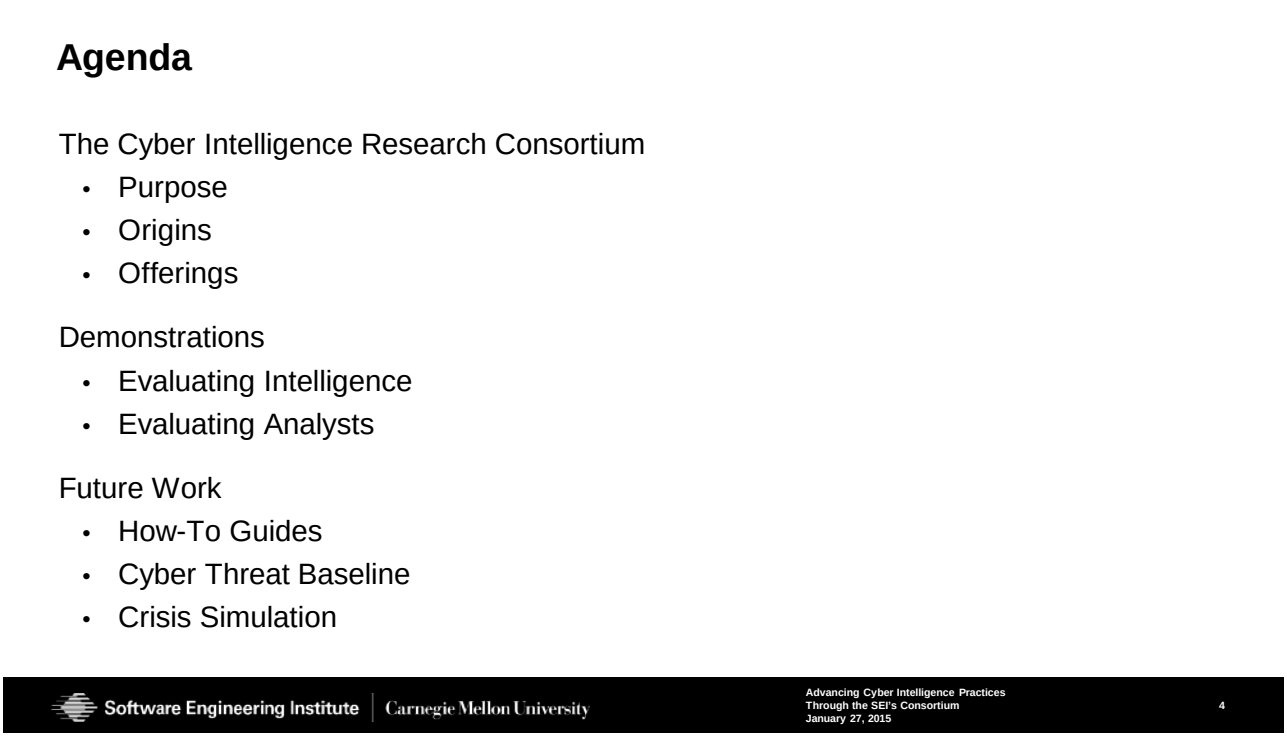
And now, I'd like to turn it over to Jay McAllister. Jay, all yours, welcome.

Jay McAllister: Thanks Shane. Welcome everybody. Today we're going to talk about the cyber intelligence work we're doing here at the SEI's emerging technology center. We've been looking at cyber intelligence for about the past three years. And we wanted to talk to you about a lot of the research that we've been doing in that space to include mostly a consortium that we're currently running called the Cyber intelligence Research Consortium.

Copyright 2015 Carnegie Mellon University

**003 Three big things we want to talk about today.

Agenda



**004 And those include the consortium, its purpose, origins, and then the offerings. And then what are we actually doing? What does it mean to do research and development, R and D, within the cyber intelligence space? We're going to give you two examples of some of the many things we're working on for our consortium members. That's going to be talking about evaluating intelligence as well as evaluating analysts. And then we're going to talk about future work, things that we're doing to finish up year one of our consortium and then moving on into year two, year two beginning in July of this year.

Advancing Cyber Intelligence Practices Through the SEI's Consortium

**005 Melissa Kasan Ludwick:
We're going to be talking about our Cyber intelligence Research Consortium. And Jay mentioned that that started this year, this past June. So, we're a little bit more than halfway through our first year.

Purpose

Purpose

The Consortium is a member-funded initiative that researches and develops technical solutions and analytical practices to advance the art and science of cyber intelligence

Cyber intelligence: The acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities to offer courses of action that enhance decision making

It was formed because government, industry, and academia were looking for…

- Access to cost-effective resources for cyber intelligence workforce development and technology scouting
- Awareness of analytical practices from all organizations, regardless of size and economic sector
- Insight into SEI and Carnegie Mellon skills and capabilities

**006 The purpose of the consortium, it's a member funded initiative that researches and develops technical solutions and analytic practices to advance the art and the science of cyber intelligence. So, before we go any further, we thought we'd talk a few minutes about our definition of cyber intelligence. There's lots of them floating out there. But we define cyber intelligence as the acquisition and analysis of information. This information is identifying, tracking, and predicting cyber capabilities, intentions, and activities. And most importantly this information is going to be used in your organization to offer courses of action that enhance decision making.

So, what we mean by information, you're looking at both the technical and the strategic. You're looking within your organization at your technical network data. You're looking at information from your finance department or your strategic development group.

And then you're looking external. You're looking at kind of what's happening in the news right now, the major cyber threats that are occurring. What the president might talk about cyber in his state of the union address. You're looking at social media, what's happening on Twitter, and what's happening open source, news articles, anything that you would find online. So, you're using that technical and strategic information and you're taking it and applying it to a cyber threat.

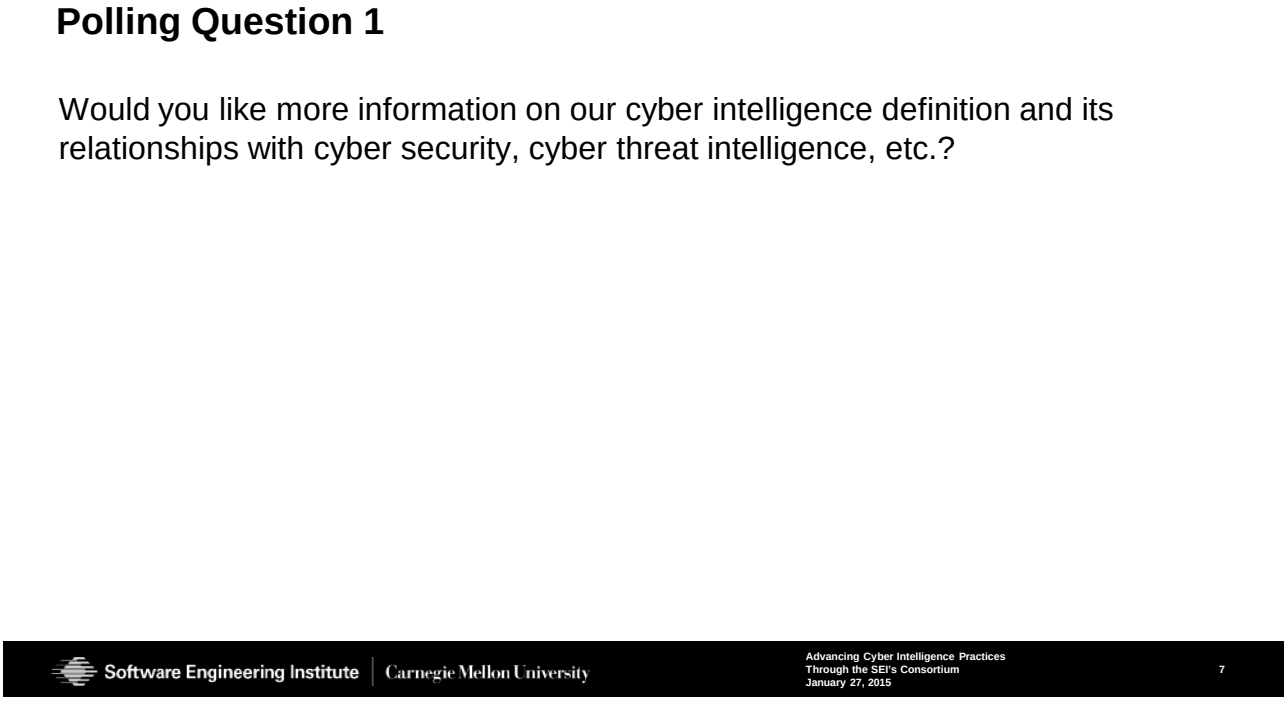
So, our consortium was formed because our partners in government, industry and academia were really looking for three things, access to cost-effective resources for cyber intelligence, workforce development, and technology scouting. So, our membership, they really work in an operational pace, very busy. And they don't have necessarily the time or the resources to have a research and development function. So, they're able to pool their resources together in our consortium and use us as their research and development. So, we do this work for them.

Our members are also looking for awareness of the political practices

from all organizations. And we say regardless of size or economic sector. So, our membership kind of have a varying range. They represent multiple sectors both in government, industry, and academia. But the important thing is they're all taking technical and strategic information and they're applying it to cyber threats. So, regardless of size or economic sector, they're all doing kind of the same function. And there's a lot we can learn from each other there.

Finally our membership's looking to the insight and the access that we have here to SEI practitioners and Carnegie Mellon practitioners and their skills and capabilities.

Polling Question 1



**007 So, our origins, we've been working in cyber intelligence for just over three years now.

Origins

Origins

Cyber Intelligence Tradecraft Project

- www.sei.cmu.edu/etc/cyber-intelligence/citp
- Studied how 30 organizations from government, industry, and academia performed cyber intelligence

Overall finding

- Effective organizations balance the need to protect their network perimeters with the need to look beyond them for strategic insights

Deliverables

- Summary of Key Findings: Best practices and lessons learned
- Implementation Frameworks: How-to-guides for analysis
- White Paper: Practitioner core competencies and skills

**008 Before we get into that, do you want to take a polling question?

Shane McGraw: Yeah, we're going to ask a quick polling question. One of the things Jay and Melissa wanted to do folks, throughout the webinar was kind of make sure you get what you need out of this webinar. So, we're going to ask a couple polling questions throughout to make sure you're getting your questions answered and make sure you're understanding what's being posed. The first, or actually the second question we want to pose is would you like more information on our cyber intelligence definition and its relationships with cyber security, cyber threat, intelligence, etc. So, if you need more of an understanding of what we're talking about by the

cyber intelligence, how it refers or relates to cyber security, go ahead and vote now. And we'll give them about fifteen or twenty seconds. We can get into origins. And we'll come back to that in a second Melissa.

Melissa Kasan Ludwick: Great. Thank you. Okay. So, we've been working in this space for about three years now. We started with our Cyber intelligence Tradecraft Project. And this is a project that was sponsored by the office for the director of national intelligence. And we were really looking at the cyber intelligence capabilities through a broad range of organizations. We looked at thirty companies representing government, industry, and academia. And we looked at how they were conducting cyber intelligence in their organizations.

I think our overall most important finding that came out of this is we found that successful organizations that really utilize cyber intelligence really balance the need to protect their own network, and their network perimeters. And they balance that with their need to look past them for strategic insights.

We had three deliverables coming out of this. The first was our summary of key findings. And this is really where we document the work that we did. We take the best practices, common challenges, lessons learned from our thirty organizations. We document it there.

We also developed three implementation frameworks. And these are really how to guides for analysis. So, like I said, we did three of them. The first one was on threat prioritization. The second one was on collection management. And the third one was on workforce development in management.

And finally our last deliverable for this project was a white paper where we examined the trades, core competencies, and skills of successful cyber intelligence analysts. It's a benefit for participating, as a thank you for participating today, these deliverables will all be downloadable to you. Okay.

Shane McGraw: So, if I can show those results from the survey real quick. We got about sixty-six percent looking for more information on what we're calling cyber intelligence. So, can we do a little bit deeper dive into that space?

Jay McAllister: Sure thing. I can field that. Cyber intelligence, there's a whole bunch of different names out there in the space right now. So, when we started our research about three years ago, we first went to organizations, whether it was a Fortune 500 company in the financial services sector, the healthcare sector, retail, energy, or it was a federal agency, and sat down and said, "Okay, what do you do for cyber intelligence? Let's start getting into the nitty gritty of your processes, your methodologies, your tools, and

your training." And they immediately looked at us with a blank stare and said, "What do you mean by cyber intelligence?" So, we realized that we had to at least explain what we meant by cyber intel. And that's where we came up with our definition.

Other phrases or other terms you hear out in this space, cyber security, cyber threat intelligence. Again, to reiterate what Melissa said, cyber intelligence for us is a strategic, holistic approach to assessing or dealing with cyber threats. We look at the strategic aspects. We look at the tactical, or the technical, so who, what, when, where, why, and how.

A lot of organizations, when they talk about cyber security, that focuses a lot on more technical analysis, and maybe doesn't bring in the strategic or at least reference the strategic as much as we would like. When you get a lot of definitions for cyber threat intelligence, a lot of that is indicator sharing, so the passing of ones and zeroes, and again at a very technical level. We wanted to really reinforce the need for both. So, when we say cyber intelligence, it can incorporate aspects of cyber security. It can incorporate aspects of cyber threat intelligence, or whatever definitions are out there. But it can also be serving its own purpose.

Kind of if you look at say the difference between if you're doing counter-intelligence work and if you're doing physical security.

There's overlap, but they're two distinguishing entities. And that's how we take our approach to cyber intelligence.

Shane McGraw: So, I think we have a relevant question here from Robert asking, "Is there a correlation between this topic and network centric warfare?"

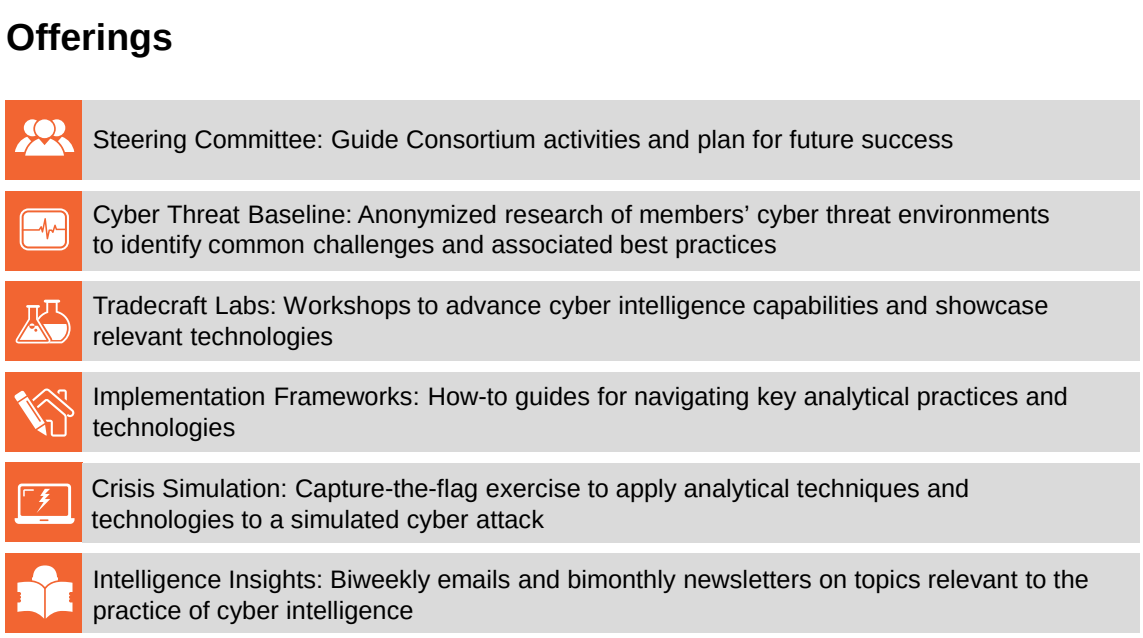
Jay McAllister: Yes and no. Yeah, that's a good phrase that's used out there in the military and government, and I think some private organizations have obviously picked that up as well. A lot of folks we talk to, especially who have that experience in the military, kind of say, "Oh, you're just saying the same thing-- you're doing the same thing that we were doing in the 90's. You're just calling it something different now." And to an extent, that is the case. The world of intelligence has been around for hundreds of years. It started with the office of naval intelligence when our country was first beginning and has moved on since then. So, there are aspects of that. Again it's really-- it's taking the technical and the strategic now in this kind of cyber threat, Internet of things space. So, hopefully that helped.

Shane McGraw: Okay. Great. Very good, yeah. Melissa, we'll go back to you and move on.

Melissa Kasan Ludwick: Okay. Great, thank you. So, I'd like to take a few minutes to talk to you about

the offerings that we have for the consortium. Now, this is what we're doing for the first year. The offerings are going to look very similar for the second year, except we'll be focusing on different topic areas.

Offerings



**009 We won't be regenerating the same thing. So, first we have our steering committee. And we're actually really fortunate for this first year. We have a great steering committee. They're very involved. They're very helpful in guiding us in our research. So, we want to make sure everything we're doing is really representing our member's interests and really giving them what they like to see out of the consortium. So, they're directing our research and our prototyping efforts.

Second, we have our cyber threat baseline. Now, this is going to be all anonymized data. And this is research into your own members' cyber threat environments. So, we've developed assessment factors. And we're going to be looking with our membership at their environments to identify the common challenges and the best practices that they have. Along with this baseline, we'll also be developing a summary of key findings to share these common challenges, the best practices, the lessons learned through our research.

Next we have our Tradecraft Labs. We have two of these the first year. Our first one we had this past November. And our next one will be held in May. And this is a member-only, in-person workshop. And we're pulled together to look at advancing cyber intelligence capabilities and showcase relevant technologies that our membership's interested in. Okay.

Next we have our implementation frameworks. And we are going to-- we'll be talking about them a little later in the webinar. But we have four that we are doing this first year. And we'll talk about those in a little while.

Next, we have our crisis simulation. And Jay will be going into this later in the webinar. But really, this would be kind of our big event that's going to close out year one and launch us into year two for the consortium. And this is going to be a large, in-person

event similar to a capture the flag exercise. But we're going to have our members' analysts come here and work on a large cyber threat scenario together. We're really excited for this one.

Finally, we have our Intelligence Insights, our bi-weekly emails and our bi-monthly newsletters. So, our biweekly emails are really just a way for us to keep in contact with our consortium members. We give them an update every two weeks on the work that we're working on. We like to showcase what our members are actually working on in their respected organizations. And then we're also sharing with them conferences, and workshops, and interesting news items that we've run across in the previous two weeks. And then finally our bi-monthly newsletters, these are sent out. And they really just cover different topics a little bit more in depth to topics relevant to cyber intelligence.

**010 Jay McAllister: Okay. Great, thanks Melissa. So, what does it look like to actually do R and D in the cyber intelligence space at least from our perspective? We wanted to give you some insight into that. Melissa talked about a lot of different offerings that we have going on here with the consortium. And we wanted to give you a sampling of some of the output that we've done for our members to date. And again, since we just started in June, we're only about half way through our first year. And we've already put together some interesting stuff. So, we're going to talk about two in these offering demonstrations.

Evaluating Intelligence

Challenge

- Cyber intelligence is a phrase often used, but interpreted in many different ways, leading to a diverse output of threat analysis categorized as cyber intelligence
- Such output is difficult to evaluate and compare, stifling an organization's ability to establish guidelines and goals

Solution

- An evaluation template based on standards observed during our research and set forth in U.S. Intelligence Community Directive Number 203
  - http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards%20pdf-unclassified.pdf

**011 The first being evaluating intelligence. We, in talking to our members, in talking to just other organizations whether it be at conferences or in other interactions they have with the SEI and CMU in general-- and we talked about this really with our definition. Cyber intelligence is a phrase that's often used, but it's interpreted in many different ways. When this-- with all these different interpretations, you're going to get a ton of analytical output.

You could have an intelligence service provider giving you a paragraph summary on a recent threat to the banking industry. That is a form of cyber intelligence. You could be getting a strategic product, a yearly basis, kind of what Verizon

does. That can be another form of cyber intelligence. And when an organization or a person is getting this type of information, how do you evaluate that information?

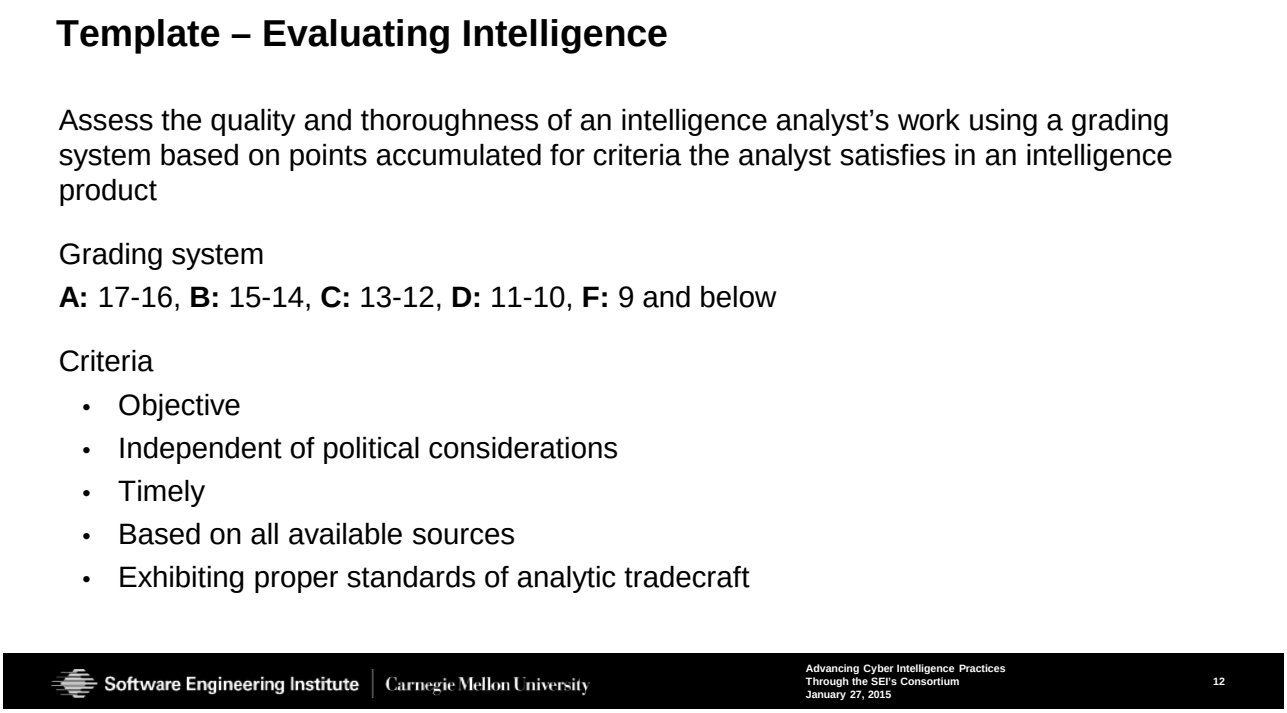
We saw in talking to some of our members and some of the participants in the previous projects we worked on, that if they actually had the resources and the personnel to do this, started putting together some type of standardization when it came to evaluating these different intelligence products that they received. And we thought well, that's great. How can we apply that to a broader scope? How can we make that scalable?

And so, we took those best practices. And then we looked at things that already existed to come up with an evaluation template that anyone can use regardless of their size or their economic sector to evaluate intelligence. We pooled a lot from the U.S. intelligence community's directive number 203, directives that come out that try to give standards to the U.S. intelligence community for a whole host of different aspects of their job, one of those being doing standards for evaluating intelligence. So, when we talk about the criteria that came with our evaluation template, really a lot of this is built off of intelligence directive number 203.

They're-- Melissa and I easily can sit down and come up with some criteria. However, this has been

something that's been iterated with a lot smarter people over a lot more years then we've put into it. So, we wanted to utilize what's pre-existing out there and try to build off of it for our own purposes.

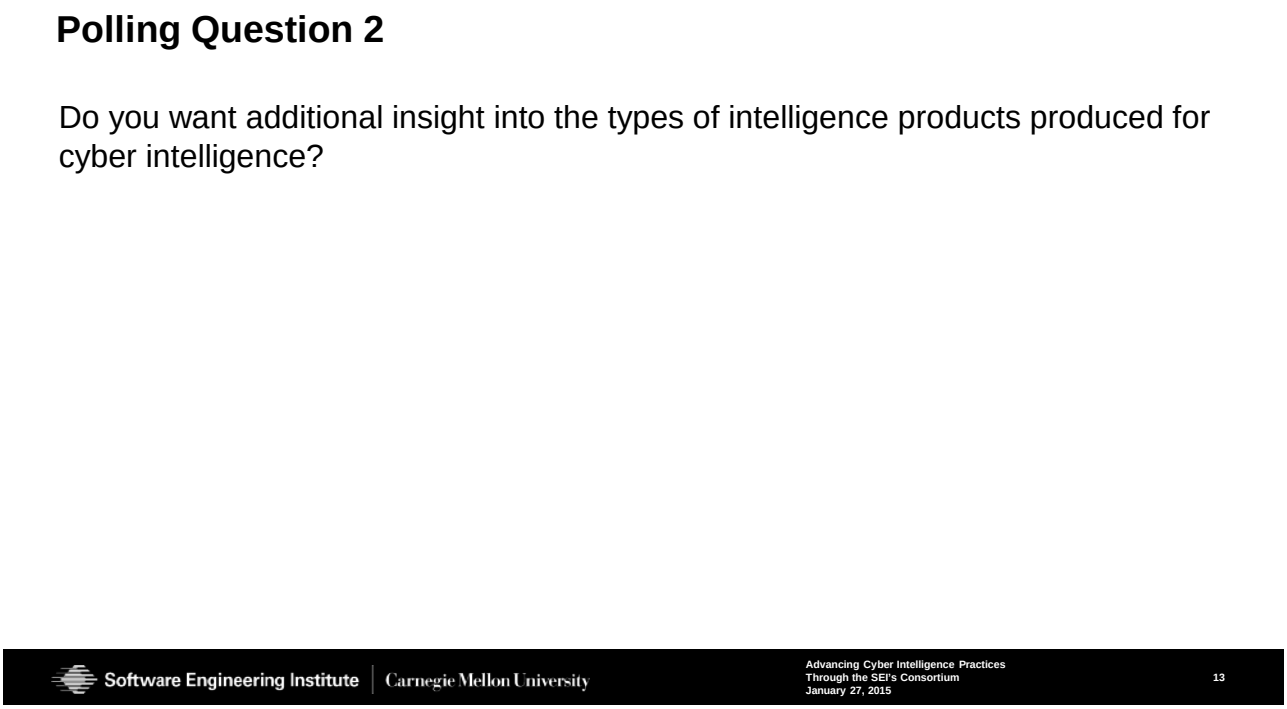
Template – Evaluating Intelligence



**012 So, here's the template. We put together kind of a first version automated template for you again, thanking you to participate, and to be able to give you something as you walk away from this webinar. So, in the downloads, you will have a template for evaluating intelligence. Essentially, what you can do is you can assign a grading system to any type of piece of intelligence that you would like. The grading system is A to F. You can see it's a max of seventeen points. And there's criteria.

These five criteria do align back to the intelligence community directive and our hopes of getting some standardization out there, and building off the great work that's already been done.

Polling Question 2



**013 We can go into a little more detail on all of these. But first, I think we'll take another time out for a polling question.

Shane McGraw: Yeah. So, we're going to give another polling question to help direct the flow a little bit folks. And that question is, "Do you want additional insight into the types of intelligence products produced for cyber intelligence?"

And while you're voting on that, we've got a couple questions, people asking about an archive, or the slides, or where these references and materials are available. The event is being archived. So, that should be up at some point tomorrow. The login is the same as you had today. You just go to the registration page, login with your-- the email that you use at registration time. And you'll be able to access the archive.

Jay mentioned the files are in an actual files tab in the console. You'll see the presentation slides there. You'll see the template that Jay mentioned from everyone attending today, a sample of the eNewsletter, the presentation slides, an overview of the consortium for government and industry. So, I hope you walk away with all those materials today.

So, let's take a look at our results here. And we got about eighty-two percent saying yes, they would like additional insight. So, can we do a deeper dive there Jay?

Jay McAllister: Sure. So, intelligence products can-- they really run the gamut. Again, if you're doing kind of-- I think maybe an example would be hopefully the most beneficial. One of the more forward-leaning organizations that we've dealt with in our research, they're in the information technology space. And they are a product-based organization. So, they focus a lot of their cyber intelligence work around the products that they are developing

throughout the lifecycle, from basic research to commercial implementation. And they focus their cyber intelligence around that.

When it comes to producing actual intelligence for their decision makers and for their stakeholders, they have a plethora of offerings. So, they will have at a very basic, say for general employees that don't have significant technical experience with cyber, they have the basic security awareness newsletters. So, maybe it's on a bi-weekly or a bi-monthly basis, putting out newsletters like here's the proper passwords that you could use. Here are some things that you might have seen out in the press about say the Sony attack, or what happened at Target, or what happened at Home Depot. Here's how it affects you. Here's how it affects the company. And here's what you can do moving forward. It can give some training opportunities. Those are some examples of some intelligence products.

If you're looking at more a technical range, and if you're focused more on say that cyber security space, information that organizations receive from the US-CERT that's talking about different threat streams, the passing of indicators, those type of write ups that are putting context to information. I think a lot of times you'll see things classified as intelligence. But if it's an Excel sheet with a thousand lines of different indicators, that's information. That's not intelligence. Once you put

knowledge to that information, it becomes intelligence. And so, that's really where we distinguish when we talk about intelligence products. So, you can-- if you're getting those daily input from US-CERT-- from the SEI's own CERT, that is certainly a form of an intelligence product.

And then you can get to the strategic level. So, every morning the president has a briefing, a presidential briefing where he receives news on national security and a whole host of other issues. That's an intelligence product. the binder of that, or the presentation that he's getting every day, are paragraph to two paragraphs of national security issues from terrorism, to counter intelligence, to cyber. And those are all forms of intelligence products.

It could also be the sixty to seventy page report that you'll get from organizations that talk about here's our deep dive into Stuxnet, and who we think was responsible. That's a form of intelligence. So, there's really a whole host of different intelligence products. But those are a few examples kind of going from technical, to non-technical, to strategic, to not as strategic that we consider when we use that phrase.

Shane McGraw: And another-- just a relevant question came in here from Joe asking, "Is the consortium developing any analytical tools for its members?"

Jay McAllister: Yes. So, the consortium does not-- we're not operational. We're not providing intelligence in the form of, "You need to take this type of approach with your network security," or "You need to-- this threat actor is bad and you should avoid them at all costs." That's not the purpose of the consortium. It's to do the research and development that our members want. And that includes analytical tools.

Some of the things that we're focused on when it comes to that is helping to beef up the evaluation of intelligence like we're currently talking about. How-- what type of tools can be put in place to automate as much of that evaluation as possible? That is significantly helpful for organizations when contract renewals come up for external intelligence service providers. If it's a major organization that has many different directorates or divisions, all of those play in the cyberspace in some form or fashion, so have a need for cyber intelligence. And that can come in handy when dealing in organizations in that world as well.

Shane McGraw: Terrific. We're ready to move on.

Jay McAllister: Great. Okay. So, going back into evaluating cyber intel--

Criteria - Objective

Criteria - Objective

Worth 4 points

- Functions from an unbiased perspective
- Gives due regard to alternative perspectives
- Gives due regard to contrary reporting
- Acknowledges developments that necessitate adjustments to analytic judgments

**014 Yeah, evaluating cyber intelligence. We've got the five criteria. Again, it goes back to the US intelligence community directive number 203. The first one is being objective. These are all factors that are really important to consider, not only when you're writing an intelligence product, but when you're evaluating one. So, it really can apply in both instances. We're applying it for the evaluation of intelligence. You have to be objective. And this criteria is worth four points. And there is four different aspects, a point each.

You've got to function from an unbiased perspective. So, that information you're reading, that information you're receiving, that has become intelligence, has to be unbiased, that there's not personal

biases within there. It gives due regard to alternative perspectives. You can say X is occurring. But you need to say it could be Y, Z, M, a whole host of alternative perspectives, but then come back to why it is that you went with X.

Regard to contrary reporting, this is very important. I'm saying something, but these five people don't agree with me. Here's why they don't agree with me. But here's why I'm still saying what I'm saying. That's important to put-- to add credibility to an intelligence report to see the validity of it.

And then acknowledge developments that necessitate adjustments to analytic judgments. You're always hoping for the hundred percent solution. That's not really feasible. But you want to try get as close to a hundred percent as possible. So, you have to look is the intelligence product a living document If it's time-stamped from 1980, and you're still trying to quote it in 2015, depending on the content, you might be a little out of your league, and might not be as-- people might not want to believe what's in that report as much. So, that's something to consider when you're evaluating an intelligence product.

Criteria – Independent of Political Considerations

Worth 2 points

- Provides objective assessments informed by available information
- Is not distorted or altered with the intent of supporting or advocating a particular policy, political viewpoint, or audience

**015 The next criteria, independent of political considerations, so there's objective assessments. It's being informed by available information. They actually cited their sources. You can see it's not just something they came up with over the weekend or their own personal feelings. And then it's not altered or distorted in a way that looks at a particular policy, a viewpoint, political stance, or curtailing to a certain audience. You obviously want to be aware of your stakeholders. But you don't want just to satisfy them even if that's incorrect information.

Criteria - Timely

Criteria - Timely

Worth 1 point

- Is actionable

**016 Next timely, pretty straightforward. Is it actionable? Is this something that is-- do you have a quick turnaround? Is that intelligence product coming to you within a day, within four hours? Is that time justifiable? Has that been taken into consideration?

Criteria – Based on All Available Sources

Worth 3 points

- Is informed by all relevant information that is available, including open source information
- Addresses where critical intelligence gaps exist
- Identifies appropriate collection, dissemination, and access strategies to fill the gaps

**017 The second to last, based on all available sources, there's three parts to this one. All the relevant information is available even utilizing open source information. For government entities, this is still really a big push. People want to put a lot more stock into classified information. But you really can find almost just as good, if not better, information out there in the open source world. And it's important to consider that and incorporate that into intelligence product.

Another big one is addressing intelligence gaps, especially if you're trying to put together, say, for a decision maker that's in charge of network security, you have to get them the sixty to eighty percent solution in a matter of hours. But are

you identifying the gaps that you still need to fill so that they know this is a work in progress assessment? And not only what are the questions you still have, are there gaps that actually are identified, but how would one go about collecting, disseminating, and accessing the information needed to fill those gaps? A solid kind of A level intelligence product is going to focus on all of this information.

Criteria – Exhibiting Proper Standards of Analytic Tradecraft

Criteria – Exhibiting Proper Standards of Analytic Tradecraft

Worth 7 points

- Properly describes the quality and reliability of the underlying sources
- Caveats and expresses confidence in analytic judgments
- Distinguishes between assumptions and judgments
- Demonstrates relevance to the stakeholder(s)
- Uses logical argumentation
- Exhibits consistency of analysis over time
- Makes judgments and assessments that are justified with supporting information

**018 And finally, the biggest criteria of them all is exhibiting proper standards of analytic tradecraft. Melissa alluded to this. Analytic tradecraft we look as an art and a science. So, the art is what's going on in your brain? What's going on in that analyst's brain? What are the experiences they have that are

influencing that? What's their educational background? What type of mood are they in? Is this a Monday morning or a Friday afternoon? That could significantly change the analysis that they're putting together.

And then it's a science. What tools are they using? What methodologies do they leverage to come up with this? That's important to capture when you're evaluating an intelligence product. It can be a little trickier in getting into somebody's brain. But this can help a little bit.

So, it's worth seven points. There's seven different aspects. What are the quality and reliability of the underlying sources? You'll see this a lot. You'll want to make sure that, if you're getting a product that's on a cyber threat, let's hope the source is, say, a malware analyst instead of a member of the janitorial staff. There's probably going to be a big difference in how they're assessing a threat. And you want to make sure you have the right type of sources in that product.

You want to caveat and express your confidence in analytic judgments. So, do you have a high confidence something's going to happen or a low confidence? And then what is your estimate of likelihood of this threat occurring? Almost certainly, about fifty percent equal or very low confidence that this is going to happen because you're very unlikely to see this event occur.

You want to distinguish between assumptions and judgments. Those are important. And it's important for whoever wrote that intelligence product to do that. The author of the intelligence product also needs to be relevant to the stakeholders. We kind of talked about this. Going to be different in how they're going to write that analytical assessment for a CEO compared to say the head of the security operation center or the SOC. For the SOC, you could probably get a lot more technical. For the CEO it's not going to have as much of an impact. That should impact how relevant that intelligence product is and then how it gets graded.

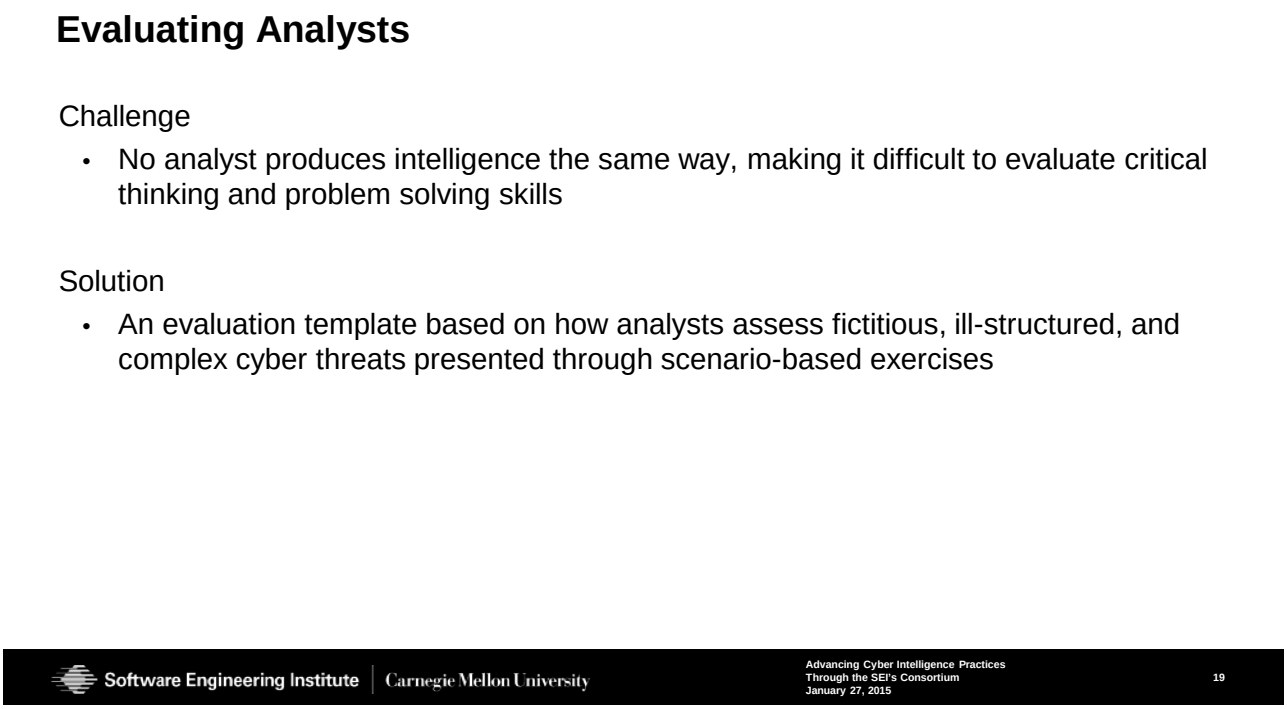
Using logical argumentation, consistency of analysis over time, and then making the judgments and assessments that are justified with the supporting information. You can probably see through these criteria we talk about supporting information a lot, very important that the intelligence product is based off of credible and reliable information.

So, when you put these all together it adds up to, if you're doing a great job, seventeen points. And you can grade accordingly on down. In the template that you can download, you have space to if you wanted to take any type of an example of an intelligence product and try this. You have fillable space that you can utilize in the PDF and then put in a score. And it will automatically tally it up. It can be a starting point for

putting together an evaluation cycle or process for evaluating intelligence.

And now, we'll move on to the second one, which is evaluating analysts.

Evaluating Analysts



**019 Melissa Kasan Ludwick: Okay. So, we'll spend a few minutes on how to actually evaluate cyber intelligence analysts. This really came about because no two people think the same. No two people have the same shared experiences. And no analyst produces the same intelligence the way another one might. This is really tricky for organizations to evaluate the critical thinking and the problem solving skills of both the workforce they currently have, and new hires that

they're looking to bring onboard as many of our organizations are right now.

So, a solution we're proposing to this is an evaluation template that is based on how analysts assess a fictitious, ill-structured, and really complex cyber threat. And it's presented through scenario based exercises. Now, we're suggesting that organizations would use this to either evaluate their current analysts, and then they'll be able to really see where they need some additional work, and then they can also use them for-- as part of the hiring process to look at interview candidates and prospective new analysts and really set them through the same scenario and kind of see what they come up with.

Polling Question 3

Polling Question 3

Are you interested in hearing more about the competencies and skills that make a good cyber intelligence analyst?

**020 So, the template, Jay will talk about that in just a few minutes. But I think we have a polling question first.

Shane McGraw: Yeah, we're going to give our fourth and final polling question here folks. And we would like to know, are you interested in hearing more about the competencies and skills that make a good cyber intelligence analyst. So, take about fifteen seconds or vote there. We'll continue to move on. We'll come back to these results here, Melissa.

Melissa Kasan Ludwick: Great. Okay.

Template – Evaluating Analysts

The template conveys a holistic approach to assessing cyber threats

- It consists of three components
  - Threat actor potential to execute the cyber threat
  - Organizational impact of the cyber threat on the target
  - Target exposure to the cyber threat because of potential vulnerabilities

**021 So, this template for evaluating analysts, you know if you step back, it comes in three different parts. So, you'll have a threat scenario. And you can really use any scenario. For example, you could use Stuxnet, and put your analysts through that scenario.

But at a very high level view, you're looking at three different components for this holistic view of assessing a cyber threat. The first one you're looking at the threat actor's potential to actually execute the cyber threat. Next you're looking at the organizations impact of the cyber threat on the targets, so you or your organization. And finally you're looking at the target or your organizations exposure to the cyber threat because of potential

vulnerabilities within your system or within your folks. So, now I think Jay will walk you through kind of each one of these aspects.

Shane McGraw: Jay, before we go there just a quick update on the poll. We got about seventy-nine percent looking for more information on the skills that make a good cyber intelligence analyst. So, if we could do a deeper dive there?

Jay McAllister: Sure.

Melissa Kasan Ludwick: Sure. Okay so, when we look at what makes up a successful cyber intel analyst-- and I'll point you again to the papers that you're able to download. We have a white paper on traits, core competencies, and skills of successful analysts. We worked with our members in our organizations, our previous research effort. And we really looked into what makes up a good cyber intel analyst.

And it's really kind of threefold. First are the traits. And these were things that can't necessarily be taught. You can certainly have them encouraged through coursework. But it's being curious, having an open mind, really wanting to dig into the details.

And then next you have kind of technical and strategic skills. So, you're technical skills, you're looking at computer networking, malware analysis, pentesting, red teaming, things that are easily taught in a classroom environment. And then

you're looking at more strategic or more softer skills. So, this is research methodologies and processes, critical thinking, communication, so the ability to write and communicate for decision makers or for your leadership.

So, I'm happy to talk more about this. This is a personal favorite of mine. So, I would encourage you to check out the white paper. We have a spider graph, and infographic there, and again, reach out because we're happy to talk more about this.

Shane McGraw: Terrific, let's move on.

Jay McAllister: Yeah, and I think just to touch on that one final. It really can depend, too, where the organization is at in their cyber intelligence kind of maturity. No, we don't like that word, just in how they're capability. What we'll see is if you-- if an organization has been around, say, an organization from the financial services sector, been focusing on cyber intelligence for a while now, say, since the mid, early '90s, they've got the resources. They've kind of got the people in place now that they can specifically hire for, say, a malware analyst. And all that person is going to do is focus on malware. They can hire the strategic analyst. And that person's going to focus solely on strategic.

What we've found, for a lot of organizations today, is they don't have that luxury quite yet. So, they need a renaissance man or a

renaissance woman that is a knower of all, master of none type of approach. So, the person in the morning can be sifting through indicators to put together an assessment for the security operations center, and then in the afternoon, turn-- taking that technical topic into a non-technical room of, say, the board of directors or the C-level executives or a senior policy maker in the government and having to talk them through here's the cyber threat and this is how it affects your upcoming acquisition or your upcoming movement of military personnel.

So, I think Melissa, I think we both see that that it-- currently, a lot of organizations need that kind of Renaissance man or Renaissance woman when it comes to the cyber intelligence work, which is tricky I think. For the individuals that have that, that's fantastic. You're in a good spot right now because that is sorely needed. And it's kind of a talent driven kind of marketplace right now when it comes to that aspect.

Okay, but we can go-- we'll now go back into evaluating analysts. And so, Melissa mentioned we have a template. This comes from research that we really sought. So, she mentioned we have three different aspects, threat actor potential, organizational impact, and target exposure. We put together this holistic approach because when we talked to organizations, what we saw was very interesting.

So, organizations, the couple that we saw in the federal government-- and again, we're not making any blanket statements like the whole U.S. federal government does this or anything. But the organizations that we interacted with were really focused-- when we asked them, "How do you prioritize threats? How do you assess a cyber threat?" they focused on threat actor. And that was-- that was their focus was the threat actor.

When we talked to organizations in industry, it made more sense for them, whether it was, say, the energy sector or the healthcare sector or the information technology sector was we'll just focus on the impact, the organizational impact, that a cyber threat would have on us. We're a product company, this is-- that's what we're focused on. We're worried about our brand reputation. So, we'll prioritize and assess threats based off of that.

Others would come and say, whether it was within the same sector or elsewhere, we'll look at our vulnerabilities. We know the vulnerabilities cost from our employees, from our contractors, from our Internet presence. And we'll assess and prioritize threats based off of that.

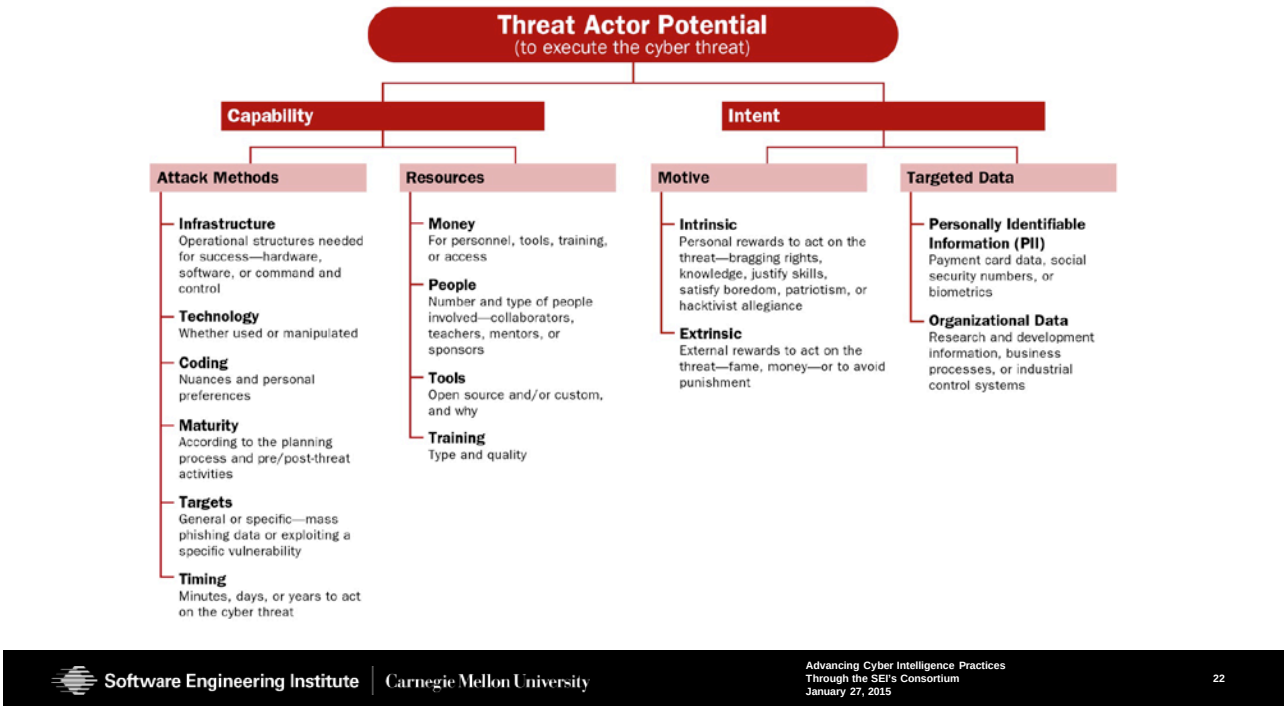
So, when we looked at if we're evaluating an analyst in a perfect world, this analyst would look at a threat from all three perspectives. And so, that's why we put together

this holistic approach and why we're looking at it in this way.

We've mentioned scenarios. We have developed actual scenarios that our consortium members have access to that they can utilize for potential hiring people or for taking maybe a baseline of their current analytical core. That will be available to the general public in the future. We'll probably look at the end of spring, early summer for that release. So, if you are continuing to follow the SEI, and at the end we have our own emerging technology center Twitter, you'll know when that stuff's available. But we mentioned scenarios because we do have some. They're just currently available for our consortium members.

So, in looking into these three different kind of aspects of assessing a threat--

Threat Actor Potential



**022 We've got some nice spider graphs for you. The first threat actor potential, to execute the cyber threat, we break that up into capability and intent. You want to look, within capability, the attack methods and the resources. So, you're seeing the potential of this threat actor or threat actors. What's they're infrastructure? What is there maturity? How do they go after a target? That can really change your approach to how you're assessing a threat.

Specifically for the target, is this something that they've been planning for two years? Or did the threat actor just create some new type of intrusion tool over the weekend? And it's a federal holiday. And nobody's at work. And so now, this is kind of a

target of opportunity for them. That's really going to sway how you can assess a threat.

When you look a resources, pretty basic. What type of money do they have? Where's the cash flow? How does that impact what they're able to do, the type of people that they have? What are the training of those folks? Do they have the Carnegie Mellon computer science background? Have they taught themselves on their own? That certainly should be weighed into how you're looking at the threat actor.

And then when it looks at intent, motive can really tell you a lot. It goes into kind of these human factors. Is it just personal rewarding? Does it give them their own internal sense of pride? Or are they being paid by an external entity to do this? Are they in need of financial resources?

And then the targeted data, what is it? Is it organizational data? Is it personally identifiable information? That's going to tell you a lot about the treat actor potential as well as kind of their intent.

Organizational Impact

**023 The next is the organizational impact of the cyber threat on the target. We look at the target as more an organization. But you certainly could look at it as an individual person or a group, any of those type of entities. And we break it down into operations and strategic interests. So, operations usually you can quantify when you're doing this type of an assessment or an evaluation of how an analyst assessed a scenario.

Related to kind of monetary quantifiability, you can look at direct costs. So, what would incident response cost an organization with this cyber threat? What would the down time look like for the business? How would that impact the bottom line, and then the mitigation and

prevention of moving forward or going back to clean something up?

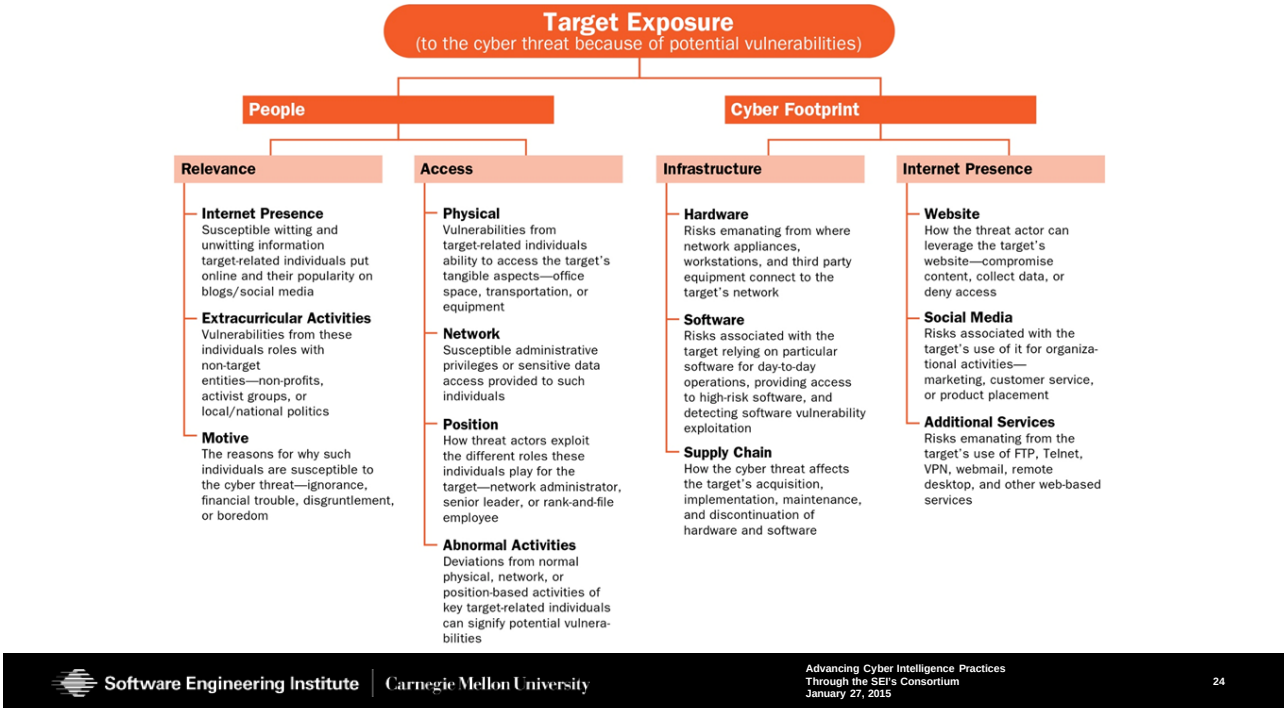
Business operations come into play as well. How will this cyber threat affect the supply chain? Or does it emanate from the supply chain? The logistics, how is going to impact all the different aspects of logistics for the organization? And then the future earnings, what's this going to look like for future acquisitions, for future R and D for the bottom line.

The strategic interests are usually not as easily quantifiable with money and numbers but certainly not any less important. When you look at organizational interests, how does this cyber threat relate to strategic planning? A lot of private companies have three and five year strategic plans. What's the impact on that vision? And how is that going to change if this cyber threat is effective or if it's already occurred? It just depends on at what stage of analysis it occurred, whether was the activity ongoing or has it yet to happen.

The stakeholders involved, I mean you're talking employees, external stakeholders, if you have a board of directors, if you have stockholders, that type of stakeholder. And then the culture, culture can play a big impact as well. Did everybody share desks so they have a lot more opportunity to get on a computer that is unlocked? Is there much more rigor when it comes to physical security? What is the culture of the organization?

And then your external interests, how does this cyber threat relate to the market and the industry of the organization? Geopolitical aspects of where, say, the organization has locations, partnerships, are they involved with their ISAC, or their information sharing and analysis centers? Brand reputation, how will this impact the brand?

Target Exposure



**024 And then for the final-- the third one, is the target exposure to the cyber threat because of potential vulnerabilities? And we break this down into vulnerabilities caused from people and cyber footprint. People is kind of obvious because there's always going to be a human involved. What's the relevant and what is the access with regards to people?

So, relevance, Internet presence, what's occurring when employees go home and get on social media? Are they providing information they don't think would be relevant to threat actors but is very helpful for threat actors? Extracurricular activities, we see this a lot with organizations, especially in the private sector. Are your board of directors, they're involved with your company. But they're also involved with other entities. Some of those entities might come under the microscope of hacktivists or nation states. And then you now indirectly have a cyber threat. What's your exposure because of that as it relates to certain cyber threats? That's something, when you're evaluating an analyst, they should be covering when they're looking at a different cyber scenario.

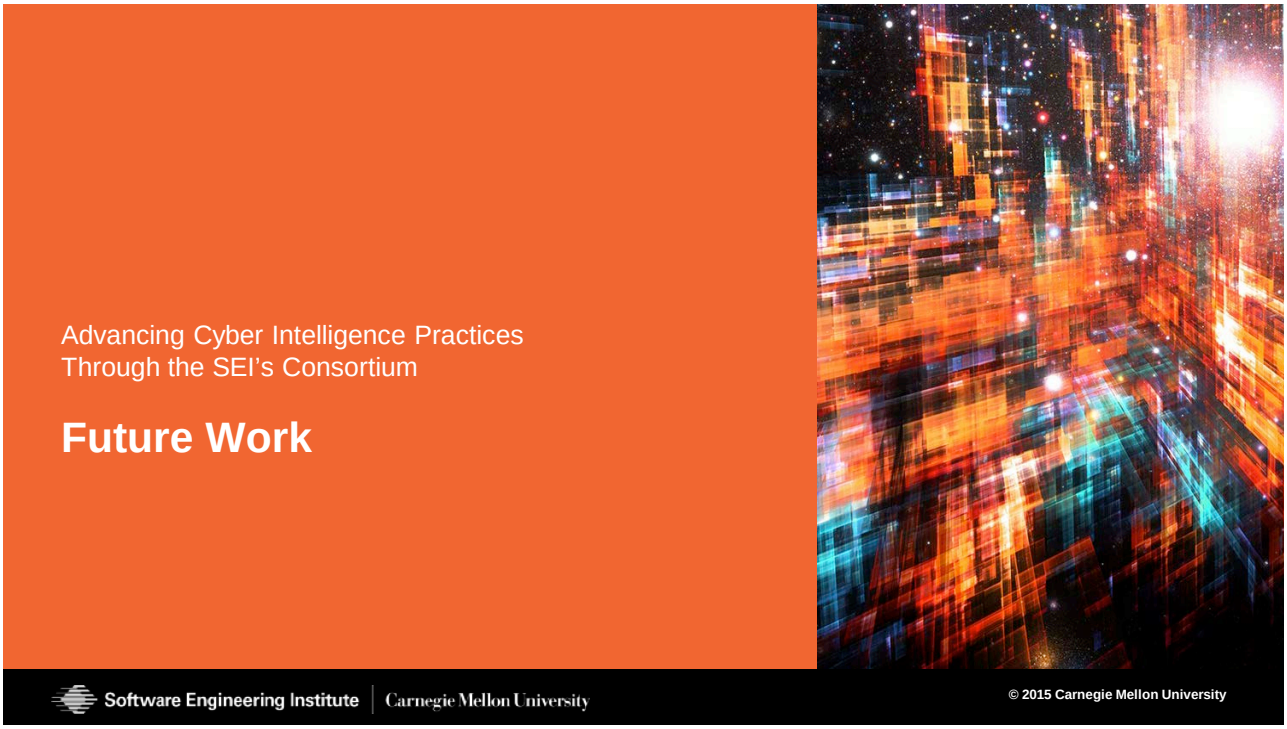
And then the motive. And for access-- pretty straightforward, physical access, network, their position, and abnormal activities. Usually, abnormal activities, establishing a baseline for what network administrators are doing can be time consuming, can be frustrating. But it certainly can pay a lot of dividends at the end when you start identifying your abnormal activities.

For cyber footprint, infrastructure, again pretty basic, what's your hardware, your software, and your supply chain? And then your Internet presence, is this organization-- does it have a website? If it doesn't, man that makes things a lot easier. Social media, and then additional services

that are available, can you VPN in? Can you telework? What's all the different aspects that that relates?

So, when you add these three together, you can assess how an analyst is looking at a cyber threat. So whether it's you're bringing in someone and you want to hire, or if you're looking at the current layout of your analytical core. I think a great example could be if you have ten analysts. And you kind of want to see we've got to devote the resources next year for their professional development. So, who's going to go to a conference? Who's going to go get some training?

If you put them through a scenario, and you had them do a write up, what we propose is you take the scenario, you take the write up that they did or the analysis that they did, you can apply it to these spider graphs. So, you can see where they're exceling and where they maybe need a little help. If all those ten analysts really struggle in taking a cyber threat and applying it to the organizational impact, maybe they need kind of a here's your company 1101 on what we do, who we are, and that type of information. That's going to be a telltale sign for you and can help you in that type of baselining and divvying up of resources.



**025 Okay so, enough of that.
Now, we'll go back to Melissa.

Melissa Kasan Ludwick: Okay, so I'll talk a few minutes about the future work that we have coming for the consortium. First, we are working to automate the templates that you have here for evaluating intelligence and evaluating analysts.

Future Work

Future Work

Automation of templates for evaluating intelligence and analysts

Implementation frameworks

- Predictive analytics
- Red teaming
- Intelligence collection management

Interactive platform for learning how to build a cyber intelligence capability

Crisis simulation

**026 As Jay said, right now there always available to our members first. Look later in the spring, early in the summer for them to be released to the general public.

And we're also continuing our implementation frameworks. Remember, these are our how to guides. We have three of them coming down the line focusing on predictive analytics, red teaming, and intelligence collection management.

Jay McAllister: Two of the other things that we're working on to finish up year one of the consortium is we're producing kind of an interactive platform for learning how to build a cyber intelligence capability, whether you already have one, whether if you're trying to figure out if you need

one, or whether you don't even work in this space, and you're kind of-- you're concerned or you want to-- you're interested in how it could impact what you're doing. If you think about it, cyber is a very general term. It touches on pretty much every aspect of an organization whether you work in HR or marketing or actually are a cyber intelligence analyst. So, cyber intelligence is important to you no matter what if you look at it from that perspective.

So we're trying to put together an interactive platform where all these different stakeholders can come together and learn how to build a cyber intel capability, again, whether they have one, whether they want one. Or, in a lot of cases, organizations don't have the opportunity to have a cadre of ten to fifteen cyber intelligence analysts. So, they need to outsource. They're going to have intelligence service providers. And there's many options out there. This can help in kind of identifying what exactly do I need.

And so, we're going to put that together. It's-- we're trying to be creative with it. So, we'll be a little dodgy right now. But hopefully, people will like it when it is produced.

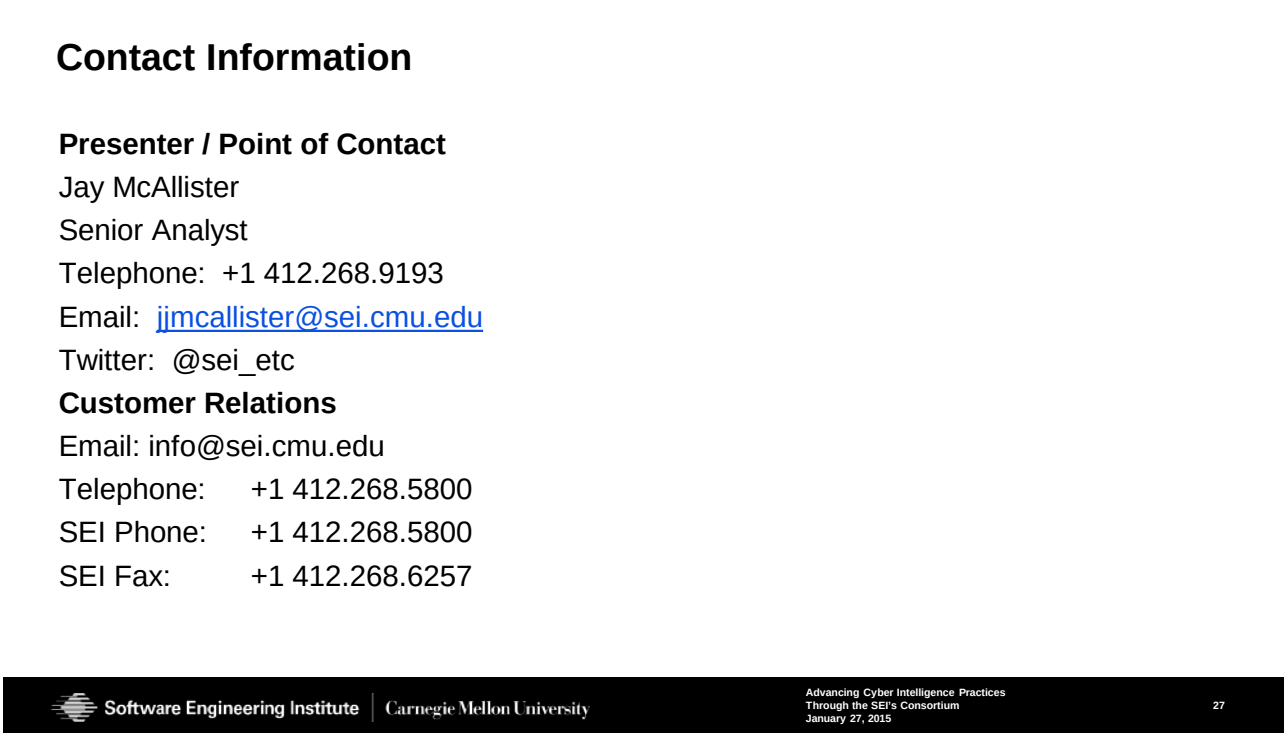
And then our crisis simulation, so you'll probably mostly hear about this as a war game. But we like to call it crisis simulation to be politically correct. This is going to be a great kind of capture the flag exercise where we're going to bring in the

strategic and technical analysts and put them through a very interactive crisis simulation.

We talked now just about evaluating analysts. And we showed you those three spider graphs, the three different perspectives an analyst should be taking for threat actor, organizational impact, and target exposure. Our crisis simulation is built off of those spider graphs. It's built off of that model. So, it's going to put analysts of our consortium members through that so that they are interacting in real time with cyber scenarios and cyber threats. And they're utilizing all the different aspects of those kind of threat assessment guide or model to make sure they're getting a holistic approach when they're going through those two days of the crisis simulation.

For our members, this will occur at the end of June. And after that, we'll see about making other versions available for the general public. But those are-- that's a lot of the bigger things we've got going on for the last six months of the consortium.

Contact Information



**027 We certainly thank you for your time in learning more about the consortium and the cyber intelligence work that we're doing. This is our contact information. If you're interested in going into more detail about anything we've talked about with regards to what we're focused on in cyber intelligence, or if you are interested in consortium membership, this is my contact information and then the general SEI contact information. Feel free to reach out.

We mentioned a lot of things will be coming down the road for the general public. If you follow our Twitter account which is @SEI_ETC, you'll get to know when all that stuff is available. And then you can head to the SEI website. You can also do that by following the SEI Twitter

account. We try to give you as many options as we can.

So, with that, turn it over back to Shane.

Q & A

**028 Shane McGraw: Jay, Melissa, thank you for the terrific presentation. Before we start our question and answer session, folks, I just want to remind everybody to please fill out that survey before exiting as your feedback really helps us drive and improve these future events that we may do.

So, let's get into our questions. From Florina asking, "How much do the other "INTs"-- it's H-U-M-I-N-T G-O-I-N-T contribute to your cyber

intelligence, government versus private sector?"

Jay McAllister: Well so, just want to distinguish, we're not the actual producers of intelligence. But we always stress-- and you can see it, I hope, in some of our models, especially in the evaluating analyst section, all the INTs should come into play. When we look at a strategic cyber intelligence product, it should be looking at human intelligence or human sig-int, which is signals intelligence if you're thinking NSA, Geo-INT, which is Google maps, or what the national-- or NGA does. That's your Geo-INT. There's Maz-INT, measures and-- now, I'm blanking. But essentially, for Maz-INT, we certainly promote or we talk about how can you augment your cyber intelligence collection capabilities.

If you just had sensors on all the towers of the computers in an organization, if that sensor gets hot on a Sunday at six in the morning, that should go back to some type of a watch center that says this isn't normal activity. We need to see what's going on. And if nobody's at that desk, well now what's going on? Has somebody already gotten in? That's another form of an INT that should be coming into play with cyber.

So, again, we aren't R and D capability. So, we're not actively producing real time intelligence. But when we put together the

methodologies, the processes, the tools, and the training that can help those operators doing the day to day work, we look at it from that holistic approach of bringing in every form of intelligence or every INT. And open source, too, that's-- there's always debate of open source falls in us-- some of the others, but you know, I'll just throw that out there as well.

Shane McGraw: Okay, from Jewel asking, "These analytic trade work standards, aren't they all based on ODNI's standards, or have they been revised for cyber?"

Jay McAllister: So, we've added to-- so, ODNI, the Office of the Director of National Intelligence, oversees the intelligence community. They should be that arm that kind of gives guidance for the whole intel community. So, we do have some standardization. That comes from-- that criteria is the general criteria that comes from intelligence directive 203. When we put whether our students here at CMU, we teach graduate level courses in cyber intel, or if we're interacting with our consortium members, we certainly put that cyber intelligence flavor to it.

So, when we're talking-- I'm trying to think of an example. So, the timely criteria for evaluating intelligence, that needs to have-- when you're evaluating that piece of intelligence, timely needs to be based not on the editing function of that internal organization, but it needs to be because this is a certain threat or

piece of malware, whatever it might be, if that intelligence product isn't relating the timeliness of that, how quickly a remediation needs to occur, then likely it probably need to happen hours ago. That's where we try to bring in the different aspects of cyber.

In the slides, it's probably looking at little more general. But when you're considering that evaluation criteria, yeah it's always applying it to the cyber domain.

Shane McGraw: Okay, next from Robert asking, "What are your thoughts about using personality trait testing, example Briggs-Myers?" Is that something you're familiar with in your work?

Jay McAllister: We are familiar with that. We've gone through a bunch of those ourselves when we have our team off sites and all that stuff. I think a lot of that-- so, when we first came up with the core competencies and skills, Melissa went through a session that she can talk about that really talked all these thirty different organizations we were interacting with about their core competencies and skills. And we certainly got a lot of comments about, "I'm starting to think in that space of the Myers-Briggs." And, Melissa, you can talk more about that.

Melissa Kasan Ludwick: Sure, so many of our participants when we were-- we were trying to gather this information, they talked about skills.

And as I mentioned, they talked about technical. But they also talked about more of the softer skills, the communication-- excuse me, and the research methodologies. And then they started talking about traits. So, yes, there was a lot of talk about a lot of this whatever makes up a successful cyber intel analyst is just natural them. They are naturally looking for more information. That's not something you might necessarily be able to teach in classroom environment.

So, there's some work being done right now that's really dong behavioral testing, similar to Briggs-Myers, during the interview process. And I think that's certainly an area that we could expand and we can look into more. Yeah, we'd definitely be more interested in that to actually look at some personality testing during the interview process and for your current analysts.

Jay McAllister: And a lot of that drove when put together evaluating analysts, or when we talked-- when Melissa talked earlier about core competencies and skills was how do I-- if I'm hiring for a malware analyst, technically, I know what questions to ask them. I know if I want to a CISSP, I know what I'm getting with that. But if I'm trying to figure out the more, I guess, softer science, critical thinking skills, problem solving skills, how can I figure that out? And that's where-- that was really the impetus for us to put together here's how you can evaluate analysts in

looking at it from those different perspectives because you'll see, one of the scenarios is you have an hour and twenty minutes. Here are five different pieces of intelligence from different INTs, give us a write up. Give us an assessment of your opinion of this cyber threat. And from that, you can kind of start to see those kind of critical thinking and problem solving skills.

But a lot of our consortium members and a lot of our organizations we interact with say, "Yeah, we went and did the Myers-Briggs." Or there's another one, DISC, D-I-S-C. And I know I'm introverted. I know I'm this and that. How does that, then, play into the cyber world? And we can get into a lot of good discussions with that.

For instance, we talked to a government organization that they-- to produce a strategic intelligence product, on average, it was taking them two weeks. If you think about that in the cyber space, that's way too long. You needed that in probably hours or at least maybe a day. But you're starting to push it.

They found that just by looking at some of this more softer science, they took their technical analysts and their strategic analysts that were in separate facilities and put them together in a way that complemented some of the introverted and extroverted natures. And that reduced that time. And it's kind of silly to think this was all you needed

to do. But by having them sit next to each other, the two weeks went down to about three days, so just an example.

Shane McGraw: Okay, this question is for me from Abdul asking, "When can we get an encore of the materials of this lecture?" So, we're not done yet and people want an encore already, so good job.

Again, it's being archived. So, it'll be up tomorrow. You can log in the same way. As for the materials, just go to the files tab right there. And you can walk away with everything today.

From Dawn asking, "What outcomes are typically revealed in cyber intelligence? Can it be unauthorized access, loss of data, tampering with data erosion, performance, denial of service? Or is it all of the above?" Is it--

Jay McAllister: So, it can be all of the above. I'll also mention, if Melissa wants to chime in too, I would say overall, the biggest challenge that we see from organizations, some even saying, "Don't even bring it up. I don't want to go down that road," is return on investment. So, I think that's maybe caveat, getting a little bit away from your question. But you're right, all of the above will constitute as kind of outcomes. It really depends on the stakeholder. Again, the CEO's going to want to know something very different from if you're going to talk with physical

security if they have-- if they're relevant to a cyber threat.

But the return on investment is incredibly difficult. We thought, going to the financial services sector, that that would be maybe the least concerning for them because they could tie it back to money. And we were wrong. Some organizations would say, "Okay, yeah every two weeks, I'll show here's how much money I've saved the bank because we didn't have these intrusions or these accounts weren't taken from us." We want to a bank down the street. And they said, "Well, we consider that soft money. So, we don't-- that's not considered credible when we do our forecasting or when we have those bi-weekly C-level meetings." So, it's very difficult.

Shane McGraw: Okay, Robert would like to know, "Are you aware of FBI regional outreach programs on the topic of cyber intelligence to help establish industry awareness? And if so, do you have any comments?"

Jay McAllister: I know there's a lot being done within the federal government. And I think we have to hand it, at least from what we've seen with ODNI, the FBI, DHS, and NSA trying to work together to get these type of regional developments. I think, obviously, there's probably a long way to go. And we're not as pleased with the progress. But I think they're doing a lot of great work. There's a lot of entities out there that can be helpful.

So, you've got the ISACs. You've got the information sharing and analysis centers. Those go by sector. But I also know there's talk about of bringing the different-- of doing overlap and bringing all the sectors together. I know they continue to work. And the FBI is great with working on trying to make the relationships between the public and the private sector so it's not just a they come and take and never give back. I think they're trying to work on that.

You have place, I mean just here in Pittsburgh, so we've got NCFTA, that National Cyber Forensics and Training Academy. That is a great kind of entity that can bring together these government and non-government types from across a whole bunch of different entities to share information at a more regional level. So, yeah I mean I think that's probably where we can end our comments because we know there's a lot of initiatives out there. It's probably not as fast as people would like. But I know they're certainly trying.

Shane McGraw: Okay, great. From Phil wanting to know, "What decision supports system, or DSS, tools should we be feeding our threat info into for helping us to one, assess threat levels, and two, helping us quickly optimize our own decision making?"

Can we comment on specific tools?

Jay McAllister: We'll probably have to get back to you on that one. I

think overall, we could state that the vast majority of organizations that we talk to, they might leverage some tools. But they have the most success with making their own internally. Some of them will get some tools and then kind of tear it apart and make it their own. So, I think anything that allows customization can be helpful. I'm sorry that's not probably as specific of an answer as you'd like. But follow us on Twitter. And we'll give you some feedback following that up. I think that's a great question we can take to our current consortium members and see what they're currently using.

Shane McGraw: Great. We've got about a minute left. So, we'll wrap up with this one from Keith asking, "Is there currently a database or group of people that keep track of how companies have reacted to cyber threats that could be then accessed and used as part of actionable intelligence? This being for a company or analyst dealing with a situation."

Jay McAllister: Melissa, any--?

Melissa Kasan Ludwick: Yeah. I mean I know there are folks that are capturing that information. And they're capturing the threat information. To my knowledge, I'd be happy to look into it, but to my knowledge, there's not any one thing that would be given out publicly and accessible that way.

Jay McAllister: Yeah, I mean I know there's-- it's a little tricky. And I think we're pausing just because as a federally funded research and development center, we're not going to-- we can't really say this is the best place to go to or give that type of stamp of approval. We just-- that's not the space that we operate in. but I know that there are opportunities out there. I think if you looked in maybe more of the intelligence service provider realm, even just Googling intel service providers, you'll get I think a good listing of organizations that are offering those capabilities.

Shane McGraw: Okay, folks, we are at two thirty. That's all the time we have for today. Again, thank you very much for attending today's webinar. Again, fill out that survey upon exiting. And everyone have a great day. Thank you.