Adapting to Changing Risk Environments: Operational Resilience
Transcript

Part 1: Why Operational Resilience?

Stephanie Losi: 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 Stephanie Losi. I am a journalist and graduate student at Carnegie Mellon working with the CERT Program. Today I'm pleased to introduce Rich Caralli, a senior researcher with CERT in the area of Operational Resilience. We'll be discussing why this topic is important for today's business leaders. So, Rich, let me just jump in right here and ask you: What is operational resilience, and why is it a growing area of interest and concern?

Rich Caralli: Well, operational resilience, in very simple terms, is the ability of an organization to adapt to changing risk environments. And so most organizations are very aware of the need to do that, and as they enter lots of different new unknown spaces and markets and things like that, they really are exposing themselves to these risk environments over and over again. In business terms, the operational resilience really means the organization's ability to keep the business processes and services that most support the organization's mission able to do what they're supposed to do, to contribute to the mission.

Stephanie Losi: Okay, and no matter what happens, is that the idea?

Rich Caralli: Sure, because resiliency is really, in essence, both trying to protect the assets that the organization depends upon, as well as being prepared to react to the consequence if those assets are in fact some way interfered with.

Stephanie Losi: All right, and so basically what would you say is the main problem that is addressed by operational resilience? Why should business leaders care about this topic and really try to wrap their minds around it and understand it and also figure out how to apply it?

Rich Caralli: Sure. I mean it's a growing area of interest because organizations are starting to realize the value of being able to manage it. In other words, as you enter all these different risk environments, as the world changes around you, you can't react to it anymore: it takes too much energy to do that, it takes too much reliance on people, the conditions change so rapidly that your competency for reacting over time is just really diminished. So you have to have some way to actively manage it, and as organizations try to grow and to really do the things that the shareholders want them to do, they have to be able to manage the environment that they're entering, so they have to try to get some handle on that.

And, for example, I'm working more and more in the banking and finance industry, and for them it's more not only to be able to do what I said, but it's also a regulatory driver. It's something that the regulators really want to get a handle on.

Stephanie Losi: Right, or have told them that they have to, I mean in some cases with Sarbanes-Oxley.

Rich Caralli: Absolutely, right.

Stephanie Losi: How can a business leader assess their organization's current state with respect to operational resilience?

Rich Caralli: Yeah, I think one thing that's important to point out early on in this podcast is that enterprise resiliency and operational resiliency are different things.

Stephanie Losi: Okay, and can you explain the difference?

Rich Caralli: Sure. Operational resiliency has to do with managing the hazard risk essentially that emanates from day-to-day operations, right? It's basically inherent in the things that an organization does to achieve its mission. Enterprise resiliency is a broader term, so it brings in all the other aspects of risk management, like business risk and market risk and credit risk and all of those things. So operational resiliency is really taking out a slice of that picture and it's saying, you know, "From the operations standpoint, what are the kinds of risks that the organization is exposed to, and how can we actively manage them?" So it's very different than that bigger picture.

Stephanie Losi: Okay, and so what areas would you say operational resiliency is confined to? I mean, IT might be one of them.

Rich Caralli: Yeah. I think absolutely IT, but it certainly centers around all of the things that business processes touch. So if I take the traditional definition of operational risk, which is tied to operational resiliency, and we can talk about that more, it looks at things like failed internal processes, and fraud, and inadvertent and deliberate actions of people, and of course it's as broad as hurricanes and tornadoes and natural disasters and terrorism, things like that. So, it is this very broad space that our organization really has to manage within to keep its mission viable.

Stephanie Losi: Okay, and so how would you, if you were a business leader and you were starting out to try to assess where you stand, how would you measure your level of operational resiliency?

Rich Caralli: That is a very difficult question and it's the central question of the research project that we have going on. Today organizations measure their operational resiliency in terms of what hasn't happened. In other words, "Well, we went the last three months without a major disruption, so we must be doing pretty well."

Stephanie Losi: Right, "So this is good."

Rich Caralli: "We're resilient," right?

Stephanie Losi: Yeah, right.

Rich Caralli: Or, "We went the last two weeks without a virus," or something like that. The problem is if you're an executive in this domain and you're called in front of the stakeholders and they say, "Well, are we secure?" or, "Are we sustainable?" or, "Are we resilient?" you can't answer in the affirmative. You can just sort of answer in the absence of information. And our research project is built around giving organizations the ability to say, "We are resilient, we are competent in that space, and here's why, because we're doing all the right things."

Stephanie Losi: Okay, okay, and so how does it give people that ability? What does it really give them, what tools, what measures?

Rich Caralli: Well, today, one thing an organization can do is they can pick up common practice sets, like ISO 27001, okay, in the security space. Or they can go to some of the BC/DR (Business Continuity/Disaster Recovery) space practices. Or they can go off to the operational IT operational space, like with COBIT and ITIL, and they can do a quick comparison against those practices. And they can kind of know that in their industry or overall, these are the kinds of practices they ought to be doing to sort of manage resiliency in its chunks.

The problem with that approach that we found is that operational resiliency is really dependent on the collaboration between those three basic activities and actually several more. The ones we're focused on are security, business continuity and disaster recovery, and IT operations service delivery excellence, essentially.

Now, one of the interesting things that we found in this research project was if you look at practice sets in the security space, or the BC/DR space, or IT ops space, they always sort of cross into the other ones, right.

Stephanie Losi: Right, okay.

Rich Caralli: By necessity, what they're saying implicitly is, "Well, operational resiliency is the goal. The reason we do security is to make business processes more resilient. The reason we care about continuity is to make business processes more resilient. The reason we need to keep the IT infrastructure available, right, is to make the business processes that rely on it more resilient," so –

Stephanie Losi: Okay, so everything is sort of coming back to the business mission?

Rich Caralli: Absolutely. We not only want to be able to react, you know, to be able to be okay when something bad happens, but we want to be able to manage that situation to the extent possible, and by the way, if something does happen, we want to be stronger because it's happened.

Stephanie Losi: And so learn from mistakes.

Rich Caralli: Exactly.

Stephanie Losi: Okay.

Rich Caralli: Exactly. I'd like to go back for a second, though, to this whole concept of how these things interplay to operational resiliency, because that is how we are giving new meaning to fields like security. For three years we sort of searched for, why do organizations even put their money in this space? Why do they give $20 million to the security people in the organization? What are they getting for it? When you link it to the fact that security is really about managing operational risk, and when you manage operational risk, you are actually managing operational resiliency, then it gives security meaning.

Stephanie Losi: Right, it sort of gives you a context as to why we are doing this.

Rich Caralli: Exactly.

Stephanie Losi: Okay.

Rich Caralli: Exactly.

Part 2: Determining How Much Is Enough

Stephanie Losi: And so how can you determine how much resilience is enough? Like, when do you know, "Okay, we have done x, y, z, we've taken the following measures, we feel that this is tied in in the following ways, and we feel that this is sufficient."

Rich Caralli: Unfortunately, that's the big research question, and it's a very challenging question. One way that an organization or at least some of the foundations an organization has to do that is, you have to look to many factors: like what business are you in, how important is it that you meet the mission, how much reserve do you have. In other words, how many mistakes can you make and it still be okay? We saw some recent things happening in the airline industry, you know —

Stephanie Losi: With JetBlue right?

Rich Caralli: Exactly. I mean, how many planes on a runway do you have to have before that becomes a major dent in your reputation and your business, and for some businesses that would've ended their business. So maybe JetBlue's a little more resilient than those other ones because it can handle that.

Stephanie Losi: That's true, and again, I think maybe it comes back to customer expectations. I mean, perhaps customers realize that, "Okay, you know, if the weather is not good maybe my flight will be delayed," so there may be some tolerance in there, although this seems to have been a bit outside the bounds of that.

Rich Caralli: Right. So setting those targets really comes back to an organization really being able to turn the mirror on itself and saying, "Okay, we know what industry we're in, we know what we want to accomplish, we know what the challenges are, we know what our risk appetite is," – a very important concept here. If you have no sense of the limits of risk – what you're willing to accept and what you're willing not to accept – you really can't get a good basis for resiliency, right, to know how much resiliency is enough. And it also sometimes depends on where you are relative to your peers.

You know, if you look at the retail industry we have some giants, right, like Wal-Mart, and you have to suspect that they can take a lot more of a hit from all sides, you know. They get a lot of reputation hits, and they get a lot of projects that they're working on that don't pan out, but they can take a lot more because they're so big and they have so much reserve. Whereas a smaller organization, retail organization, that doesn't have deep pockets and all of the experience and such that a Wal-Mart has, can't do that.

Stephanie Losi: Right, but the same disaster is much worse for them.

Rich Caralli: Exactly, exactly.

Stephanie Losi: Great, so can you maybe provide sort of a guide in terms of steps that business leaders can take to say, "Okay, we have decided that this is our risk appetite, this is our threshold, and how can we get to that level?" Is there a first step, or are there certain things that you need to do before other things?

Rich Caralli: I think it's what we're learning in the development of a framework in this area, and we'll talk about that a little more, is that an organization really has to know: what are those business processes and services that absolutely directly connect to the mission? An organization has to know the things that it does do and has to do, sort of like its critical success factors in a way, that support the mission. When it knows that, it also needs to know what assets are important to those processes. I take it almost as a cost accounting view.

You have a business process in the organization that, say, produces widgets, and that business process consumes one or more of four types of assets: people, information, technology, and facilities. Those things all need to be resilient. A disruption in any one of those things attached to a business process can bring that business process down.

So it comes down to some basic things for an organization sometimes, you know: (1) know what business you're in; (2) know what your strategic and business drivers are; (3) attach business processes and services to those drivers so that you know those are the ones that are actually pushing you toward the mission; (4) figure out which assets are associated to those business processes and services; and (5) make sure those assets are not only protected from risk, but also sustainable in case a risk is realized. I know that sounds simple, but it's a huge task if you're a really large organization.

Stephanie Losi: Oh, I can imagine, because you would have like, you know, thousands of business processes and thousands of people and different facilities all over the world.

Rich Caralli: Right. And until now, especially in the banking and finance industry, operational risk has sort of been seen as one of those things that's just a, you know, it's a byproduct of doing business. It's a necessary evil. Today the tide is changing to where regulations like the Basel Accords, for example, were saying, "No, you really have to manage this. You have to get a handle on this. This is a type of hazard risk that can affect your ability to meet your mission," and it is simply stated that way.

Stephanie Losi: How can you track progress toward a goal, and then how can you make sure that your organization is structured such that your operational resilience effort is sustained?

Rich Caralli: So this is the really important aspect of the research that we're doing. We really feel like organizations don't have the benchmark they need to know how competent they are in this space, what things they should be doing, how competent they are relative to their peers, how they can sustain any success they have in this space.

Because let's take security, for example. One of the problems with security risk assessments or security assessments in general is they're point-in-time examinations. So if I'm a practice-based organization, meaning I rely on a set of best practices to perform my security task, and I look at those best practices today and I say, "They're fairly successful," can I guarantee the success of those practices tomorrow?

Stephanie Losi: Well, no. I mean, that's what we learned from JetBlue, you know, they thought that this was a good process and now of course they'll go back and deal with that.

Rich Caralli: And they're going to learn from it, right? Can I repeat my success in the future? Can I sustain my success? So it almost is like we give organizations some sense of, some false sense of accomplishment, by saying, "You passed the examination. That means you're doing the right things." But what we're not saying to them is, are you doing them consistently, are you doing them in a way that's repeatable, and all of those things.

So the framework that we've started to imagine is that it's something that shows all of the competencies that an organization has to have, to really get its arms around managing, truly managing, operational resiliency. And when I take all those competencies and I string them together, what I get is a process definition for what we call resiliency engineering; which is simply the practice of initiating, identifying, you know, doing all the things that we're talking about in this conversation, around that operational resiliency space, and those assets and those services and those business processes. So it's a very disciplined and systematic approach that until now many organizations don't really do. I mean, it's sort of an ad-hoc thing, right.

Part 3: Resiliency Engineering: A Preview

Stephanie Losi: Okay, so can you maybe sort of talk about what some of those competencies might be?

Rich Caralli: Sure, you know, I think it would be best to start with a definition of resiliency engineering, which I'm going to read to you because it's kind of involved.

Stephanie Losi: Go ahead.

Rich Caralli: It's the process by which an organization designs, develops, implements, and manages the protection and sustainability of business-critical services, related processes, and associated assets such as people, information, technology, and facilities. So, you know, that whole sort of realm <laughs>.

Stephanie Losi: We will put that in the show notes if you want to read it.

Rich Caralli: But if I had to bring it down to one phrase, I would say it's requirements-driven security and business continuity. And what we have found in organizations is that the security people are over here working on one set of risk assumptions, and the BC/DR people working on another set of risk assumptions, and always affecting the same assets, instead of looking at the asset holistically.

I have an asset of information. It's my customer database. Lots of processes share it. What needs to be done to protect it from risk? So the traditional security side, or the management of the condition, the threat, and what needs to be done to sustain it in case a threat gets through, because we can't mitigate all risk. So when you look at the asset holistically that way, and you attach it to the business processes that matter, you are taking a structured engineering-based approach to it. This is something that organizations really don't do today.

So when I put the framework out there, and I say, "Well, there's these twenty-four or so competencies," it spans the globe really of things like defining requirements for these assets, understanding and identifying your suppliers, and knowing how they affect operational resiliency.

The whole way to something we call enterprise focus: do you know what your strategic objectives are? Do you align your risk tolerance to those objectives? Do you actively govern this resiliency engineering process? And we could do another whole podcast on governing for resiliency, because I mean somebody's watching over this now, or somebody needs to be watching over this, so that that feedback loop is created, so that we learn from our mistakes.

So, you know, it covers all of those things as well as to the very practitioner-level activities like vulnerability management, incident management, technology management, problem management. These all seem like very disparate things, but when you put them all together, they are really giving the organization a handle on managing – actively managing – operational resiliency.

Stephanie Losi: Okay, that's great. So it sounds like you're really creating kind of a repeatable process.

Rich Caralli: Sure.

Stephanie Losi: That an organization can follow.

Rich Caralli: Right, and the thing I think that we're adding to this – because we have this unique vantage point at the SEI. We have these process improvement folks who have created an entire community around process improvement in the systems and software engineering space, and then we have the CERT expertise in the security and continuity space. What we're doing in this framework is overlaying some of the process improvement concepts, so that we can get repeatability and sustainability and improvement in resiliency engineering, so that it's not a one-time activity.

Stephanie Losi: Great, and so how do you see resiliency engineering evolving in the future, going forward from this point?

Rich Caralli: I think the way we see it evolving is that through the use of the framework that we're developing – it now has, you know, not a very pretty title, the Resilience Engineering Framework – we see that as a way to give organizations maybe the first target that they've had to compare what they do versus a sort of normalized standard. Realize that we are building this actively with the banking and finance industry. They have some of the most mature practices in this area.

Stephanie Losi: Okay, so the normalized standard for that may be more than what a company in another industry would need?

Rich Caralli: Could be, exactly. And, you know, we take a lot of their lessons not only from the fact that they support the U.S. economy and perhaps the global economy, but, you know, they went through 9/11, a lot of them.

And I'll give you an interesting example of something that comes up in our discussions. Lots of companies had post – they had disaster recovery plans post-9/11. They could move their operations to another building, but they forgot about the psychological impact on the people. So they moved operations to another building in Manhattan, but nobody would work above the fourth floor. You're not very resilient if you can't get the people asset to work.

Stephanie Losi: Right.

Rich Caralli: So those sorts of considerations from this broad set of experiences that these people have had have been brought into the framework.

Stephanie Losi: Okay, and so all of this knowledge really is incorporated in this framework as sort of a composite standard?

Rich Caralli: Yes.

Stephanie Losi: Okay.

Rich Caralli: One of the nice things about what we're developing is that it's a process definition. So it is at a higher level where we believe we will start being able to get some metrics that are meaningful. For example, when we say to folks, "What are some metrics in the security field that you establish and measure?" and they say, "Well, training. We trained 135 people this year in security," and we say, "Well, that's great, but what does that mean?"

Stephanie Losi: Like, "What did you gain from that?"

Rich Caralli: Right, and maybe you should've trained 500. So we're not sure that there are meaningful metrics in this space.

Stephanie Losi: Right, are there 135 people in the company, or are there 13,000 people in the company?

Rich Caralli: Exactly. But when you go to the level of processes which can have meaningful metrics and measurement, you are taking it out of that realm at the practice level and you're moving it to the process level where it can actually be quantified, at least that's our hope, and we're starting to come up some of those. The nice thing about this is if an organization has a real affinity for ITIL, for example, we don't change the context on them. So the things they're doing using ITIL fit the process definition, or if they use COBIT, it fits the process definition, or if they're a 27001 shop, it doesn't matter what practices they use, they will all essentially fit the process definition. So they don't have to change what they already know.

Stephanie Losi: Are there other organizations working in the field? And additionally, we'll definitely link to CERT's work in our show notes. And if you have any other pointers to where our listeners can learn more about these efforts, let us know.

Rich Caralli: Sure. I would have to say right now we don't know any organization that is actively working in this field. Many of them are talking about resiliency and resiliency engineering, for example in the banking space again, organizations like BITS are talking about this. And Carnegie Mellon is a participant in the Council on Competitiveness that is really pushing resiliency as the new security, right, because it's giving meaning to that field. So a lot of folks are talking about the problem space that we've talked about today. We have seen few examples of real road maps to improvement in this space. And so we're hoping that the one that we put out soon will be the first real road map for improvement.

And I should also qualify it by saying lots of people get our framework confused with an operational risk management framework. We're really not in the space of showing organizations how to manage operational risk, although that is a very deep thread in what we're doing. We actually take it a little higher and link those risks to the business processes and to the mission, which is where it gets that operational resiliency context. So it's a little different. There's lots of models out there for managing operational risk and enterprise risk, things like COSO for example – again another thing that fits very nicely into our framework. So we've kind of bitten off a very specialized chunk of this.

We will be establishing a WIKI, the address now being www.resiliencyengineering.cert.org, and that page will be a collaborative space in this field. Parts of the framework will be out there, and we'll be soliciting comments, and it's kind of an exciting thing for us.

Stephanie Losi: Well, that is great. Thank you very much. I feel like I have learned a lot, and I hope our listeners have as well, and I thank you for being here.

Rich Caralli: Okay, thank you.