Resilience Panel - CERT CS2 Team

Table of Contents

CRR Domains

CRR Domains

The ten domains in CRR represent important areas that contribute to the cyber resilience of an organization.

The domains focus on practices an organization should have in place to **assure the protection and sustainment of its critical service**.

CRR Domains	
AM	Access Management
CTL	Controls Management
CCM	Configuration and Change Management
VM	Vulnerability Management
IM	Incident Management
SCM	Service Continuity Management
RM	Risk Management
EXD	External Dependencies Management
TA	Training and Awareness
SA	Situational Awareness

**001 ~~~
Announcer: And welcome back to the SEI virtual event CERT Alignment with Cyber COI Challenges and Gaps. Next on the agenda is the resilience panel discussion, and it'll be moderated by Matt Butkovik of CERT. And Matt is the Technical Manager of Cybersecurity Insurance within the CERT division. He performs critical infrastructure protection research and develops methods, tools and techniques for managing risk. He has more than 15 years of managerial and technical experience in information technology, particularly information systems, security, process design and auditing. Across the banking and manufacturing sectors.

And now I'll turn it over to Matt to introduce the rest of the panel. Matt, all yours.

Presenter: Thanks, Shane. I'm joined today by Katie Stewart. Katie is a senior engineer and member of the technical staff here at CERT, along with myself. Our work focuses on risk management and resilience, and she's joining us remotely from Chapel Hill, North Carolina today. So greetings, Katie.

We're also joined remotely by Sean McCloskey. Sean is the Branch Chief for Stakeholder Risk Assessment Mitigation with the Department of Homeland Security's National Protection, and Programs Director at NPPD, and the Office of Cybersecurity Communications. In addition to his service at DHS, Sean is also a marine. He's been a reservist for 19 years in the Marine Corps, and he's an active drill reservist.

Also joining me here in Pittsburgh is John Haller. John Haller's a member of the technical staff here at CERT, focused primarily on supply chain and resilience. John is a former field artillery officer and a U.S. Army veteran. So greetings, everyone. Thank you for joining us.

So I wanted to provide a little context to this panel and how it fits with the overall message of the day. So we've heard a lot of technical detail. Bob Behler gave us an idea of how software, for instance, is affecting the aviation community. We're going to talk about core concepts of resilience. So how can you ensure your organization can meet its mission

when it's faced with destructive events? The folks that we have assembled here today all work in programs designed to measure the resilience of organizations. And this is one of the Department of Defense challenge problems, which is how do we ensure that infrastructures are resilient? And more specifically, how do we create measures in a system of measurement for those infrastructures

So we're taking up a level from Rhiannon's very great talk on a very technical subject to a more generalized governance and management discussion of resilience. But that's not to say that there isn't detail. So we will step through the ways in which all of the panelists have constructed tools, techniques and methods to assess cyber resilience.

So let me just kick off with a question and then we'll go to each of the panelists for an answer. So I would like each of the panelists to please describe briefly how their programs assist organizations in determining their cybersecurity posture. So that is what have you done to measure the cyber resilience or cybersecurity of organizations? And let's start with Sean, please.

Sean McCloskey: Sure. Thanks, Matt. As Matt said, my name's Sean McCloskey, the Branch Chief for Stakeholder Risk Assessment and Mitigation within Cybersecurity and Communications at DHS. Our

primary mission as a branch is to go out to different critical infrastructure facilities across the country. We cover all 16 different sectors of critical infrastructure, and we help them conduct assessments all based in a cyber realm. So we have several different assessments but our primary methodology is the cyber resilience review.

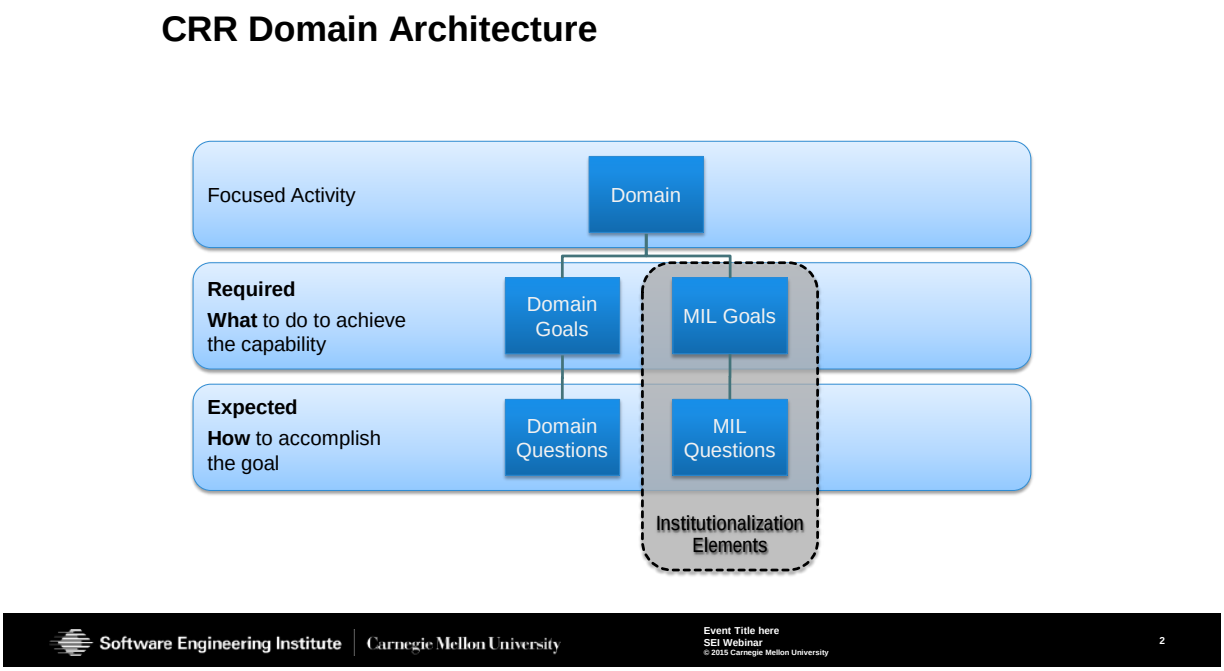
The cyber resilience review is based on the resiliency management model from the CERT SEI. One of the things that we did with working with the SEI is we took the 20-plus process areas within the RMM and condensed them into 10 functional areas that we call domain areas. So things like asset management, configuration change, risk, external dependency, situational awareness, the things that are, you know, those, there's about 10 different process areas that we focus on. And the thing that makes the CRR a little bit unique and different from most, from many technical assessments is that it's not controls based. It's based on process. So we're trying to come in and get an idea of how well an organization manages cybersecurity from, you know, from internally.

So we're focused on practice. We ask, "Are you doing these specific practices?" But we also try to identify how mature those practices are. So the assessment itself is, comes in two different flavors. We have a downloadable self-assessment package that is part of the CQ voluntary program that was released

via executive order last year. And we also offer a facilitated version to critical infrastructure owner/operators. Usually takes about six to eight hours we ask for, to conduct the assessment. We come in, we talk with folks from IT operations, IT security. Sometimes there's personnel folks in there. It's a mix of folks throughout the organization that we ask very focused practice questions and there's 10 critical domain areas.

One of the things that we also try to focus on is we don't try to focus on an IT infrastructure at large. We try to identify those critical services for an organization that have IT underpinnings. And we try to select the most critical for that organization. So we get a very narrow slice of what they're doing, but we're trying to identify what's most crucial to them and how they protect it with process and people. And so I'll just tie it up with--

CRR Domain Architecture

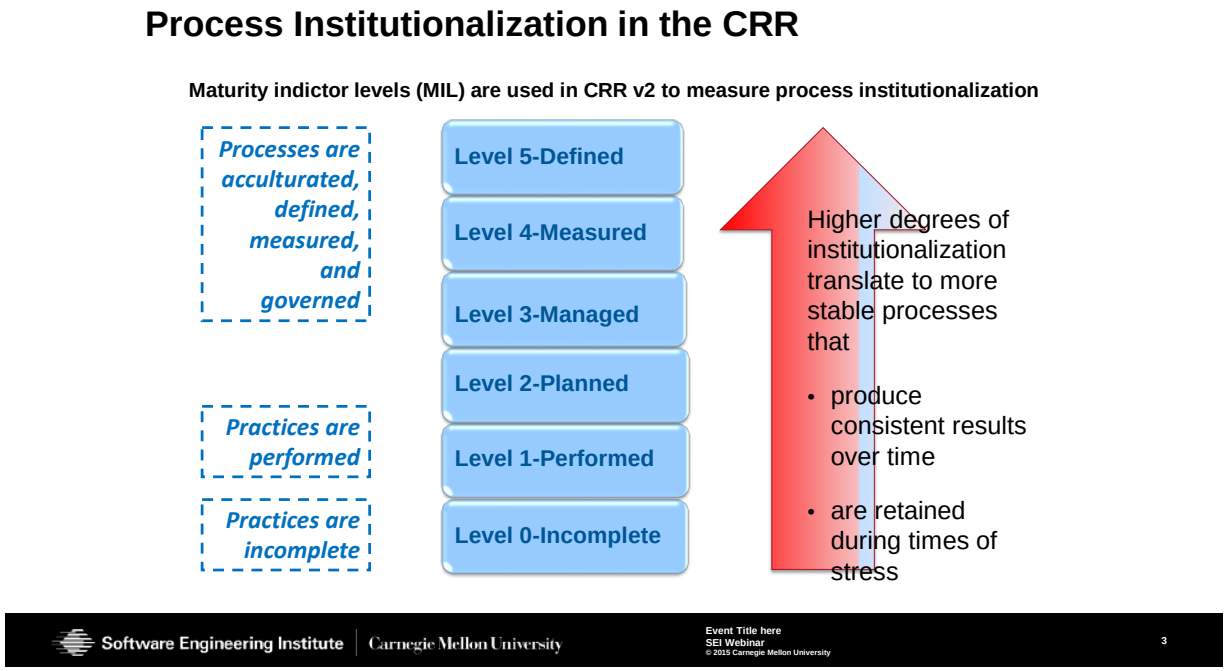


**002 --one of the key concepts with this also is when we talk about cybersecurity assets we talk about four different areas.

We talk about the people associated with it, that run it and work with it. The technology itself that is stored, the routers, switches, servers, computers. The facilities that house those people and that technology and then the information that's actually processed or required to process on that system.

We have three different ways you can answer these practice questions.

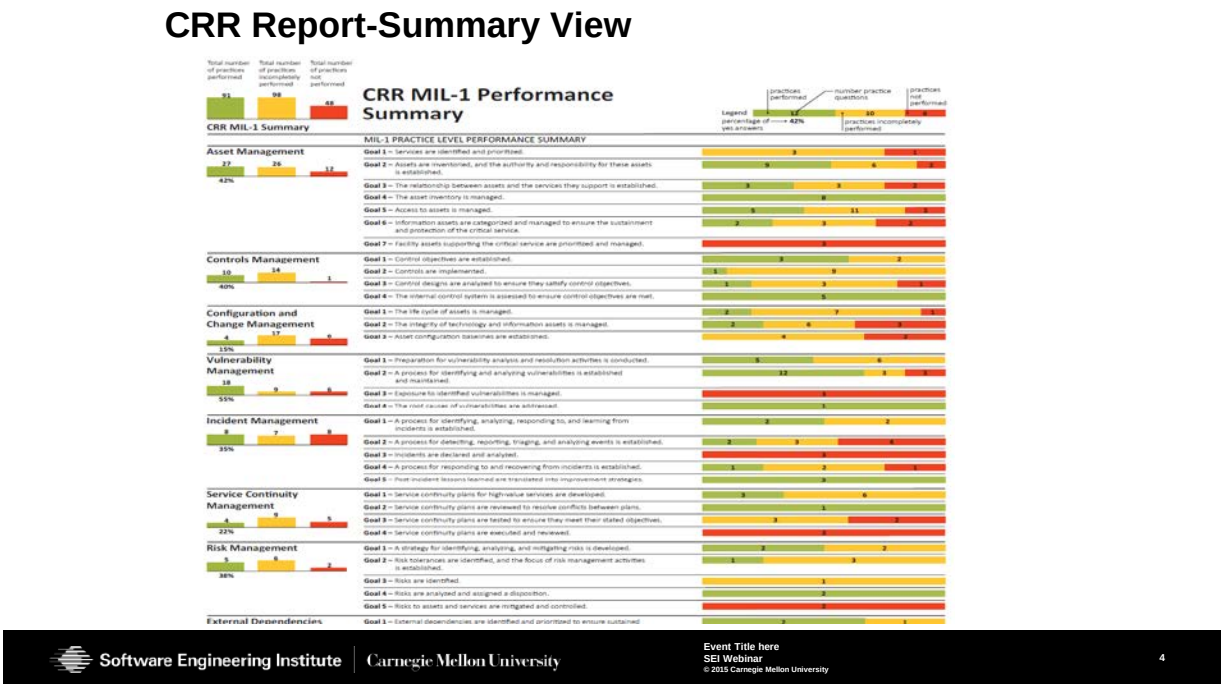
Process Institutionalization in the CRR



**003 There's "yes, we're doing this process," "no, we're not doing it at all," or somewhere in between. So incomplete answer. So there's a "yes," "no," and an "incomplete." As I mentioned, we also try to assign a maturity level to those practice areas or domain areas, starting with level one being that these practices are completed or performed. So that's a "yes" answer to all the different questions. And we try to identify, "Is there a plan to do that particular function?" For, say, asset management, is there a defined plan to conduct asset management? That would be a level two maturity. Level three would be managed. That you're actually applying people and resources to that. You know, that it has an actual budget line and it's a tangible thing within your organization. Level four is measured.

There's metrics being taken against that particular process and then level five is, it's common knowledge throughout the organization. It's well, it's defined, it's repeatable as a matter of course and policy policy throughout the organization.

CRR Report-Summary View



**004 So that's what I mean by maturity when I say that. Most of the organizations that we look at come out between a zero and one. So as part of our future plans for the cyber resilience review, we're trying to identify how an organization can improve within that zero to one range. So we've developed with Carnegie Mellon's help a different view between that zero and one level of maturity.

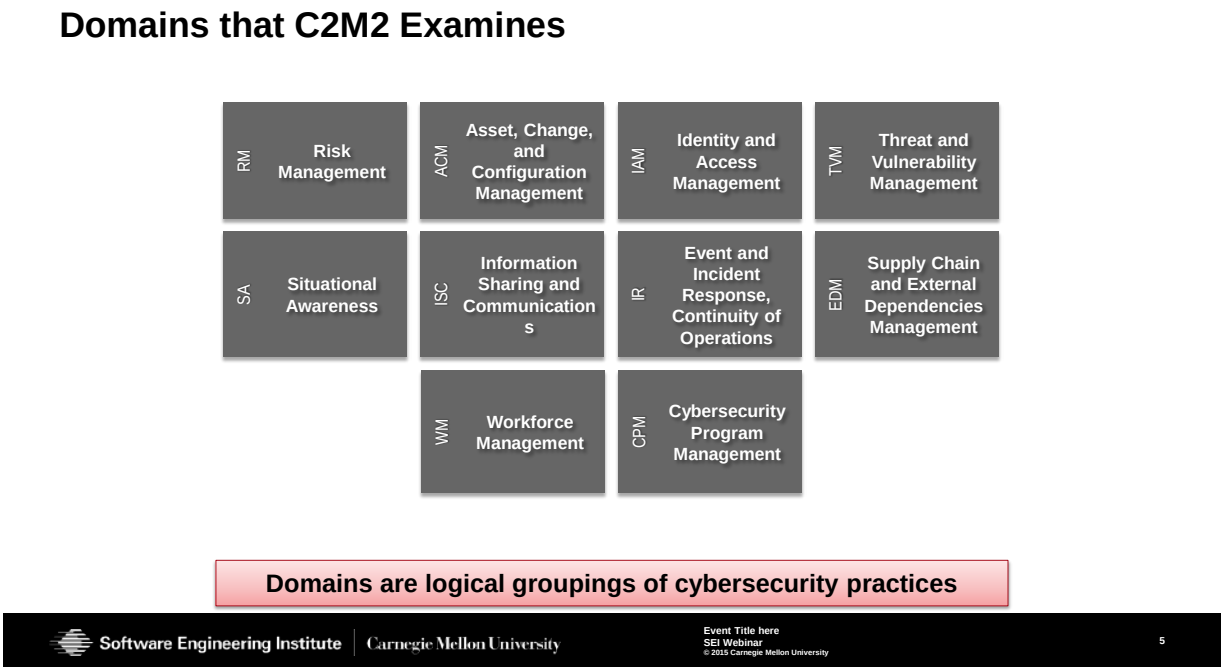
Okay. So... And that's really all I have on that, Matt.

Presenter: Thanks, Sean. Thank you for the overview. I know that this is a--there's a lot to unpack there, but thank you for the overview. There's a few themes we'll hear again from the other presenters, which is taking abstract concepts of resilience and then articulating those into usable tools. In the case of the cyber resilience review, it's taking the critical infrastructure owners and operators, giving them the understanding not only of the absence or existence of practice, but the institutionalization. In our context, we refer to that as the maturity of those practices.

So now I'd like to ask the same question of Katie. Katie, if you could please give us an overview of the methods and items you've constructed for the Department of Energy to gauge and to measure cyber maturity.

Katie Stewart: Sure, Matt. So the ES-C2M2 is the electricity subsector cybersecurity capability maturity model.

Domains that C2M2 Examines

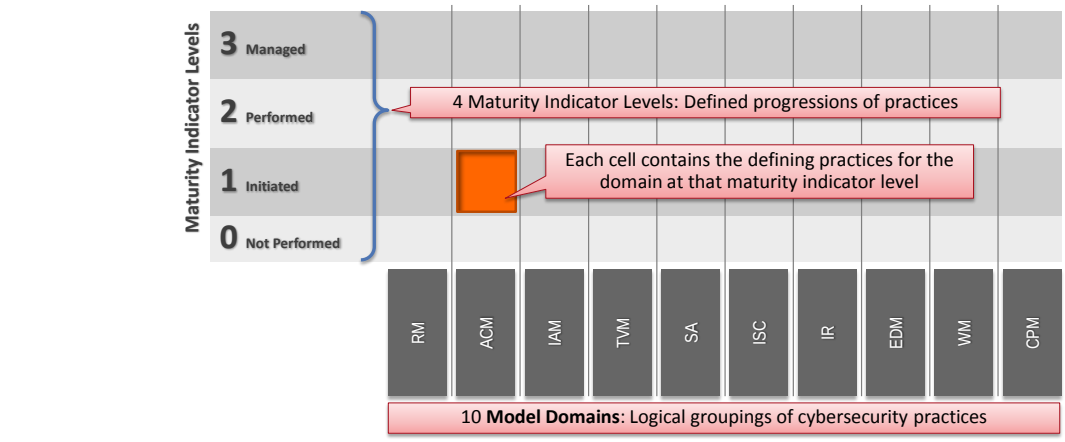


**005 Work began on the C2M2 in 2011, after the White House issued a challenge to understand the cybersecurity posture of the grid.

So Department of Energy sponsored an effort to pull together both private and public sector folks across the electricity sector to develop this model to help to try and understand the posture put forward by the White House memo. CMU CERT, we participated as the model architect. What we brought to the table was, as Sean mentioned, the resilience management model work, and we were able to facilitate the development of C2M2 in about six months. So it was very fast-paced deliver, development. We iterated it, tested it with industry and put it out there for use. The ES-C2M2 is not meant to be a compliance tool. It's

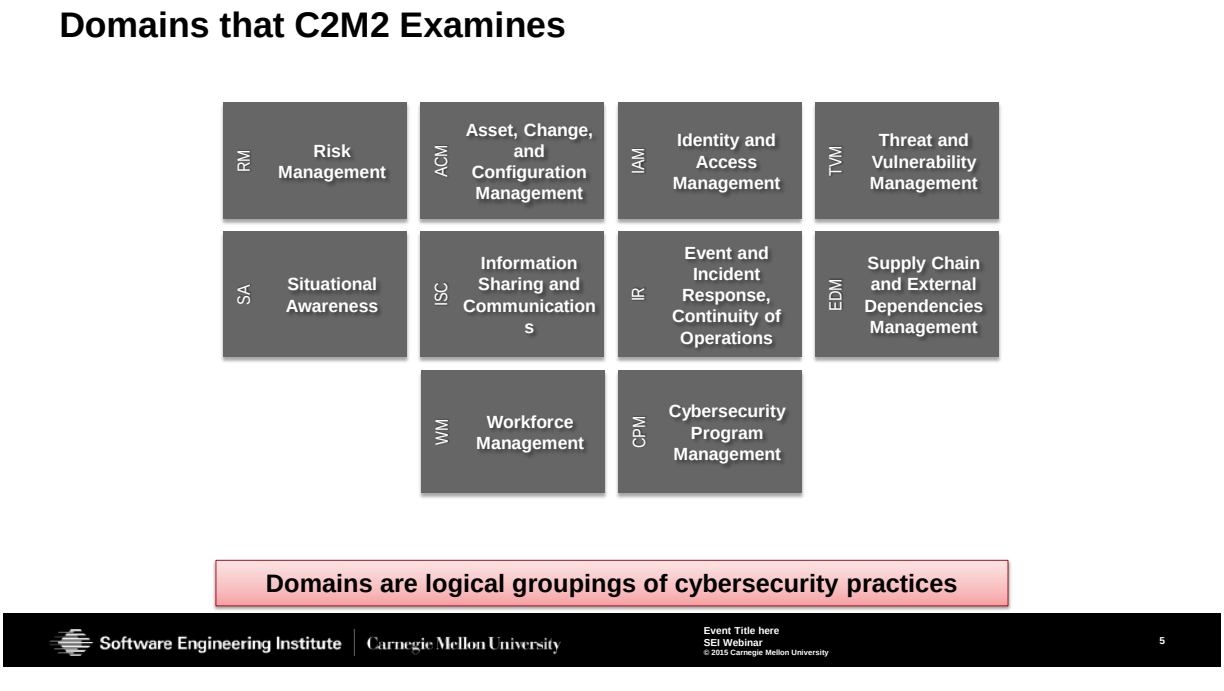
not meant for regulation. It's meant to be a tool to be used by utilities to understand what their biggest risks are within their organization. So what comes out of it is a--

C2M2 Structure



**006 --framework where utilities are able to understand their risks and either choose to accept them or make a plan to address the risks that are put forward. I put--I think there's a slide up now on the 10 domains in C2M2.

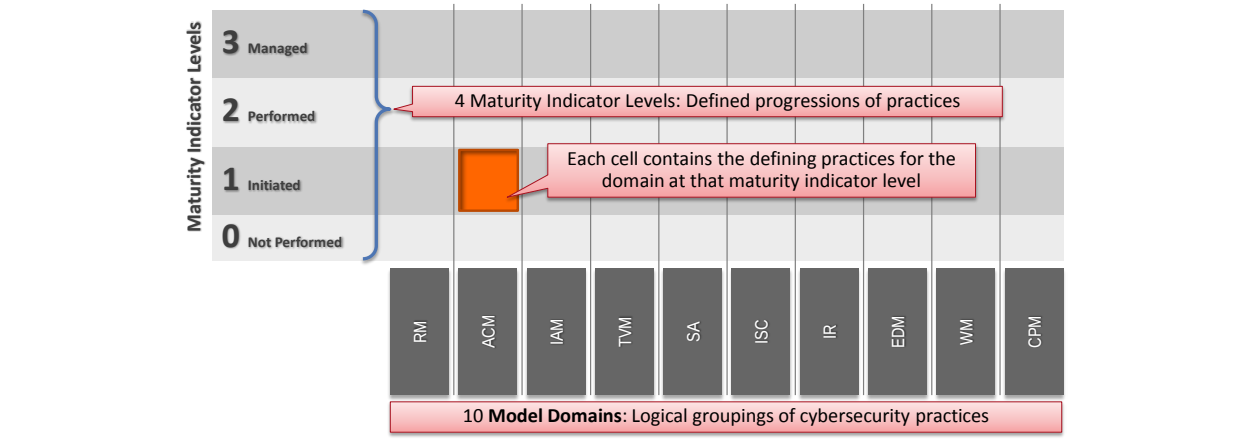
Domains that C2M2 Examines



**005 Similar to the CRR, these were the 10 domains that we decided were most critical to the electricity subsector. And we developed the model using these 10 domains or these logical groupings. And created it in the vocabulary for the sector in a way that could be easily digested and answered.

Again, the facilitations are done in about a one-day period, you know, six to eight hours, and there's a set of questions that go along with answering the maturity levels for each of these.

C2M2 Structure

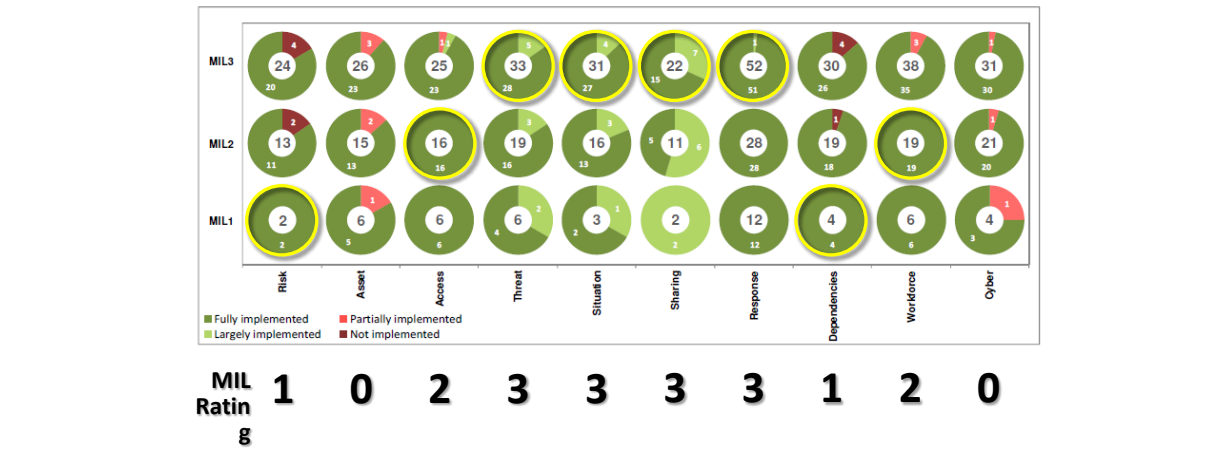


**006 Our maturity levels are a bit different, but again, you know, we're putting-- than the CRRs, but again, we're putting forward a scale to which organizations can, number one, understand their maturity and as they implement practices to improve it, be able to take measurements and see them rise above, you know, rise up the scale. It's like too, Matt, the structure that we used are a zero, one, two and three. A level zero would be no evidence of the practice being performed at that level. A level one would be initiating perhaps the processes being performed ad hoc. I like to refer to this as the beer truck test. If someone came in and got hit by a beer truck, couldn't come into work, would the process still go on? If not, they're probably in the initiated state.

The performed is very similar to the CRR. This is a documented process. You can refer to it. We have the proper trained people in place to do this process.

And then the managed process within C2M2 is the process that you're evaluating for effectiveness and making improvements on as needed. The last slide put forward is kind of this, a summary score.

C2M2 Sample Summary Score



**007 So again, this is what a utility or an organization who chose to . This is the type of that they would receive. It's a picture. They can see where they're performing well, where they maybe need to improve, and really what are the low-hanging fruits. So for them to go up in maturity level in one process domain, maybe there's a

smaller step that could be done. You know, because obviously we have to weight costs and as utilities make improvements.

Couple other points on C2M2. It's been used to evaluate the IT services side as well. With very good success. And as a result of that, we're making improvements to the model. The other thing I'll say is DOE, Department of Energy, has sponsored the development of material and guidance for using the ES-C2M2 model to align with the NIST cybersecurity framework that was published. All of this is online off the Department of Energy website, a simple search for C2M2. It's downloadable. You know, I think you just have to put in your e-mail address, but it's all publicly available and again is put out there for utilities to use this as a tool in their risk management, so...

Presenter: Well, great. Thanks, Katie. And I should probably explain. Each of these methods probably could merit its own half-hour webcast. So we're covering a lot of ground here. I should mention that the cyber view that Sean was describing is also available for download from a DHS website that we'll provide in the show notes, or in the webcast notes.

So in concept, the two are very similar in many ways. I'd like to transition to the third method that we'll discuss today, which is the external dependencies management

analysis work that John Haller's doing in support of Sean's program at the Department of Homeland Security.

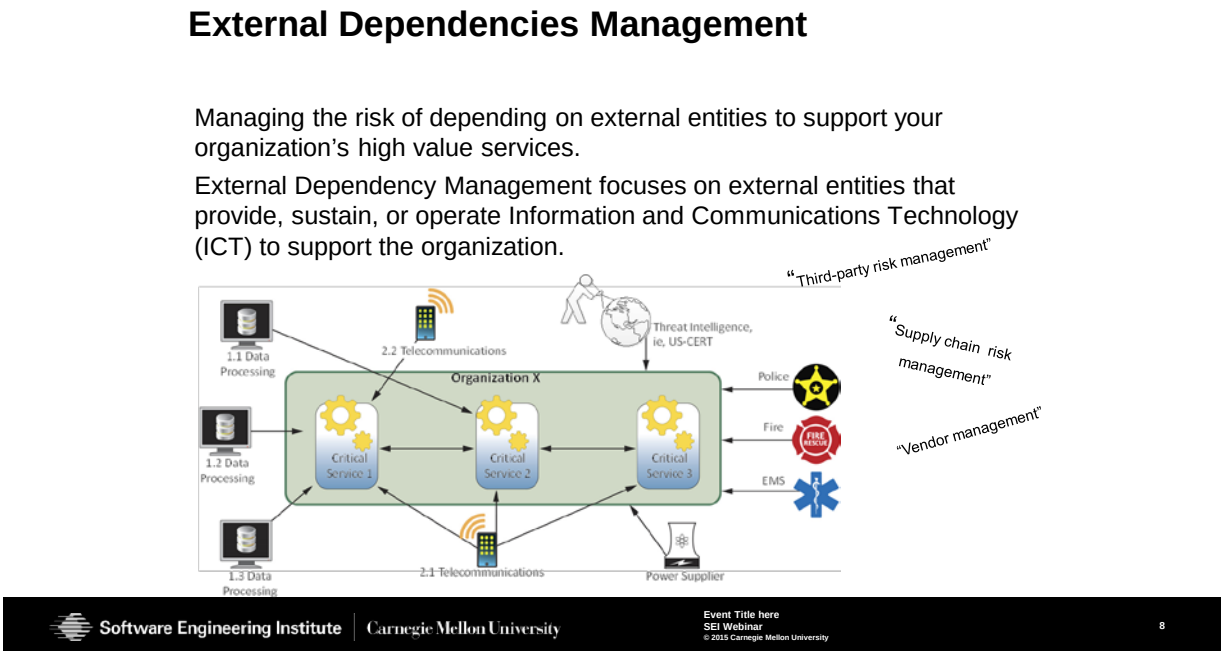
John, just for the sake of time, if you could please give us a very quick high-level overview of--

John Haller: Sure.

Presenter: --of what we're trying to achieve and how we do it.

John Haller: Sure. My pleasure, Matt. So what I'm working on is essentially an external dependencies management assessment. Now, it's closely based on CRR in terms of how it's structured.

External Dependencies Management



**008 In fact, the way that we present an organization's score or maturity is pretty much very similar to what the

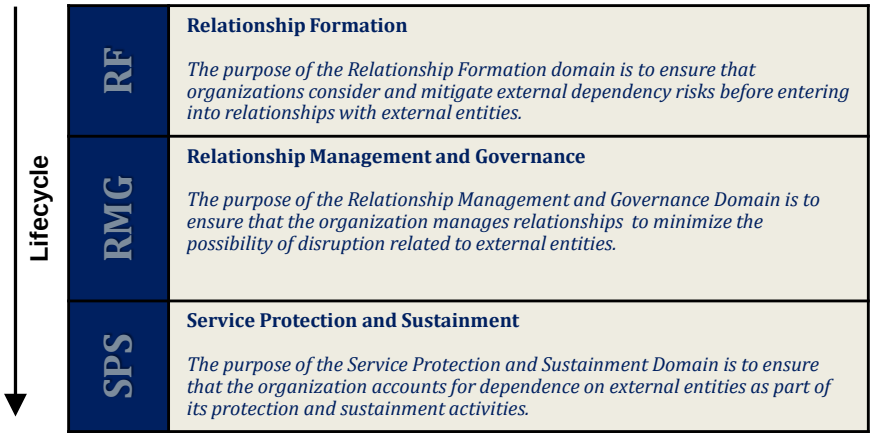
CRR does, so I'm not going to go into that in any real depth.

What do we mean by external dependencies? So it's basic question. This is any time your organization relies on outside parties that supply information and communications technology or that support your organization's use of technology. Or any time your organization relies on third parties that use cyber technology themselves, right?

In different sort of infrastructure sectors, it goes by different names, and one of the challenges in this area is different stakeholders call it different things. You know, in the financial sector it's called third-party risk management. DoD refers to it as supply chain risk management. Frequently when DoD uses that, or often when DoD uses that term, they're referring to malicious tampering of hardware and software or concerns about counterfeit hardware and software. The external dependencies management assessment assesses an organization's ability to manage.

EDM Assessment - Domains

EDM Assessment - Domains

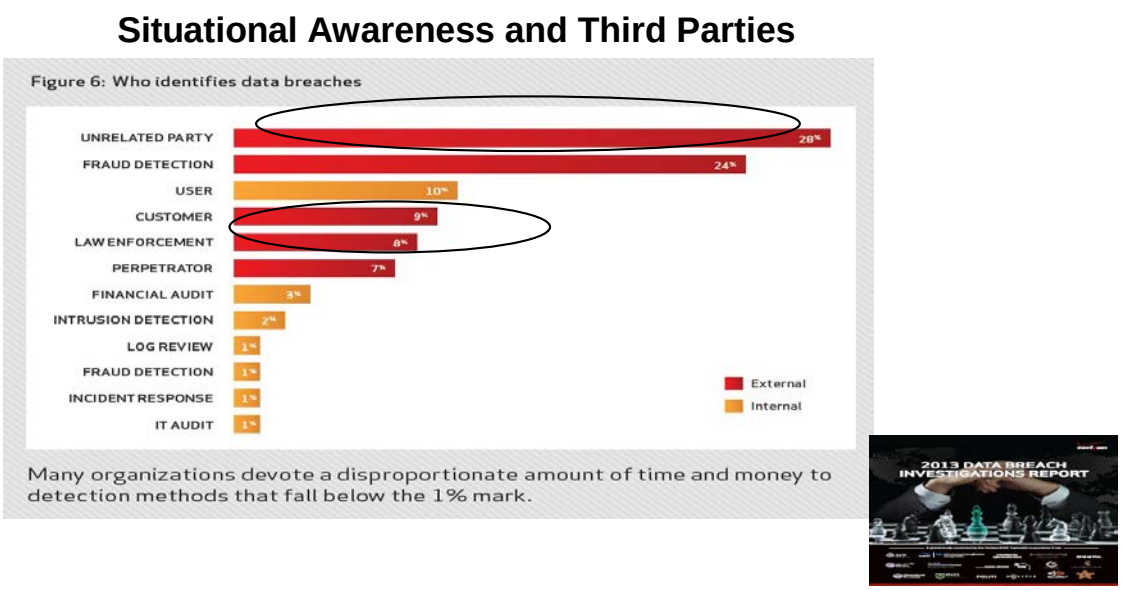


**009 And the organization's capability to manage and sustain the management of all of those problems, external dependencies broadly.

So as Matt and Sean have sort of mentioned, we're looking at the practices that an organization has in place to manage the problem. What do the people and the managers actually do to manage that problem? How well do they do it? And then as Katie really highlighted, do they actually sustain that over time so that if there's a disruption that happens can the organization continue to manage the problem? And when I say disruption, that can mean different things. It can mean an actual event, a disruptive even. Whether it's, you know, a physical attack or a cyber event. But particularly in the supply chain space

it can also mean things like changing services, changing vendors, changing contracts, mergers and acquisitions. There's lot, there are a lot of things that were events that can disrupt how an organization manages supply chain and external dependencies.

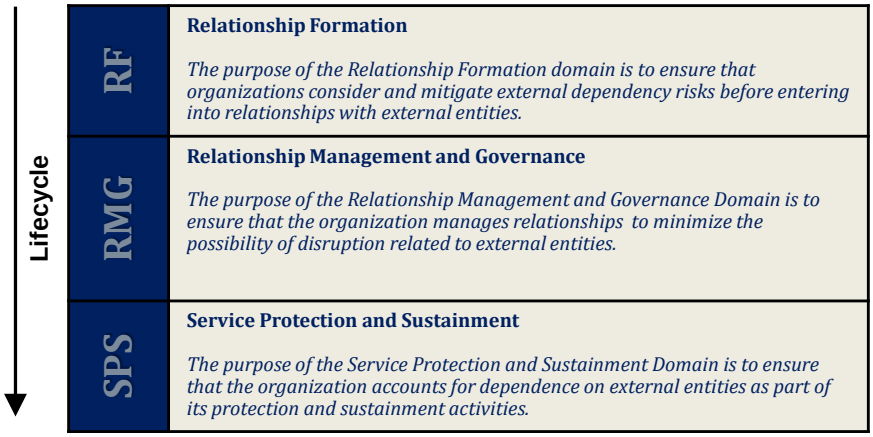
Situational Awareness and Third Parties



**010 In the actual assessment--

EDM Assessment - Domains

EDM Assessment - Domains



**009 --Let's just stay on that slide, in the actual assessment we're talking about three areas which also roughly correspond to domains. How well the organization forms relationships with outside parties or with third parties to support the organization's critical services, right. How well the organization manages those relationships over time, right. And when we say manages those relationships, we're kind of talking about lots of different things, right. Are you actually talking to third parties and contractors about risks? Are you making sure they are managing vulnerabilities? Are you managing the access that third parties may have to your organization? And this is very similar to kind of the target scenario and the target breach, which probably a lot of

folks watching, hopefully a lot of folks watching are familiar with.

And then the last domain, service protection and sustainment. We're really focusing on business continuity and incident management. How well is the organization incorporating those third-party considerations in incident management and service continuity as well as situational awareness? So really it's meant--we, you know, I think to sum up this section of the work specifically. It's an adaptation and focused use of the resilience and CRR approach. It focuses specifically on external dependencies/supply chain/third-party risk. Different folks call it different things. And it provides the organization or any organization the ability to have more confidence in how it manages those types of concerns over time, not just at one specific point in time, but in the future in a repeatable way so that it could have more confidence in its operations.

And I guess I'd also close by along the lines of what both Katie and Sean highlighted, we're really focused on the--in this work specifically we're focused on the critical infrastructure space in the United States, ranging from financial institutions, electricity, water power, oil and natural gas, et cetera.

Presenter: Sure. John, thank you for the overview, just to build on that point. So I think it's fair to say that all three of these methods are

designed to ensure the owners and operators of critical infrastructure have confidence their ability to whether a disruptive event and protect things the best possible. So I think from the perspective of the federally funded Research and Development Center, sponsored by the Department of Defense, we are supporting the mission to protect the homeland in constructing these things.

Which leads me to my next question. And John, let's take this question to you first. We know that the vast majority of infrastructure in the U.S. is privately owned. Something like 83 percent. We know that the Department of Defense is dependent upon this infrastructure, in addition to defending this infrastructure. So there's points of intersection between what the DoD needs and what private industry's providing. So if you could just speak briefly to the way that you see external dependency management supply chain, and managing the supply chain, helping the DoD in its challenge based in cyber.

John Haller: Right. So I think that there are a lot of intersections and there is a lot of potential here. So one of the--and I think Sean spoke about this a little bit--one of the foundational concepts of the CRR is the idea of critical services, right. So critical infrastructural organizations have certain core services and we can kind of all name them, I think. If it's electricity distribution, if it's an

electricity company, it's distributing electricity. If it's a bank, it's something like account management, right. There's a corollary on the DoD space. They might not call it critical services. They might call it mission capability, right. In other words, there are core service or mission capabilities that whether it's the Army, Marines, Navy or Air Force, they rely on, at this point in our history, they rely on information and communications technology to help them provide that mission capability, right? You know, if it's land warfare, we're talking about fire direction. Right. Or naval capability, anti-submarine warfare. All of these, you can certainly apply the same lens to military capabilities. And as Sean highlighted, they're also supported by information, technology, facilities and people who are using technology to support those missions, right?

So I think that kind of the core organizing principles behind the CRR, behind the ES-C2M2, ultimately behind RMM, are really, can really be potentially useful for helping leaders in DoD to tie mission capability more directly to the cyber assets that support those mission capabilities.

Specifically on the supply chain or external dependency space, there are quite a few examples. So I'll just pick one. DoD Transcom, for example. So Transcom is the U.S. DoD transportation command, which is responsible for moving military assets around the continental United States. About year and--about a year

or so ago, there was a culminating series of investigations that indicated that 22 of Transcom's 25 primary contractors had basically had cyber intrusions and information stolen at the hands of an overseas power, essentially. Transcom itself was only aware of three of those breaches, right.

So here you had a core military capability, which is moving men and-- personnel and materials around the country, which essentially the attack surface is a lot broader than you might think at first, right.

Presenter: Sorry, John. And it includes civilian organizations that underpin that transportation mission.

John Haller: That's right.

Presenter: So it's that join of private industry and the DoD that we're referring to.

John Haller: That's right. Exactly. So the attack surface that you're worried about, and this is in some of the COI material talking about attack surface, is a lot broader than just Transcom systems. It extends, as Matt's highlighting, to all of the private contractors that support Transcom. And of course it matters whether their confidential information supporting DoD is secure or not. So something like the EDM assessment and this approach can be used to help organizations like Transcom be, manage, those risks better. It's kind of not an offensive cyber capability. It's part of the defensive capability to

help mission owners understand their cyber vulnerabilities and better manage the problem.

You see a similar thing--I know we're a little tight on time--you see a similar thing in the concern about unclassified controlled technical information and some of the changes to the clause. Those are, that's a very understandable, sensible way to approach it. But you know, to understand if the contracting community or the defense industrial base can actually meet those requirements, in the future we're going to have to dig a little deeper to see if they actually have the processes in place to do it, right? And I think some of these tools can help.

Presenter: Okay. Thanks, John. We could use another 40 minutes. There's so much to talk about here.

John Haller: That's right.

Presenter: Maybe in the next webinar we'll do that, but...

John Haller: Yeah.

Presenter: But I'll turn to Shane. Are there questions from the audience?

Announcer: We did get one. A quick one from Jody asking--I think this is in regard to the CRR. How does this tool compare to the CSET tool?

Presenter: Sure. So I think that's the perfect question to position for Sean to answer. So Sean, the question was--

Sean McCloskey: Sure.

Presenter: --how the CSET and the CRR work together. And maybe if you could highlight how they, they sort of complement each other.

Sean McCloskey: Sure. The CSET, the cybersecurity evaluation tool, was developed by our industrial control system CERT at DHS. It's the same cybersecurity and communications group that I'm part of, but the ICS CERT is actually part of a national--the NCCIC, the Communications and Integration Center, National Communications and Integration Center, at, within, CSSC. So the CSET tool was originally designed primarily for industrial control systems. It's in its fourth, almost fifth iteration now. And the unique thing about that is that you can be actually, you can select a different set of standards to apply to whatever service that you're evaluating.

So the CSET is a little bit more standards based as far as strictly checklist based. You can run a NIST 800-53 assessment against it, or whatever particular set of compliance standards that you want to evaluate. The CRR is more process-oriented. It kind of focuses--I call it more of a holistic type of assessment. It looks at different parts of the organization, tries to identify those specific

practices that are cross-cutting throughout the organization. Then the main difference is the maturity aspect. We're trying to identify and look for indicators of maturity within the processes that we're evaluating. Think that's the primary difference.

Presenter: Great. Thanks, Sean. So--

Sean McCloskey: The CSET is also available free for download as well. Sorry.

Presenter: Sure. So we sort of, we quickly need to wrap up, but I wanted to just highlight anything that we are developing or introducing, any of these free programs, it's new initiating for the audience, so I'll maybe kick off. So Katie mentioned that the C2M2 tool gives you an understanding and gives you guidance relative to the NIST cybersecurity framework. I wanted to highlight that we have the same correlation capability and the same crosswalk concept in the cyber and the CRR.

So let's, quickly John, in two minutes, new and interesting things coming down the pike in the EDM assessments space.

John Haller: Well, in the EDM space, there's generally an issue or an interest area in interdependencies between critical infrastructure, right. So one of the areas of research that we've been looking at is basically dealing with the cyber insurance

industry and the reinsurance industry, right. So if you think about reinsurance, essentially it's a way for insurance companies to spread risks, right. With the growth of cyber insurance, there is an interesting question about, "Well, how do cyber insurance companies look at the concentration of risk across an entire set of customer organizations and how would they go about actually trading that risk and being aware of dependencies and interdependencies?" Just like if you would insure a giant, or one large geographical region, you want to spread that risk. Well, what are the cyber corollaries? I actually think that's also relevant to the DoD when you think about systems and capabilities across an enterprise as large as the DoD.

Presenter: Sure.

John Haller: So it's applicable

Presenter: Sorry, John, .

John Haller: Yeah.

Presenter: So I think it's important to--you're highlighting a vein of research or an area of research that we're doing sort of in addition to these very accessible and practical tools that CERT helps to develop and deliver for the DOE and DHS.

So with just a few moments left I wanted to then ask Katie if there's any new capabilities are new tools or techniques that you are introducing in the C2M2 space.

Katie Stewart: So building off of the insurance work that's being done, we're actually looking at taking that model and developing a risk score that kind of rolls up all of the C2M2 data into a FICO score, like, index so that utilities can use that to communicate and compare themselves to their peers. So there's that effort going on, and that's based a lot off of the modeling that's being done for the insurance agency, because it a lot of the same concepts. We also are in the process of possibly making an overhaul to the model. We don't collect data, however, the utilities do and they compare. And we are in the process of going through some lessons learned there to see if we can get some efficiencies in the model, either combining domains or making this as good of a tool as we can, and as usable as we can. So there's iteration going on there as well, and those are, that's also being done outside of Department of Energy from some of our lessons learned and researched against RMM, the resilience management model.

Presenter: Great. Thanks, Katie. And I know, Sean, that DHS is always striving to refine its methods and models. There's a number of things in the CRR space, including data analysis, that we probably don't have too much time to talk about. But would you like to maybe close out with thoughts about new capabilities or new offerings that DHS is bringing forward soon?

Sean McCloskey: Sure. Just a couple things. We are releasing, and it's in testing right now, a new version of the CRR Self-Assessment package, Matt, as you well know. We're testing that now. Hope to have a release soon on that, but the unique thing about that is it's going to have overlays that compare your CRR results to the NIST cybersecurity framework. So there will be unique views that allow an organization to compare itself against the framework, as well as we saw on the slide earlier, some of the mil zero to one comparisons to allow an organization to get a little bit more detail at the practice level of how they perform. So those are two things. And then in addition, close, last comment, DHS is, you know, we are always in the process now of, at least with my branch, working with fielding new cybersecurity advisers which are folks that are aligned to FEMA regions that help conduct these assessments and help critical infrastructure facilities assess cyber resilience and gain access to CSSC DHS capabilities.

Presenter: Thanks, Sean.

Announcer: Thanks, Sean.

Presenter: Unfortunately, we're out of time. I'd like to thank all of the panelists for joining us, and certainly is a wealth of tools and informations available to those that are interested in cyber resilience or those that may be responsible for securing infrastructure. So I think, Shane,

next time we're going to ask for an hour.

Announcer: There you go.

Presenter: So...

Announcer: You guys deserve it. Great presentation, guys. Thank you very much for your time. So we're going to take a 10 minute break. We'll be back with Rotem Guttman, speaking on Generalized Automated Cyber-Readiness Evaluator or ACE. So we'll be back promptly at 2:20 with Rotem. Thank you.

Carnegie Mellon University

Copyright 2015 Carnegie Mellon University

DM-0002555