Assuring Mission Success in Complex Environments
Transcript

Part 1: Background and Evolution from OCTAVE

Julia Allen: Welcome to the CERT Podcast Series, Security for Business Leaders. The CERT Program is part of the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org.

Show notes for today's conversation are available at the podcast website.

My name is Julia Allen. I am a senior researcher at CERT, working on security governance and executive outreach. I am very pleased today to introduce Chris Alberts, a senior researcher in organizational and security risk management. Today we'll be discussing new work in progress, addressing how to ensure mission success in the face of increasing complexity and inherited risk. And Chris will tell us more about those. Welcome, Chris.

Chris Alberts: Thanks. Great to be here, Julia.

Julia Allen: Yeah. I'm really happy to have a chance to talk with you about what you're doing. So let's get started. You were responsible for CERT"s information security risk evaluation method, OCTAVE, Operationally Critical Threat, Asset, and Vulnerability Evaluation. Tell us a little bit about that experience and how it influenced your current thinking.

Chris Alberts: Well, when I look back at the original ideas behind OCTAVE, it was really to help enable people within organizations to perform assessments and to understand the current security posture and how to improve that.

I think what we were trying to initially look at was what we call local optimization, which is where you focus on maybe a subset of all your issues, let's say security, in a system or in an organization. Well, as soon as you start partnering with other organizations, your security is only as good as their security. If your partners are not doing the same thing, the overall mission or the overall objectives you're trying to achieve might not be achieved because not of something that you're doing, but something that one of your partners, collaborators, or customers are not taking due care with from a security perspective.

Julia Allen: So it kind of goes back to this notion of "you're only as secure as your weakest link." So when you've got these interdependencies, to not take those into account could give you a false sense of security.

Chris Alberts: Exactly, a false sense of security. And so instead of looking more statically at these assessments, we're looking more dynamically, looking at what are the interrelationships and dependencies, and how do they affect one another.

We wanted to look at security in the broader business context, and to do that we had to broaden to look at: What are all the factors, or at least as many of the factors as we know about, that affect the ability to achieve the business objective?

Julia Allen: Right. So you're trying to put the security issues in context, because clearly security does not stand alone. It supports the business. It factors into the work processes of the business,

the information flows of the business. So you're saying you need to take a broader set of considerations into account.

Chris Alberts: Yeah, exactly. And then what you can do is once you look at this broad picture, now you can start better allocating resources where they're most needed. And so this also starts making the case for security in many instances, because many organizations neglect security issues because they don't really make the connection back to the business.

Now what we can do is show them how neglecting important security issues may affect their ability to do whatever it is they're doing, such as if they're in a hospital, deliver healthcare to their patients. If they're building software systems, being able to build the systems, things like that.

Julia Allen: I know, because we've been arguing for a long time in our security governance work this whole notion of putting security in context, because if you can't describe it in a way that makes sense to the leaders of the organization in terms that are meaningful to them about the critical success factors for the business, then it's not apparent why they should necessarily invest.

Part 2: Assuring Mission Success

Chris Alberts: Yeah. What we're really looking at here is developing confidence in your ability to achieve your objectives. And we're focusing mostly at the local level of processes and programs that are distributed across multiple organizations. So an example we've worked with in the security area is incident management. You think about the ability to detect and then respond to incidents. Very often the people who run the call center operations are different from the people who monitor the networks for an organization, and they're different from people who actually do the response. And, in fact, often they're doing this all for, let's say, a government customer. So you have at least four players in this particular situation.

And so now what you have is a truly distributed environment that becomes fairly difficult to manage. We were getting some requests from people to say, "I'm not really sure that we're going to be able to respond when we have to."

Julia Allen: Right. Because I really don't have control over that whole process flow, or impose all those rules and responsibilities.

Chris Alberts: Right. And not only that, I'm getting all these different status reports, but I can't make any sense out of them because I really don't know how what one contractor is telling me relates to what another contractor is telling me. I don't have the big-picture view.

And so that's what we are trying to put together in this ability to assure mission success. Because what we're trying to do is give that manager or a group of managers some sense of confidence that they'll be able to do what they intend to do.

Julia Allen: Is there a particular way that that confidence can be expressed so that they can really understand what their exposure is?

Chris Alberts: Yeah. Normally, most managers understand at least the dimensions of success that they're looking for. In incident management, there is a quality of response. Are you doing the right things?

Julia Allen: Right.

Chris Alberts: What's the impact on your constituency? So they kind of have those dimensions understood.

Julia Allen: Right. In other words, I will know what good incident management is when I see it, because I have kind of this innate sense of what an acceptable level of performance is.

Chris Alberts: Right. So we start there, and what we have is a systematic way of breaking down those objectives, as we call them, or dimensions of success. And looking at what is the best-case scenario, what's the worst-case scenario for each of the objectives, and what are some scenarios in between. So what we start doing is having them think about: What is good performance? What's bad performance? What's acceptable, and what's not? So let's take the case of where we do five scenarios from best case to worst case. How many of those in-between scenarios are actually acceptable performance, and how many are not?

Julia Allen: So does this equate back to kind of notions of risk tolerance or risk threshold, this notion of acceptable and unacceptable?

Chris Alberts: We're looking more at the aggregate. We're not looking at individual risks. We may look at causal chains that create the outcome, but we're really looking at: What is the most likely or expected outcome? And also what are the range of outcomes that you can expect based on various conditions that you might encounter as you're trying to achieve your objectives? And so by doing that, then we can look at where your likely outcome is in relation to where you want to be. And now that gives us our gap that we can now start to look at improvement.

Julia Allen: Also, I've noticed in looking over some of your work you describe this concept of inherited risk. Can you say a little bit about that, because I think that is kind of a novel way to think about risk dimensions that maybe business leaders haven't considered before.

Chris Alberts: Yeah. That gets back to the notion that we're not working in isolation. We talked about incident management and working multiple contractors to manage incidents. And so the idea of inherited risk is that it gets back to the idea of local optimization that I talked about a little bit earlier. At some point you can improve your operations as much as you can. Depending on what your relationships, what your interfaces are, with your partners and collaborators, their actions are influencing your risk. So you're inheriting some amount of risk from what they are or are not doing.

Julia Allen: So sometimes we talk about this notion of upstream and downstream, like in the supply chain you've got providers giving you goods and services and information. And then similarly you're turning around and providing that to somebody else. So I assume you can inherit risk from your upstream, but you can also pass on risk to your downstream.

Chris Alberts: And we call that imposed risk. So you inherit an imposed risk, and so each link in the chain is receiving risk from upstream and giving risk from downstream. And as you look at any process, the risk is either amplified or dampened as it moves from point to point, because you can compensate for some amount of risk that you inherit, and maybe actually reduce it or dampen it. On the other hand, your local practices may actually amplify that risk.

Julia Allen: Right. They actually make it worse.

Chris Alberts: Make it worse. And so what happens is that you start looking, as risk flows through the process, you can now start looking at how it's either amplified or dampened, and if you have successive amplifications, it can start getting out of control. And that's when you get into a lot of

problems with a lot of these distributed processes and programs, because there are no controls for the risk that is inherited and imposed throughout the chain.

Part 3: Methods and Tools for Tackling Risk in Complex Environments

Julia Allen: So let's try and get, if we can, a little more tangible and maybe get into some arenas where you can actually say, "Okay, so you've got this incredibly complex arena that you're operating in and probably getting more complex every day. So what can business leaders really do?" So let's stay with your incident management example, and could you describe kind of in fairly simple terms how the methods that you're developing might help an organization who has upstream risk, has inherited risk, has the potential for imposed risk, and how they could use your methods to actually gain higher confidence that their incident management process is robust?

Chris Alberts: One of the things that we assume, and is a very safe assumption, is that people are doing some things in terms of their management of their process, management of their risk, being able to resolve and manage problems, and also managing the actual product or service that they're providing, as well. So they're doing things, but they're often disjoint.

Julia Allen: Right. And maybe stove-piped.

Chris Alberts: And stove-piped. And so what we're doing is we're actually creating a suite of tools that we're putting under the banner of what we call SEI MOSAIC, and that stands for Mission Oriented, Structured Analysis and Improvement Criteria. And that kind of takes and forces to come up with an integrated view of the objectives you're trying to achieve, and then look at how what you're doing—from a process perspective, a product or service perspective, and risk in a problem management perspective—how all those various things that you're doing affect the eventual outcome that you're trying to achieve.

In the area of incident management, what we do is take what you have, your current knowledge of the process, your current risks that you've identified, all kinds of documentation about what you're trying to achieve—

Julia Allen: Right. Maybe some of the roles and responsibilities that players in the process currently have.

Chris Alberts: Exactly. And we take all that information, talk to people about what's actually going on in these processes and look at the deviation from what's documented versus what people are actually doing, and then put this big- picture view together that says, "Here's where you are in relation to where you want to be."

So in terms of the incident management example I talked about before, we'll look at what the call center's doing, what their practices are, look at the documentation, see what their risks are, and we'll do that for each of the players involved, so the people doing the monitoring of the networks, the people who actually do the response, the people from the customer side. And so now what we can start doing is putting together that big picture of how do all these different parts play together.

Julia Allen: So in the case of your methods of the MOSAIC approach or the tools that you have within that tool suite, how would you help an organization solve that particular problem?

Chris Alberts: We've designed something we are calling the mission diagnostic protocol. I often refer to it as just the mission diagnostic, that's really kind of a setup of roughly ten indicators that we tailor to any specific situation that we're looking at. So it's not always the same ten indicators.

If you're looking at security incident management, that's different than if you're looking at investing in technology, for instance.

Julia Allen: So in the case of incident management, what might be an example of an indicator, just so I can better understand what those are?

Chris Alberts: We would be looking there at indicators related to how the process is working. So we would look at things like, "Is there a design for the process?" "Are risks being managed?" "Are stakeholder pressures affecting the way that you're doing your work?" Another one might be, "Is your mission explicitly defined?" So by a number of simple questions, you can kind of get a gauge for the general health of what you're doing. So you can determine whether you're reasonably good, very good, or poor.

Julia Allen: So that helps focus where the attention needs to be applied for improvement.

Chris Alberts: You can start looking for gaps at the local level, and then you also, if you look at this across the whole end-to-end process, you could look at the things that you might not see at the local level that kind of become apparent at the end-to-end process. I'll give you an example of that. In one of our pilots, the different groups were actually working towards objectives that were actually running counter to each other.

Julia Allen: So they were kind of at cross purposes and probably didn't even realize it.

Chris Alberts: Exactly. And so it wasn't until we looked at the end-to-end process that that particular issue came up. And if that didn't get fixed there was no hope for them to actually work together and actually achieve the mission, because they were kind of working at these cross purposes that affected their ability to achieve their mission.

Julia Allen: So it sounds like you'd want to take a look at this assuring mission success approach, and maybe even use it while you're considering a new project or a new initiative or a new process, to help you construct that approach with the potential for higher confidence in the outcome. Is that reasonable?

Chris Alberts: Exactly. It's a life cycle approach that you can start at the very beginning, when you're first making choices about, "What's our mission, what kind of staffing are we going to need?" A lot of the risk, whether it's a development project or an operational process like the incident management, is that a lot of the decisions that were made early in the life cycle regarding scope of the work that they're doing, how much funding—

Julia Allen: Requirements.

Chris Alberts: Requirements, and all of that, affects what happens in the field. But once you get to the field, it's very hard to go back and change those things. And the other thing, we have other, more sophisticated tools that actually kind of build into current process management techniques, such as workflow diagramming. And we have a way of taking a technique called MAAP, which is Mission Assurance Analysis Protocol, which actually takes a workflow and where we can actually create a risk causal chain to look how risk flows from the beginning to the end of the process.

Julia Allen: At each step and where risk is maybe being created at one step and being handed off to the next.

Chris Alberts: Exactly. The indicator look gives you a broad-brush look and some general indications of where your troubles are. I kind of liken our approach to healthcare. The general physician says, "We know you have some problems in these areas. You need to go to a specialist." That's mission diagnostic. MAAP is more of the specialist, where you take that real detailed look to say, "Here's exactly where your problems are."

Julia Allen: Oh, that's a good analogy. So, closing up on our conversation, I just have a couple of remaining questions. What role in the organization is in the best position to make use of the methods that you've described? Is it a chief risk officer? Is it a program manager? What have you found so far in your pilot work—people that are in the best position to try and embrace some of these approaches and get them into their business processes?

Chris Alberts: We've been focusing on the management of processes or programs. In terms of the incident management example I gave earlier, the government organization that owned that mission, they're the ones that were responsible for it being done ultimately. That's who we normally go to, because they have the contractual oversight of all the different people that come together to do this. And they're working on behalf of a set of constituents that are relying on these services. So it's really the people ultimately who oversee these complex missions, is who we're mostly targeting.

Julia Allen: Right. It sounds like also it's the people who have the purse strings, or at least have the ability to authorize spending for the project, and therefore want to make sure their money's well spent to ensure a successful outcome.

Chris Alberts: Right. And then also as all improvement projects require, sponsorship at the senior level, because a lot of times to get the approval for these kinds of expenditures requires approval several levels up in an organization's hierarchy.

Julia Allen: Just in closing then, can you say a little bit about the current state of your work and where we can find out more about it?

Chris Alberts: Sure. The current state of the work is we've been piloting these various techniques I've talked about in the field. We're publishing some technical reports, highlighting some of the things that we've done. We have a new webpage up on the Software Engineering Institute's website where people can come for more information as well.

Julia Allen: Great, Chris. Well, I think this will bear some very beneficial fruit to organizations that find themselves operating in this highly complex environment that you've described and hopefully will take full advantage of the experiences and the tools and the methods that your team is developing. Thank you very much.

Chris Alberts: Thanks, Julia.