Carnegie Mellon University
Software Engineering Institute

Shane McGraw: Hello. Welcome to today's SEI webcast, "Risk Management for the Enterprise: How Do You Get Executives to Care About Risks?" My name is Shane McGraw, Outreach Team Lead here at the SEI, and I'd like to thank you for attending. We want to make our discussion today as interactive as possible, so we will address questions throughout today's talk, and you can submit those questions in the YouTube Chat area. We will get to as many as we can.

Our features speakers today are Brett Tucker and Matthew Butkovic. Brett is a Technical Manager of Cyber Risk Management at the SEI. He's responsible for research and development portfolio, focused on improving the security resilience of the security and resilience of the nation's critical infrastructures and assets. Prior to joining the SEI, Brett was a Global Risk Manager for Westinghouse Electric Company, where he managed the enterprise risk portfolio and global insurance programs. Brett also served at the CIA as a veteran of the United States Navy.

Brett, welcome. Thanks for joining us, and a quick question for you. Given the situation that we're all being remote at home now, what is your best work-from-home hack?

Brett Tucker: Ah, thanks, Shane. It's a pleasure to be here, and actually, my hack is so non-technical. My-- <audio cuts> home hack is I love actually being able to change my scenery on any given day. So I'm in my office, or I can go down to my basement where it's nice and cool in a rec room, and I really like going out on my back porch where get to, you know, get some fresh air and get the stink blown off. It's good.

Shane McGraw: Much needed for everybody. Thank you for that.

Brett Tucker: Yeah.

Shane McGraw: Yeah. Matthew Butkovic is the Technical Director of the Risk and Resilience Team here at the SEI. Matt performs critical infrastructure protection, research, develops methods, tools and techniques for evaluating capabilities and managing risk. He has more than 15 years of managerial and technical experience and information technology across the banking and manufacturing sectors.

Now I'm going to turn it over to Matt Butkovic. Matt, welcome. All yours.

Matt Butkovic: Thanks, Shane. Great to be here. So Brett, I like your tip for sort of changing up the scenery during these very unusual times. So changing scenery is at the heart of the discussion today, which is risk is kind of constant, ever-evolving. So I was hoping maybe as an intro to our discussion today we could spend a little time talking about risk uncertainty, and maybe, Brett, if you could explain both the down side and up side of risk?

Brett Tucker: Yeah, absolutely, and that's a great place to start. I mean, let's just level some of the idea that risk truly is what you said, it's uncertain. It's not knowing an event or a incident that may occur, and yes, risk has a two sides to it kind of a thing, like a coin almost, you know. One side of the coin it could be a threat. In other words, the impact of an incident occurring or a risk coming to fruition could be negative. It could threaten the ability for an organization to achieve their objectives. On the opposite side though it could also be viewed as an opportunity. So you could have something happen that's positive. So a good example here, and actually a real practical one, is the fact that people like to gamble, right. Some have a high-risk appetite and want to seek that opportunity side. So, you know, they sit down like a chip on Black 22 or whatever it is they play and they view that very much as an opportunistic risk that they're taking, versus folks, you know, like, more like me, a little more conservative, I'm like, "Why would you want to spend your money on that?" That's like a real, like, loss. I'm going to lose my money on that. That's a negative impact that I'm not seeking. So it's a threat to my business objectives, you know, if I'm trying to save money or whatnot. So risk can be two-sided, as you said, and it certainly is uncertain.

Matt Butkovic: Thanks, Brett. So I think it's important to remind ourselves that, especially as someone who's a cyber security practitioner, we tend to think about the down side of risk or the unwanted consequences of risk, but we have to remember there's also opportunity in risk, and I think to reference kind of the extraordinary times we're in, we're seeing that in things like shifting to new modes of operation or even personal calculations that we take every day.

Brett Tucker: Absolutely.

Matt Butkovic: So we've been--

Brett Tucker: Yeah.

Matt Butkovic: We've been working in this risk space for a long time at the SEI, so Brett, I think one of the takeaways that our viewers should have for today is that we're on the verge of releasing a new version of our primary risk management, framework, which is OCTAVE, but to really understand where OCTAVE is today, we have to retrospectively look at where OCTAVE came from and sort of the design philosophy behind OCTAVE. So would you mind just taking us through a brief history of OCTAVE?

Brett Tucker: Sure, sure. So about 20 years or so ago, we had a group of folks at CERT who published a textbook, and actually, I have a copy of it, always available on my desk. You can find it on Amazon. It's "Managing Information Security Risks," and it is basically OCTAVE, and it's about a, you know, a 300-or-so-page take on OCTAVE. By the way, OCTAVE, just as an aside, is an acronym. It stands for Operationally Critical Threat and Asset Vulnerability Evaluation. So the whole idea was to evaluate assets in their organization and understand the threats and vulnerabilities related to it.

Now, some challenges came up early on with OCTAVE. It had a broad customer set. It was adopted, you know, in fits and starts, and a lot of the customers were coming back and saying, "You know what? It's a little heavy. It's--" yeah. I mean, it's a textbook, for goodness sakes. Like, "Is there a way we can kind of lighten the process up?" So what you saw over time within the first, ah, 5 to 10 years of its life, were iterations where they were trying to lean it down. There was OCTAVE-S and a couple of these other versions that came out that were industry-specific, maybe sector-specific. But where it really, really got good was about 10 years ago they hit upon this new model called OCTAVE Allegro, and I have the process here up on the screen if anyone's interested in looking.

You can see it's a eight-step process. It is lighter weight than the original OCTAVE process, and it focused moreso on the information risk side. So if I have as an asset-- remember, by the way, assets can be people, information, technology or facilities. In this case, Allegro was focusing on the information assets. It really was helping people analytically, especially at the front lines, boil down their risk and understand how they could respond to it and prioritize it as well, and now, about 10 years later, after Allegro, by the way, has a very broad community that uses it as a large base out there, we recognized that there needed to be a stronger connection between the front lines, the people who were actually analyzing these risks and identifying them, and connect them more to the board level, the executive level of any organization. Because what was happening was there's a disconnect between the bits and bytes analysis that was taking place with Allegro and the dollars and cents argument or business case that needed to be made to get that proper risk response that you alluded to, Matt, because the benefit of having a robust risk management practice or organization within your company or your organization, is the idea that you're building resilience in your organization, and I think that's a key word to walk away with here. The risk practices that we're picking up with both Allegro and Forte are leading you down a path of having a more resilient enterprise, and that is the value return you were alluding to.

Matt Butkovic: Thanks, Brett. So just to be clear, OCTAVE Allegro was focused primarily on the information asset?

Brett Tucker: Yes, sir.

Matt Butkovic: The enhancement to OCTAVE that was described today, and not to sort of steal your future thunder here, it's designed to sort of broaden that perspective, correct, to draw on the other asset types or rather address the risk to those other asset types?

Brett Tucker: Yes, exactly.

Matt Butkovic: I think that's a key distinction we need to make is that this is a reimagining of OCTAVE to be applied more broadly, and I would describe it as being better integrated with other frameworks and methods.

So I know we're going to step through each of those pieces, Brett, and--but I wanted to ask you a more fundamental question. Let's say I'm an OCTAVE user now. As you said, OCTAVE has been very successful. It's used by many organizations. Just to be clear, what we're saying is this is, the new method that we describe today, can be applied. You don't have to abandon OCTAVE Forte to use the new method, but rather you can augment and extend and make better your risk management, correct?

Brett Tucker: That's absolutely correct. So if you are not a Allegro user and you hear about Forte coming down the path, never fear. It is an augmenting or an enhancement to the OCTAVE product set that we speak of broadly, and to make that connection I was talking about between the front-line user who's doing the analysis in that executive board room, there's a lot of discussion in Forte with respect to enterprise risk management, and the application of fundamental enterprise risk management principles as an overlay to help amplify and bring to the top those cyber risks that are most improve in organization, and what you get when you apply enterprise risk is you get this nice apples to apples comparison now taking place with cyber risks, with all other risks in enterprise that are being considered, outside of the CISO's organization.

You know, there's human capital related risks. There's strategic risks. There's financial and contractual and all these other types and flavors, and you have these executive decision-makers, and by the way, I'm going to emphasize that. It's risk management for decision-makers. They want to make these informed decisions based upon the risk portfolio that they have. Cyber plays a big part of that, just as much as all those other elements. So how is it that we can get them to compare this Forte process? We'll walk you down the path to build a program where you can start ingesting all those risks and prioritize them in the same light, so that way you can make those critical decisions on where to invest your resources.

Matt Butkovic: Thanks, Brett, I--so you and I are both affiliated with the Chief Risk Officer Certificate Program at the Heinz College, right, the Executive Education program, and I think--

Brett Tucker: Yeah.

Matt Butkovic: --one of the things that we hear is that that, looking beyond the information security risk, for folks that are steeped in information security risk, is a challenge, right. So if you come from the risk management side of the house, I think you more readily understand the combination of risk. But if you're a cyber security practitioner, it's sometimes difficult to couch position or quantify your risk in the same form, right. So what I'm pointing to here is that I believe that you've taken input from those sorts of audiences, the CRO Certificate students and our partners in federal agencies, and private industry. I think it's also important to note, and correct me if I'm wrong, Brett, although we say executives, it's really decision-makers. So we're not saying that if you're not a Fortune 50 or a Fortune 500 company you can't use OCTAVE, right. I mean, quite the contrary, right?

Brett Tucker: Yeah, that's correct.

Matt Butkovic: Think it's kind of set for purpose. Would you mind describing how organizations of all size might benefit from using OCTAVE?

Brett Tucker: Absolutely, and yeah, and actually, that's a great correction on your part, and so I use executive as a loose term, but what I really mean is like what you said. Those in the enterprise who are making critical decisions about investment of resources to alleviate that risk or to mitigate it or to either avoid it happening or being prepared for that cold, dark day when it does happen, and I think regardless of the organization's scale, there are elements within Forte that are fundamental to any organization, whether it's public or private sector.

It's been quite a journey, Matt. It's been almost three years now that we've been pulling this together and developing it, and actually, thank you. You've been on that path with me for a good bit of it, and we're just about to publish the technical note that's going to give you a lot of the details we're going to go through on this.

But one of the things I really want to float to the top is that regardless of the size of your organization or what you're trying to achieve, it's all about thinking about your business objectives and how you're going to rack and stack or prioritize risks related to those objectives, whether they're cyber or not, and the good news is, like I said, you're going to start seeing a lot of interdependencies with these risks, and hopefully there's going to be a savings, if you will, down the road, if you have a risk, let's say, that addresses talent restriction as a--just as a general example.

You know, we have and value our talent within the cyber security sector, because it's so hard to come by. So there are other elements of any organization, public or private, that's concerned equally about having good talent. So you'll identify an interdependency like that and thankfully you have OCTAVE Forte that will walk you through the process of how to better leverage that interdependency and mitigate that risk so that there's like a universal win in the organization.

Matt Butkovic: Yeah, thanks Brett, and it's useful to understand the context. So there's a question here from the audience and the heart of the question really is how does risk management feel and look in an era dominated by things like Agile? So let me, if it's okay, Brett, I'd like to give you my sort of 30-second synopsis, and then as a risk expert you tell me if I'm wrong.

Brett Tucker: Sure.

Matt Butkovic: So techniques for software development, infrastructure deployment, the technology stack itself will continue to change, right? So risk is a constant, right. Meeting a strategy that aligns your capabilities with your objectives is a constant. So if we were doing this 20 years from now and we're talking about quantum computing and chemical computing and a type of virtualized infrastructure we can't even anticipate now, right, in the--and somehow there's some augmented reality or A.I. being used for this, for this webcast, it seems to me that risk management will still be a central concern. It doesn't matter if you're a small organization, a large organization, a state government or a national government, right. That risk management is arguably the most enduring feature of governance and leadership.

So I know that's a lot to unpack. I didn't mean to sort of soapbox it, but thoughts about that?

Brett Tucker: Yeah, no. I couldn't agree more, and to be honest with you, I have a recent example of this where I wrote a white paper related to risks of having artificial intelligence, and as a consumer how I go about thinking about risks related to. But as I was going down that journey of writing that document I thought, "You know, this is really generally accepted practice in terms of risk identification and management across any new technology as it comes in the door."

So you're a hundred percent right. They're the fundamental underpinnings of understanding uncertainty and addressing or identifying those uncertainties and finding ways to avoid, mitigate, transfer or, you know, address those risks in a standardized manner, such that you have a more wise or a more beneficial way of investing resources, as that is yet another limiting factor that'll always be there regardless of all these technologies too. Limited resources. So you're trying to make risk-based decisions on how best to invest those resources. I couldn't agree more with you, Matt.

Matt Butkovic: Yeah, and it seems to me, Brett, that as technology changes, right, we tend to think of it as, and rightfully so, that it's providing some marked change in capability, right. The reason you're using a new technology is does something in a way that's better, faster, cheaper, right?

Brett Tucker: Yes.

Matt Butkovic: We must remember that the introduction of new technologies and new process, such as Agile, for instance, right, or any process, that's also a source of risk potentially. So it's not just understanding how your existing risk management applies to new technology. It's also, in my estimation, it's identifying the sources of risk that are a result of the introduction of new technology and process.

Brett Tucker: Yes, absolutely, and you know, implementing Agile can be a challenge, just as much as implementing any new process in enterprise. So that change management could impact your objectives, because once again, it all goes back to those strategic objectives that you've trying to achieve and understand what uncertainties you're introducing, and by the way, I want to be quick to remind us, the audience, that it's not just about identifying the threats related to implementing Agile, for example, but the opportunities and well, and how can we enhance them and make those uncertainties stand more to the front and be more bold and have more amplification of the benefits?

Matt Butkovic: Thanks, Brett. Oh, Brett, we have a graphic up now that shows a wheel.

Brett Tucker: Yes.

Matt Butkovic: And has a set of sequence steps, and I know that what I'm looking at is OCTAVE Forte. So I want to make sure we give ample time for the introduction of OCTAVE Forte and then audience questions, so at this point, Brett, may I ask you just to describe the high-level OCTAVE Forte, and I know we're going to take the journey around the wheel, and I'm sure I'll have some questions for you, as will the audience as we traverse the wheel.

Brett Tucker: Yeah, and, you know, I'm going to do this in abbreviated manner. So the tech note that's coming out obviously is going to provide a far more extensive look at each of these steps and before I even start here I also want to advertise that within that document there's going to be a companion document that is going to provide a toolset. Almost think of it as like a buffet of tools that are available, because once again, there's this notion of scalability. What's good for some organization may not be good necessarily for others. So trying to provide a good mix of tools that can be used within each of these steps that's going to be coming out.

Now, I will go back and show you real quick again that Allegro picture, because I want that to kind of be in your mind. There's some things here that I want you to note about the new

OCTAVE Forte process where you do have a little bit of an enhancement from the old process. For example, with Allegro, and by the way, Allegro is a solid process. I'm not trying to make it lesser or anything like that, but notice that you start with Step 1 and you go to Step 8, and it feels like even graphically looking at it, or pictorially looking at it, that the process ends at Step 8.

Well, one thing that is enduring about risk management and as a theme here in this discussion that we've already had, is that risk management is enduring. It is cyclic. It's always happening in a life cycle. So regardless of where you're at in your organization, in maturity or what you're trying to accomplish, anywhere you pick up in this process you're going to go through these steps in an iterative sense and the hopes being that you're going to overall improve the maturity of your organization in terms of risk management.

So let's look at these 10 steps real quick. I'll walk you through it, and actually for nascent organizations and for organizations that may have maybe, like, fledgling or are just starting out with a risk management program, in a sense, they're trying to think of, like, what are the fundamental principles or what are the fundamental things or pillars that I need for my organization to get a risk program kicked off? And Step 1 is really all about getting you on that path, and I like to talk about the three classic pillars that are necessary for a good enterprise risk management program. One is good governance.

So there's a lot of talk about how to set up a governance structure within any organization, once again, in a scalable sense. So that way people can understand the flow or communication of risks up and down an organization. Because remember, once again, it's all about getting resources to the right risks in a prioritized manner. After governance, you have to think about how those risks are being communicated, so there's almost sort of this discussion of appetite. So that's the amount of risk that an organization is willing to take on and hold and still achieve its objectives. So there's discussion there about how to properly build an appetite statement, how to make it quantifiable, if at all possible, and how to properly apply it in your organization, and then the third pillar that it talks about is policy, which, let's face it, that can be a tricky world. For anyone out there who's written a policy before, it is hard, it is really hard to communicate to an organization specifically and exactly what you mean and get the same result, a standardized result.

The good news here, aside from providing tips for writing a good policy, which I've been party to many times before, is I've actually crafted a draft policy statement for a synthetic organization, and it's in an appendix, so I welcome anybody who reads the document to pick that policy statement up and tailor it to your organization. Scale it as necessary. Take pieces out that you like and use them. Take pieces out that you don't like and don't use them. So there's that kind of practical tool in the document overall that's going to help, and that's just to round out Step 1.

So once you have this program built, you start to think about, “Okay. What are my objectives, and strategically speaking, what am I trying to accomplish as an organization? What are the critical assets that I have in-house that I’m using to accomplish those objectives?

Now, remember, I already said that an asset could be people, information, technology, or facilities, and there’s also a discussion in there that talks about third-party providers. Because we’re all about supply chain risk now too, which is another buzz word that has been coming up quite a bit lately, right. How do we think about providers giving us the critical services that we need to deliver on our objectives as well?

So that’s another point I want to point here, that OCTAVE is not just looking inside the organization anymore, it’s also looking outside the organization as you go down this path of analysis. Anyway, as I’m going through Steps 2, 3 and 4, I’m identifying those assets and documenting them. I’m also thinking about what is it that are the bare minimum requirements necessary to keep those assets in play such that I can be a resilient organization. So that if any one of them are lost at any given point in a value stream, that I can still bounce back and keep providing critical services with as little or seamless of interference for delivering on those objectives, and I also want to think about, “Hey, I don’t want to spend additional monies that I’ve already spent on mitigations.” So I already have in my security stack firewalls and IDS, IPS, things like that. So you’re going to want to go down that path of thinking about, “Hey, clearly I don’t want to buy yet another of the same tool,” right? So we’re going to-- <audio cuts> our current capabilities right around Step 4 there to understand where we’re at in terms of what good assets we already have in hand.

Next you’re going to want to think about, “Okay. So I have these assets. I’m accomplishing objectives with them by delivering critical services. What are the threats outside the walls of my organization as well as inside the walls of my organization that are classically trying to detract from those objectives?” This could be something as benign as maybe a mistake within programming, for example. If I’m doing coding or something like that. It could be something as pernicious though as an insider threat in your organization as well. So there’s this whole gamut of threats that you need to think about, and you also want to think about the chinks in the armor that you may have too, that those threats are going to take advantage of. So that’s what we’re talking about when we’re talking about vulnerabilities in those assets as well.

Okay. So through Steps 1 through 4 now, you have a program, you have the bones or the fundamental elements of program, and you’ve effectively identified risks within your organization, and now, from Step 6 forward, you’re really focusing on, “How am I going to respond to those risks?” Now, remember, classically in terms of response, I can mitigate risks or I can take action, to make sure those risks either don’t happen, or I’ll be prepared for that cold, dark day when they do happen. I can avoid them by just not going there, right. I can transfer them away. Classically you could, you know, you can buy insurance, for example, as a classic transfer in strategy, or you could also accept a risk.

You could say, “Hey, I have a threat in my organization. It’s clear. I have vulnerabilities that are either too expensive to address or I just don’t have the technology to get there,” and that’s fine. But the idea here is that regardless of the path you pick, even if it is acceptance, that you’re making a decision with a mindful choice, it’s risk informed. You’re practically going to want to document that somehow. You want to convey that to your governance structures so they understand that that risk is being accepted in your organization, or it’s being addressed through investment of resources for mitigation, for example.

And that’s what we’re getting at in Steps 7 and 8, right. You’re coming up with, “What is that response strategy?” and then from that response strategy, more specifically, “What are the steps I’m taking? What are the plans that I’m developing?” and this really gets back to blocking and tackling. Once again, just as much as risk management is enduring in an organization despite the technology, project management is yet another discipline that classically I think is largely ignored by risk professionals in some cases when it comes to implementing some of these response plans.

You know, you see they have great ideas and you even see in cyber organizations, and for those in the audience, those out there who are going to shake their heads and say, “Yeah, we have a lot of shelfware. We bought a lot of nice tools. We knew we needed them, but we never quite implemented them for whatever reason.” Well, you have to projectize it. You have to think about the scope, the schedule of the budget, and you have to be responsible and have it reported back to your governance structure to demonstrate that the investment is being implemented. So that’s where we’re getting at in like Steps 7 and 8, that kind of a thing. But then you want to start thinking about, “Okay. So was I effective at it?”

Now, there’s a lot of ways of thinking about measurement here, and I’m just going to give you a taste of some of those means of measurement and how I know I’m being effective or not. Let’s go back and think about implementing response plans, for example, with the project management piece. There are classic tools in the project management toolset such as cost performance index and schedule performance index that I can relate back to my governance structure how those mitigation plans are being implemented, how those response plans, excuse me, are being implemented.

You can also think about it in terms of, “Okay. So if implemented said tool--” or process or whatever it is that shows, whatever technical, physical or administrative control I’ve put in place, and I want to think about now measuring the effectiveness of that control in terms of dialing that risk down, right. Now, that can be quite tailored and I know that folks in the audience too, experience in cyberspace, can really identify with this, how you measure the number of phishing emails that are sent in organization that were actually opened versus ones that weren't right, for every one sent, and classically dial it back to how effective an awareness campaign was as mitigation? That would be a classic example of how you're going to measure effectiveness of a certain mitigation response plan that was put in place.

You also want to think about one more means of measurement. You want to think about how effective your risk program is overall. How is it working in the organization? And that's where we're start going to dovetailing into Step 10. We're going to start talking about, "Okay. So I know my governance structure has regular committee meetings," whether they're risk committees or whether they're functional committees that are meeting about specific risks, are they meeting quorum, are they actually demonstrating that they have governance over risks that are coming to them? Are decisions being made, and if so, how effective are those decisions that are being made?

It could be something as easy as that to understand the maturity of risk management in your organization, and then classically you get to the top of the wheel and you're starting again. You're going to use that information that you have now gleaned about your program and about how effective you've managed your risks and you're going to tweak your model.

So you're going to go back to Step 1 and you're going to think about your policy, your appetite, your governance structure. What tweaks can I make to improve that process overall, such that the analysis is more effective, such that my response plans are more effective?" And it's, like I said, an iterative process. It's a lifecycle.

Matt Butkovic: Thanks, Brett. That was an excellent overview, and, I mean, there's a great deal to unpack in every step. A few questions have come in from the audience, but before we get to those, I--maybe this is stating the obvious, but I just want to be clear for folks watching this, that we're not suggesting you have to start at Step 1 if you have the substantive pieces parts. Start at the step where you have evolved to, right. So fair to say, Brett, that you don't have to always start at Step 1. The model will meet you where you are.

Brett Tucker: That's absolutely right. Yeah, you can--as a matter of fact, I tried to write it as best as possible that you could open the document up and go to any particular step and feel comfortable reading from the middle forward and then looping back. There's some context that is built into the document, obviously, to have that discussion for people who maybe are not as familiar with risk, but what I did is I took out the fundamental concepts of risk and actually pushed them down into an appendix so that way you read about the steps and if you missed a spot or maybe you have a disconnect on fundamental understanding, you can go back to the appendix. But the idea is, I'm trying to facilitate picking up at any point in that process and making it work for you.

Matt Butkovic: Great. Thanks, Brett. So a question about the qualitative versus quantitative means that we have in OCTAVE Forte.

Brett Tucker: Mm-hm. Yes.

Matt Butkovic: So could you please just explain the quantitative pieces that we may find here? Specifically someone in the audience interested in Loss Exceedance curves and Monte Carlo simulations.

Brett Tucker: Yeah. So I do mention those, but I don't go to that extensive a depth into a Monte Carlo discussion. You know, it's obvious a tool that's available. Modeling and simulation is very important in the risk management world. I want OCTAVE Forte though to be recast in your minds, if you're asking that question, as more of an overarching process, the bones of a program and the bones of things that you need to be doing, and Monte Carlo would be a tool like the meat that you're going to hang from the bone.

Now, that said, I have accounted for that in additional appendices as well, where I've talked about different tools and different processes that may be available to you. So you mentioned quantification, Matt. So one of my appendices would refer readers to FAIR.

For those who are not familiar with Jack Jones and Freund, they produced a document FAIR, Factor Analysis for Information Risk, and it's very good about walking an organization through getting more quantitative with their risks. That could very easily fit within this Forte umbrella, especially around steps, you know, 4, 5 and 6 kind of an idea. So there are processes that are sub to this overarching process that exists here, but I actually do have more specific tools, Matt, as well, where I'm trying to help people be more quantitative with their risk management, and a good example is with the risk appetite statements.

You know, you may recall as kids we had like mad libs, remember? They were like documents where you'd fill in funny words in the blanks and you'd build a story out of it. Well, imagine me giving you a framework for a risk appetite statement. Now instead of filling in funny words, you're going to fill in quantitative terms that are more meaningful to you as an organization, because you have your context, but you also want to appoint numbers to it, and I talk a lot about going out and speaking with the leaders of an organization to understand what their degree and level of comfort is with respect to investing resources for risk, and that translates back to appetite.

So now you have a functional risk appetite statement where people could actually read it, see where they fit in terms of the tolerances within the appetite, and know what to do about it. Where do I go in the governance structure? Who has authority to answer these questions and provide me resources I need? And of course, I've also provided for the qualitative bounds there, because not all risks are absolute in terms of quantification. As a matter of fact, I would argue that there are hardly any out there that are really, truly you're able to pin down to any specific quantitative impact. So you want to have some degrees of qualitative measurement in there to bound or provide range on what a risk impact may be. That will flesh itself out in the appetite discussion just as much as it's also going to flesh itself out in that risk analysis discussion.

Matt Butkovic: Thanks, Brett. So it's fair to say then that, and certainly OCTAVE Forte doesn't prohibit or any way, limit the use of any of those tools. In fact--

Brett Tucker: Not at all.

Matt Butkovic: --I'd suggest you could feed the use of those tools, right?

Brett Tucker: Yes. Absolutely.

Matt Butkovic: So we should look at things working in unison. I think you said something very insightful early on in our conversation this afternoon, which is all of this should be fit for purpose. So take the pieces that work for you, use them in the combinations that make sense.

Brett Tucker: Yeah.

Matt Butkovic: We don't look to OCTAVE or our other frameworks and methodologies or models, right, as the absolute only way to do something. In fact, I think that when you cross-pollinate and draw connections between these, these frameworks and models and ways of working, that's when sort of the best results are delivered, right?

Brett Tucker: That's right.

Matt Butkovic: With that said, Brett, there's a question about OCTAVE Forte and its correlation with other standards. You've mentioned FAIR and how FAIR work in conjunction. Could you please just spend a minute talking about the join between two things? First, OCTAVE Forte and the ISO series of standards, so I know you're very familiar with.

Brett Tucker: Yes, sir.

Matt Butkovic: And also the join between OCTAVE Forte and the Risk Management Framework from NIST?

Brett Tucker: Yeah, sure. So there's a discussion there too in the tech note that talks about these, and Forte is a construction of many great things. ISO being one of them. For those in the audience who are maybe not as familiar with ISO and the 31000 Series and the 27000 Series, you know, I did not write this paper blindly as I acknowledge that those standards are out there. They're very good. You're going to feel and see sprinklings of the elements of it throughout this discussion of Forte, because, let's face it, like, at the end of the day they're thinking a lot of the same things that I was trying to put in here as well. You know, there's discussion of governance, there's discussion of appetite and its application, that kind of a thing. So it definitely gives a nod to ISO as a standard. What I tried to do was to give you more practical tools and pointers as to how to implement where ISO maybe is a little bit more formal in its delivery in terms of what a standard is for having a risk program.

The Risk Management Framework, and by the way, it's more than just the Risk Management Framework that I lean on in terms of NIST. You know, there's the Cybersecurity Framework. There's a lot of great things that are provided by NIST, and I, once again, I leaned on a lot of those items. But specifically you mentioned the RMF. So let's talk about that for a minute.

You know, the RMF is very good at ingesting assets in organization and understanding and identifying risks related to those assets as they go through their lifecycle and even as you're looking to sunset them and get them out of your organization. Once again, that's a process that would be sub to this overall Forte process, where I have an organizational understanding as to what's going on in terms of risk management, and Steps 2 through, let's say 6 or 7, where I'm bringing assets in, I'm understanding what those assets are, I need to understand what risks are related to those assets and how to insulate against those risks or enhance them if they're opportunistic. That's where the RMF would play in. So you're going to get flavorings of that as well.

I also speak a lot to governance, which that has a good nod in RMF space as well, so you're going to see a lot of interweaving of those standards, because let's face it, there are lots of great things out there. But what I'm really trying to do is to give a handbook to someone who maybe doesn't really know how these things knit together well. So this is my perspective on how you can get those things to knit and work well for you in concert in an organization and not just lean on any one given standard.

Matt Butkovic: Thanks, Brett. So really, it's about convergence, right.

Brett Tucker: Yes.

Matt Butkovic: It's not finding a single universal elixir, right, that allows you to solve all of these problems, right. It's going to be a combination of tools and techniques.

Brett Tucker: That's right. Yeah, that's a great word, convergence. Yeah, it's an integration of those, of the best of what those all offer.

Matt Butkovic: And just let's talk a little bit about integration. You mentioned the NIST Cybersecurity Framework, which is focused, of course, on cyber risk primarily. I know the CERT Resilience Management Model, the CERT-MM, is something that fully correlates and I would argue is designed to mesh with OCTAVE Forte. So one of the things I'd like folks to sort of see in today's presentation is that if you're using any of these products or techniques, it can serve as an on-ramp to the others, right. There's very specific compatibility design into what you've developed.

Brett Tucker: Yes. As a matter of fact, I talk about, and actually I'm going to key off one of the things that you really said there, was the Resilience Management Model. You know, I'm solidly convinced as I've gone down this path, and it's been a journey to pull this together, that there's this risk chicken wandering around and he's laying--

Matt Butkovic: A risk chicken?

Brett Tucker: Yeah, the risk chicken, yes.

Matt Butkovic: The risk chicken. Okay. Yeah?

Brett Tucker: Yes, and this risk chicken is laying the resilience eggs, the goodness, the products that come out of having a good, robust risk management program, is that your organization is going to be more adept at answering the call of being resilient and maintaining your operational capabilities despite those risks coming to fruition at any given point in time. So yes, there is a big nod to RMM fundamentally speaking, not only as you're going to get that flavor as I do training in the CRO program, but you're also going to feel that in the tech note as well.

Matt Butkovic: Well, so two things, Brett. One is the term risk chicken makes me think you've been quarantined in the countryside too long.

Brett Tucker: Yes. I have. Yep, you got me, man.

Matt Butkovic: The second is when I think hard about risk management techniques like OCTAVE Forte or resilience management techniques like the CERT Resilience Management

Model, at the end of the day, we're trying to achieve predictability or at least we're trying to forecast the performance of an organization in response to some input, right.

Brett Tucker: Sure.

Matt Butkovic: I think this sometimes gets lost in the conversation, right, which is--and I know you've heard me say this to audiences before, Brett, you know, that the CISO, cyber security practitioner or audience, hates when you say, although it's true, that cyber security is subordinate to risk management. Right. We do these things to manage risk to a tolerable level in an organization, right.

Brett Tucker: Yeah.

Matt Butkovic: And I think that no matter which kind of stream or column you're in in risk management, if you're in charge of the people or the physical assets, you may tend to think that you're the center of that equation, right, but the truth is it's the interplay between those assets and understanding how they'll react given a specific scenario that we really have to think about.

Brett Tucker: Yeah, I couldn't have said it any better, and, you know, classically as we go through all our different customer sets, you know, whether they're public or private sector, there's always this talk about, you know, stove piping or the idea that everybody is doing their things on their little islands and it should all come together and the spirit of this document just as much, I think, as any bit of risk management in enterprise. The chief risk officer or whoever's running that risk program should be the one who she or he is bridging the gap amongst all of those pipes and making sure that they're communicating readily, and that's where it goes back to that discussion of governance, Matt. The idea of having a governance structure that's built properly, that all the right players are coming to the table and interfacing on matters that, you know, let's face it, can be uncomfortable for most people. You know, we as human beings, we don't handle uncertainty very well, unless we're, you know, avid gamblers, that kind of a thing. But when it comes down to our livelihoods and the organizations that we're supporting, we tend to, you know, kind of bind up. We don't want to expose areas of weakness or uncertainty that we may have, and I'm here to say, that idea has to go away. To have an effective governance structure in--whether it's in Forte or any other world, there has to be that great degree of communication, and I think the chief risk officer or possibly a CISO, could be that great conduit of communication for any organization.

Matt Butkovic: That's a great point, Brett, and I, I just, again, I would offer that even if you're in an organization that isn't of a size that warrants the designation of a chief risk officer or a chief information security officer, someone is fulfilling that role either explicitly or implicitly. Right.

Brett Tucker: Absolutely.

Matt Butkovic: And we're all doing risk management no matter what we do.

Brett Tucker: Yes.

Matt Butkovic: It's just a question of what techniques you apply.

Brett Tucker: Yes. Yeah, and by all means, sharing it. Once again, let's find the big wins and the interdependencies of our risks, the things that keep us up at night. If we share them and we find out that we have similar concerns, we can apply the resources once instead of two or three times and, you know, waste the precious resources we have.

Matt Butkovic: Yeah, and there is a--there's a comment here from the audience from someone that has been in the role of CISO, saying that great CISOs recognize that they are part of the enterprise risk management team. I think that's spot-on, right.

Brett Tucker: Spot on. Yeah.

Matt Butkovic: You've got to understand your role, right.

Brett Tucker: Yes.

Matt Butkovic: And that--I'll give you this bias that I've had from my time in private industry, and tell me if OCTAVE Forte can help me. When I was in private industry and we talked about risk, and again, I was doing this from the information security cyber security compliance front mainly, right. When we wanted to express risk, we failed when we expressed it as some abstract, highly technical articulation, right. Organizations, even those that aren't for profit, think in a monetized way, right.

So can you explain how using OCTAVE Forte can take you from, let's say, a nebulous understanding of a risk, be it a physical risk or a digital risk, and turn that into a monetized understanding of risk that you can take to that governance structure?

Brett Tucker: Yeah, absolutely, and by the way, critical. Because that's why I say, like, the--one of the big wins of Forte, what we're really trying to do in the spirit of things is we're trying to communicate a bits and bytes type risk into a dollars and sense notion so that way people can, you know, grasp it better. It's almost like we're, you know, it's in our culture or we're raised that way to understand dollars and cents arguments far better than the technological--

Matt Butkovic: Sorry, Brett. Let me offer one caveat to that, right, which is, yes.

Brett Tucker: Sure.

Matt Butkovic: There are certainly industries and missions where loss of life is actually the--

Brett Tucker: Oh.

Matt Butkovic: Right.

Brett Tucker: Absolutely.

Matt Butkovic: But the end of the day, even as organizations that are focused on missions and services that have a direct health and safety impact, those are underpinned by financial decisions, right. So I don't want to--

Brett Tucker: Right. Yeah.

Matt Butkovic: --I don't want to downplay that if you work in a safety critical industry that that's not front of mind for you, but in that governance cycle, that governance structure, you have to think about the dollars and sense, because resources are finite. So sorry.

Brett Tucker: Yeah.

Matt Butkovic: I just wanted to offer that before you gave the explanation.

Brett Tucker: No, and actually I can pick up on that easy, because let's go back to that risk appetite discussion we were talking about. You know, when you set up a risk appetite statement, not only are you trying to quantify tolerances within certain subject matter categories, like, let's say the objectives of my organization are to deliver great products and we're going to do it as safely as possible.

Well, that safety element may in fact be your highest priority in your organization. So that's the first tier of import in your risk appetite statement, and if you have any risk that perks up that's going to threaten an organization to have loss of life or maiming of an individual, fortunately, you know, or unfortunately, that you're going to take the actions necessary to insulate the organization from those risks first. They're going to get the resources necessary first and foremost above all others, and then from there down you think of it as a cascade. "Okay. I've addressed or I've covered my bases, so that way I've turned all those situations to a tolerable level of risk that I can have, and now I'm going to think about investments such that I can make to keep technical risks from coming to fruition," for example.

Appetite is the lens by which somebody's going to make that translation, right. A good example would be in said matrix of risk appetite statement, and you're going to get this later, by the way, when you read the document, you can see where there's equivalents of elements of loss of revenue just as much as on the same tier as loss of time, of production, and they can translate pretty easily if you think about loss of man hours that can be calculated with salaries to figure out or how much dollar loss there is for a certain risk impact. You can start seeing the equivalents of those categories and dialing them back to a level that's comparable.

Another good example would be a cyber security breach. So we go in, we do a business impact assessment. We find out that we've lost so much money in terms of loss of intellectual property or maybe loss of availability of a certain server. Once again, you dial it back through loss of productivity time and probably future revenues that you would realize with the intellectual property.

Matt Butkovic: Thanks, Brett. So I want to explore another topic, which is--I'm sorry for the surprise guest. This is one of the joys of working from home. Pardon me for that. So a great deal's changed in business models since we wrote OCTAVE Allegro, and one of the most pronounced differences is the quantity and criticality of the things we now put in the hands of others, right. So going from a situation where the bulk of the things your organization did were directly under the control of internal resources, to depending on third-party resources, right.

Brett Tucker: Yes.

Matt Butkovic: So if you could, Brett, could you explain how OCTAVE Forte allows you to address those risks that are an extension of your organization, right? So this is your business partners, your outsourcers, your cloud provider, right, and this is not a cyber-centric conversation, right.

Brett Tucker: No. No, not at all.

Matt Butkovic: Manufacturing, right. Using partners in ways we've never done before. Outsourcing entire business functions now. This is a common occurrence. Could you please explore that while I contend with my contingency scenario here--

Brett Tucker: Yes.

Matt Butkovic: --and our feline visitor?

Brett Tucker: Yeah, absolutely. And Matt, I think the best way to answer that is there's a discussion in there about value stream mapping. You know, you have to understand, at one point we're trying to deliver ultimately on some fundamental objective. You know do great things and make money, whatever that objective may be, and like I said, there's a string of assets that line up to deliver. You know, you use assets through a process of some sort to deliver a service or make a product that you're going to sell in the market, that kind of a thing, right.

Well, at any given point in that value stream, Matt, one of those assets may be owned by a third-party provider, and remember, when I say asset, it's not necessarily just a piece of equipment. Could be maybe a person who is being used as a consultancy or, you know, they have a certain skillset that you've had to bring into the organization from an external provider, and if you lose that person to attrition or maybe they go do other things or maybe the organization you're working with is no longer around because they've just maybe gone elsewhere, it could be the notion that you need to identify that asset and the possibility that there's a risk of losing that asset and how do I insulate myself? So am I going to build in-house expertise? Am I going to maybe just accept it? Maybe I'm just going to document, "Hey, it's way too expensive," but it's going to be a known choice that we're making and we're documenting it such that we know that when it comes to fruition we have accepted the fact that we're going to have a negative impact.

So I think that the discussion of supply chain risk and third-party providers, it all goes hand-in-hand when there's that asset identification process and understanding the value that each asset's delivering in the organization. Those conversations should be held seamlessly.

Matt Butkovic: Yeah. It seems to me that the rise of third-party partnerships, right, and this dependence on external entities makes this more important than ever, right.

Brett Tucker: Yes.

Matt Butkovic: Because not only is there a transference of responsibility for the execution of tasks, right, but also the means by which you can govern those activities change, right. So it seems to me that if you're contemplating any of those sorts of relationships or you're dealing with a pile of them that you've inherited or you just want to address where you stand when it comes to external dependencies, that OCTAVE Forte's a good starting point. Because all of these things apply, whether it's your own or in the hands of a third party.

Brett Tucker: Absolutely. Yeah, and so--and actually, that's a great point, Matt. So I want to advertise that I know we're going to have largely a cyber audience out there today that's watching, but for those of you who know others in your organization that are struggling with risks in the organization, share this document with them. There may be aha moments in there that are not cyber related and they don't have to be. Like we said, risk is like that continual underpinning of all other tasks that we're performing in an organization, and I would like to think that Forte as a process can be embraced by the entirety of an organization and not just a piece of it.

Matt Butkovic: Great. That's an excellent point, Brett. So you've mentioned the publication's coming out soon, so you're writing a technical report that describes the new OCTAVE Forte method. That will then come with training courses and other artifacts that allow you to apply OCTAVE Forte. So kind of two questions. The first is if I'm a current OCTAVE Allegro user, anything I need to do to get ready for OCTAVE Forte? That's question one. Question two, if I'm not an OCTAVE Allegro user and I want to consider using Forte, how best to start the process of integrating it into my organization?

Brett Tucker: Yeah, so that's a great question and actually one I hadn't entirely considered, because I wrote Forte to be independent. So if you're an organization that's never even heard of Allegro, picking up Forte would be a no-brainer just as much as you were an Allegro user. So remember, Allegro would be a subprocess to Forte, like Steps 4, 5 and 6. As a matter of fact, I have a nice overlap here where it's more on the identify, analyze side, and there's a little bit of planning that goes on in Allegro and a little bit of controlling, so maybe I need to give it better credit in this particular diagram, but to be honest with you, no, Matt. There's really no preparation necessary, outside of preparing yourself to understand that you need to have a broader perspective on your enterprise, whatever your organization may be doing, and if it's public or private. It's the idea of embracing the fact that there are risks throughout the organization and they all need to be digested in a standardized manner. So I think that's the best way to prepare is to have an open mind to applying risk management across more than just cyber-specific risks.

Matt Butkovic: I think you said something that I'd like to reinforce, Brett. Well, you said many things I'd like to reinforce, but this one is front of mind for me. So it really is that combination of experts in these other domains, physical security, physical asset experts, the people asset management function and organization. We need input from folks with those disparate skills to help us improve this, right, and I would say that's true of all risk assessment methodologies. I'd say it's as true for FAIR and RMF as it is for Forte, so--

Brett Tucker: Absolutely.

Matt Butkovic: --I would encourage the folks watching today, as you said, to not think about this, although it's coming out of an institute, focused on the digital or cyber or software challenges of the nation, to help us make this more compelling and accessible for those other audiences.

Brett Tucker: Yeah, absolutely. Risk management's a team sport.

Matt Butkovic: Absolutely.

Brett Tucker: (Inaudible) that.

Matt Butkovic: So Brett, I'd ask you this, right. So if once the report is issued, which is going to be in the very near future, and someone has their hands on this copy of the new risk--the new OCTAVE Forte methodology, where should they start, right? In the document itself. It's quite a lengthy document.

Brett Tucker: It is.

Matt Butkovic: You know, there's a temptation to say kind of read it all and understand it, but I don't think that's a viable answer.

Brett Tucker: No.

Matt Butkovic: If you're an existing OCTAVE Allegro user, where do you start, and if you're new to all this, where do you start in the document?

Brett Tucker: Yeah, that's a great question, and I can't tailor that question specifically. I'll speak broadly to it. I would say go to where you're feeling the most pain first. You know, is it the fact that you feel that you don't--you have a disconnect with your overall, you know, management structure, that you're not getting the resources you need?

Well, if that's the case, then maybe you start at Step 1 and help learn how to build out a governance structure for your program. Or maybe it's the idea that you notice that you have tons of great response plans and people come to the table and they say, "Hey, I have a risk," they present it and then you never hear from them ever again. Well, then that might be the lightning rod that tells you, "You need to go to Step 8 and figure out how you're going to projectize some of these implementations and make sure that they do go to plan."

So I would say go to the point where you're feeling pain and open to that step that is most applicable, where it can address that pain or fill that gap.

Matt Butkovic: Excellent. So Brett, I have a lighter question for you.

Brett Tucker: Sure.

Matt Butkovic: You’re both a risk management expert and a life-long Cleveland Browns fan. How do you reconcile those (inaudible)?

Brett Tucker: Yes. Because my appetite and my tolerance for pain and embarrassment is very high.

Matt Butkovic: I see.

Brett Tucker: Yes. My ability to adjust to disappointment, you know, my resilience scale there is infinite.

Matt Butkovic: I see. Sorry for the aside. (Inaudible)--

Brett Tucker: That’s so true. It’s so true. I’m from Northeastern Ohio, for those who don’t understand, and I’ve lived in Pittsburgh now, and slowly, over time, my wife, God love her, she has been very gracious to convert my wardrobe from brown, orange and white, to black and gold, so I don’t know.

Matt Butkovic: There’s a capping thought here from a member of the audience, which is saying that certainly the Forte cycle has an appeal to cyber security and risk management professionals, but in the C-suite, they may have difficulty with a 10-step process.

Brett Tucker: Yeah.

Matt Butkovic: I think that maybe that’s a misunderstanding of how we intend to use this. Could you explain sort of what the distillation or the artifacts would be that would use out of Forte that you would then present to an executive audience?

Brett Tucker: Yeah, absolutely, so--and it’s all about context of reading the document, who’s reading the document. I would say that the Forte as a process and as a document in and of itself, the technical note, is not really intended for a C-suite audience, although it’d be good if they understood the underpinnings of a program. Rather, it’s for that chief risk officer, chief information security officer, whoever’s running that risk program, to learn how to best build out their program in terms of, “What tools do I need, what actions do I need to be taking?” and then they’re going to turn around and they’re going to radiate the information necessary up to their management teams to say, “Hey, here’s what you need to know about governance. Here’s what you need to know about appetite, and here’s how you’re going to fulfill your duties within that overarching structure, that overarching process.”

At no point in this process here is there just one singular party that is committed to all 10 steps, right. It's a team sport in that we tap different people at different times to achieve the end of good risk management. Whether it's the asset owner in Steps 2, 3 and 4, whether it's the person who's ultimately assigned to be responsible for the risk, who maybe, by the way, may not necessarily be the asset owner, who's implementing a response plan, and then at the top of the process maybe it's the governance team, where you have senior executives, senior managers, leaders in an organization who are making the element decisions is that, "Go left, not right," or, "Invest money here, not there."

So yeah, I would agree that to have an appreciation for the fact that there's that 10-step process taking place, that's about the extent of really what they need to know.

Matt Butkovic: Thanks, Brett. Well, unfortunately, we've reached the bottom of the hour. So Brett, I want to thank you very much for the overview of OCTAVE Forte, and I want to thank the audience for their kind attention, and with that, I'll send it back to Shane for a wrap-up.

Shane McGraw: Yeah, Brett, Matt, great discussion today, and thank you guys both for sharing your expertise. As Matt mentioned, we'd like to thank you all for attending today. Upon exiting, please hit the "Like" button and share the archive if you found value in today's talk. Lastly, join us for our next webcast, which will be on September 15th. Our Topic will be the CMMC, with Matt Travers and Gavin Jericho, and you will all be emailed the registration link for that.

Any questions from today's event, please send them to info@sei.cmu.edu. Thanks, everyone. Have a great afternoon.

Matt Butkovic: Thank you.

Brett Tucker: Thanks, everybody.