Title: Security Risk Assessment Using OCTAVE Allegro
Transcript

Part 1: Introduction to Allegro: Rationale and Application

Julia Allen: Welcome to CERT's 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'm a senior researcher at CERT, working on security governance and executive outreach. Today I'm pleased to welcome back Lisa Young, a senior member of CERT's Survivable Enterprise Management Team. Today Lisa and I will be discussing the OCTAVE Allegro security risk assessment method and how it has evolved from CERT's original OCTAVE work. Just for information, OCTAVE stands for Operationally Critical Threat, Asset, and Vulnerability Evaluation. So welcome back Lisa.

Lisa Young: Thank you, I'm happy to be here.

Julia Allen: So for our listeners who are not familiar with OCTAVE, could you just give us a little bit about its history and how it came to be?

Lisa Young: Sure. OCTAVE's been around for many years, going on ten I think. But it was originally developed for large complex organizations who were looking for a way to evaluate their information security risk, in the context of the operation of the business. And OCTAVE was one of the first evaluation methods to consider security outside of just vulnerability assessment. It has methods to collect information about organizational vulnerabilities, and it also has many volumes of guidance on risk assessment and the principles of risk management.

Julia Allen: Building on OCTAVE and its history, and all the different variations that folks have developed, what motivated CERT to kind of look at a refresh, a next generation of OCTAVE which you call OCTAVE Allegro? And if you could kind of compare Allegro with the original OCTAVE, that would be helpful.

Lisa Young: Sure. Well, one of the main reasons is that we were looking for a way to help organizations roll out risk assessments that could be easily adopted, without extensive risk management training, and that also could be standardized and institutionalized across the organization. And also since OCTAVE was developed a long time ago, a significant time had passed and we have a lot more knowledge than we used to about – we've taught OCTAVE, we've watched organizations use the method, and OCTAVE focuses on the organization as a whole.

So while this was beneficial to organizations, it was often a barrier to widespread adoption, so we focused Allegro just on information. We noticed that people are extremely concerned about protecting information or data. And what made this a little bit easier for people to adopt is that we didn't sort of boil the ocean. We said "Okay, let's focus on information and then let's focus on where that information lives. What are the containers where the information is stored, where it's transported, or where it's processed?" So this streamlined the process and made it easier for organizations to adopt and roll out.

Julia Allen: So when you say "information" you're talking about things like PII, Personally Identifiable Information, maybe customer databases or financial databases, things like that?

Lisa Young: Exactly, yes. Information, information is becoming much more – I mean it is an intangible asset. And oftentimes in an organization the places where the information lives, the containers is what we call them, they could be people. People carry around information in their heads. It could be servers. It could be various kinds of media. It could be paper. But we found it was actually the information that people were most concerned about. And also when you're trying to apply security controls or security protection, generally they're applied at the container level. So it made it a lot easier for people to understand what we were talking about when we said "Where is information, where does it live in your network, and where does it live in your organization?" It made it easier for them to digest.

Julia Allen: So what roles in an organization, in your experience, can make best use of a method like Allegro?

Lisa Young: Well, that's a great question, because I have to tell you, in the title it says "information security risk assessment," so information security personnel of course. But this method can be applied to many other areas of the business. One of the most common things that we've seen in the field is – the reason for misalignment between senior level strategy and the operational practices of the organization is that the risk assumptions are often different, or the risk assumptions of senior management are not necessarily communicated to the operational folks.

So for instance, business continuity staff; they conduct business impact analysis. Security conducts information risk assessments. Audit conducts control self assessments. And then physical security has their own method of conducting risk assessments. And what often happens is that the assumptions that these risk assessments are based on are either not from senior level management, because they haven't been communicated, or they're based on localized – what people locally think the risks are, not what the risks to the whole business are.

One of the first steps in Allegro is to determine the evaluation criteria that are important to your organization. And if that evaluation criteria is determined based on risk to the business, and communicated to the organization, then everyone's operating off the same page in terms of knowing what risks are important to address.

Julia Allen: So when you're scoping Allegro and how you're going to apply it – what part of the business or what sets of information you're going to apply it to – how do you determine what roles need to be involved?

Lisa Young: Well, I think what generally happens is a lot of times one area of the business will decide that they want to conduct risk assessments and they'll sort of start the process. So it could sort of start on a grass roots level, at information security or business continuity, or anywhere in the organization. So for instance, evaluation criteria. The evaluation criteria in Allegro is things like reputation; customer Confidence; life, health, safety of customers; fines or legal penalties from, from non-compliance. It could be financial. It could be productivity.

And what happens is, as these questionnaires are looked at and people start to go through the risk assessment process, they realize they have to reach out to other parts of the organization to get these answers, and then it sort of starts to grow from there. So I've seen very good success from a top-down approach. I've also seen very good success from an information security grass roots perspective in just getting other business units involved.

Julia Allen: I can see with this information-centric and information-container-centric view, actually anyone who is in an information owner, an information custodian or stewardship role, or has concerns about the controls around the information that they're responsible for, could initiate an Allegro assessment, right?

Lisa Young: Absolutely, and where I've seen this have the most success is when you get the business owners involved. I have a customer and they have institutionalized this. And it's actually a medical institution, a medical facility. And they conduct regular roundtable meetings of all the different business owners, and they talk about what the risks are in their particular area. And it's really gone a long way to fostering an open communication about risk and about what's important to the business.

Julia Allen: Well Lisa, you touched on this a little bit. But could you say a bit more about what part you've seen Allegro playing in an organization's broader compliance and risk management efforts? As you said, there's all kinds of assessments, all kind of risk management, all kinds of compliance requirements, so how does Allegro kind of factor into that mix?

Lisa Young: Well, one of the main ways that an organization can strengthen their governance efforts is for senior management to communicate its risk assumptions to the business, and for all areas of the organization to look at risk in the context of the business. So many times by standardizing on a risk assessment method – and there's many of them. Allegro is just one of many. But what makes Allegro special is that it's streamlined. You don't have to have a lot of training. It's more questionnaire driven and it's more in the context of the business.

But many times an organization can derive value from its compliance efforts by taking a more holistic view of risk or perhaps using the data that it collects for compliance for other purposes such as assessing risk to the organization.

Part 2: Allegro's Eight Steps, and Getting Started

Julia Allen: Okay. Well, from your report, your technical report last May of 2007, I see that Allegro is made up primarily of four phases and eight steps, and I wonder if you could kind of briefly introduce those to our listeners.

Lisa Young: Sure, I'll just go through the steps and then I'll talk about the most important one. Step one is to establish your risk measurement criteria. This is where you start to align your risk assumptions and figure out what's really important to the business. Step two, you develop an information asset profile. And how this connects is information assets are where the information generally lives. Step three, you identify the containers, and that could be people, paper, servers, any kind of media. In step four, you identify the areas of concern. And step five, you identify threats scenarios. So we still look at vulnerabilities. We still look at organizational issues, any areas of concern that are brought to you from your business. It's important to have a way to look at those in the context. We identify risk [step 6], analyze risk [step 7], and then select mitigation approaches [step 8].

There's some ranked stacking that we do within Allegro. So we teach you how to say "Okay, well, which of these are most important to you?" and all that does is really give you a way to prioritize and rank stack in your organization. We put a arbitrary value on it to help you quantify which risks you want to look at first.

Julia Allen: Okay, you had said that you wanted to kind of highlight what of those steps, which ones you feel are the most important?

Lisa Young: Well exactly. The first step is really most important, because it's the evaluation criteria. And this is the criteria against which the risks that you uncover are evaluated. And that's really important because, as you start to look at risks throughout your organization, each area feels that their risks are most important. And so as a business leader you need a way to evaluate them.

So the very first thing we do is come up with evaluation criteria, and these are more quantitative in nature, so they could be things like reputation, customer confidence, productivity. So you can actually assign numbers to say, "If we lost this much productivity or if our computer systems were unavailable for a certain period of time," you can start to put numbers to these things and how they impact your business – fines and legal penalties – depending on what type of business that you're in. Also life, health, safety. So if you are in a business that does have life and safety concerns you can actually start prioritizing them in the context of what your business is.

Julia Allen: It sounds like these criteria are very much driven by business mission, objectives, goals, strategies, what have you, correct?

Lisa Young: Yes, that is very important. And the thing about a risk assessment is that it is subjective. I mean it is based on the risk to your business, not to everybody's business. So it has to be based on your mission, your objectives, and the things that are important to you. Also the nature of some businesses is more risky than others. What Allegro gives you is just a standardized way to uncover what's important to you.

Julia Allen: Do you think it would make sense to do an OCTAVE Allegro assessment, say, if you were looking at a merger and acquisition opportunity or if you were looking at offering a new product and service? Could Allegro help you kind of evaluate the upside and downside of those kinds of opportunities?

Lisa Young: Absolutely. I think it's really important, especially in mergers and acquisitions, that you understand what risks can be uncovered and which ones you need to know about beforehand. So I think yes, it gives you a very good picture of that. And it also gives you a very good picture, because a lot of these questionnaires are filled out by business owners and by various people in the organization. So it gives you a sense of what do the people at the operational level think are the risks versus what senior management thinks are the risks to the business.

Julia Allen: Right, and as you said, sometimes that just having that conversation is as valuable as the assessment itself.

Lisa Young: Absolutely.

Julia Allen: So how long does an Allegro assessment take that you've seen conducted in the field? And how often should an organization reassess using Allegro?

Lisa Young: Well, that's a great question. It shouldn't take very long and I'll tell you why; because a risk assessment is just an assessment of a point in time. So you're looking at risks today, and tomorrow and the next day they might change. So I think it's important to do more frequent, smaller assessments. So the scope of the assessment should be perhaps maybe just one system, or one application, or one business unit, just something you can get your arms around. It shouldn't take more than a week or two to collect the data and take a look at what you've got, do some basic analysis, and then you start collecting these on a more continuous basis. And then you can start looking – really get a really good picture of the risks across the business.

So yes, anywhere from, I would say two or three days to two or three weeks, depending on the size of the scope, but it shouldn't take a really long time. And as far as reassessment, I think it's really an iterative process. Certainly you can look at one scope and then come back to it in a few months and come back to it in a year and see what's happened, but I don't think that it's something that you do and just put on the shelf.

Julia Allen: Because it occurs to me that maybe the trend line – you do an OCTAVE Allegro assessment at some point in time. And then maybe 30, 60, 90, 120 days, or 6 months, whatever your window is, you do another. And as you said, it's a point in time assessment but the risks are always changing. But I think it would be kind of interesting to have a series of these and then kind of see where the trend line takes you. Have you seen anybody use it in that way?

Lisa Young: Yes I have, and what's really valuable about that is that you can start to collect metrics. One of the things that we're always looking for, in the security field especially, is what are valid metrics to see if we're doing a good job. And one of the things that I've seen people do with this is collect this data very clearly and start to collect metrics. Now sometimes when they start collecting them today, they're not sure if they're really valid. But after you do this two or three times you can say "Well, wait a minute. This metric isn't so important. However these are, and I'm going to start collecting them on a more regular basis because they mean something to my business."

Julia Allen: That sounds like very, very good advice and I think could provide some interesting insight around a subject that's hard for business leaders to get their head around. So, as we come to our close, if someone wants to consider doing an OCTAVE Allegro assessment, what would be a good way for them to get started?

Lisa Young: Well, I think the very most important thing is its important for business leaders to communicate their risk assumptions to the business owners, application owners, and operational staff. And one of the ways in which they can do this is by taking a service view of the organization. When you look at most, even most really big organizations, whether they make a product or deliver a service, they generally only have about 10-12 key services, right? Even the largest companies are divided into business units and those usually have about 10-12 key services that they offer. And making the connection between who you are as a business and the service that you offer, or product that you offer, and the underlying assets at the operational level, is one of the ways you can identify and prioritize the critical services. And then the operations staff will then have a better understanding of which assets are at risk in delivery of that business service. They can also tell you which assets might benefit from additional risk analysis. So this helps to assist all levels of management with decision making when you consider the risk in the context of the service that you are delivering as a business.

Julia Allen: Well, thank you very much Lisa. Do you have any pointers where our listeners can learn more about Allegro or other OCTAVE related information?

Lisa Young: Sure, on the CERT website – and we'll have that information in the show notes – there is a technical note and it's called *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*. And that's our latest tech note. It also has all of the forms and the documents that you would need to start this process in your organization. So it's definitely there and it's available for you to download.

Julia Allen: And I assume then that this is something that organizations can do on their own. They don't require CERT assistance to proceed.

Lisa Young: That is correct, and I forgot to mention that, so thank you for bringing that up. That is one of the key things about this, is that you can pick this document up, you can read it, and you can start small and start on your own, so all the direction that you need is there.

Julia Allen: Well Lisa, I'm so appreciative of your time and your expertise and giving us this insight into how CERT's information security risk assessment methods are evolving, so thank you very much for your time today.

Lisa Young: Well, thank you Julia. I appreciate you asking me to be here again. It's really nice.