Managing Relationships with Business Partners to Achieve Operational Resiliency
Transcript

Part 1: Why Are External Relationships Increasingly Important?

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 web site.

My name is Julia Allen. I'm a senior researcher at CERT, working on operational resilience and software assurance. Today I am pleased to welcome my colleague, David White, Product Manager for CERT's Resiliency Management Model. Just for listeners' information, we have posted two introductory podcasts on this work that you might want to listen to.

Today David and I will be doing a deeper dive on one of the key areas, called process areas, within the model. Specifically, we'll be discussing how to effectively manage relationships with business partners, suppliers, and other parties that are part of the operational resiliency mission of the organization.

So welcome, David. Really glad to have you with us today.

David White: Thank you Julia.

Julia Allen: So, by way of introduction, for those of that may not be that familiar with CERT's Resiliency Management Model (we previously called this the Resiliency Engineering Framework), it would help if you could just give a few words of introduction about the model and what its purpose is?

David White: Sure. Well, the model is structured as a capability maturity model, so some people might be familiar with that form a model. So, the Resiliency Management Model is a capability maturity model. And the Resiliency Management Model is really all about providing guidance to an organization to help them establish, manage, and sustain their operational resiliency activities. So the model has a process focus. It's a process improvement model. And it's also a descriptive model, not a prescriptive model. So it's unlike a standard, which are often prescriptive in how you do things. It really just describes what an organization needs to do to accomplish - develop capability in effectively managing their operational resiliency activities.

Julia Allen: OK, so what disciplines typically show up in operational resiliency as reflected in the model? What gets brought together when you think about operational resilience?

David White: Well, we take a particular perspective on operational resiliency in the model. And it's really, we take an operational risk management perspective. So the kind of activities that an organization needs to undertake to effectively manage its operational risk vary, really based on the risk environment that the organization operates in but almost always includes three fundamental activities, which are security, business continuity, and IT operations. And so in the model, we use those three activities really as the lens through which we look at this issues of operational resiliency.

Copyright 2009 by Carnegie Mellon University

Julia Allen: Right. And typically I know in a lot of organizations that I've worked with and observed, those tend to be stove-piped. And so is it - am I correct in saying that one of the benefits of the model is trying to bring these three disciplines together?

David White: Absolutely because they - you really - there are - there are a lot of touch points between the three and to optimize any one really often affects the other two. So looking at them in a converged manner is a really valuable way to view those activities in any organization.

Julia Allen: OK, so, let's turn our attention to our topic for today, which is our relationships with all these business partners, suppliers, vendors, contractors, other parties. Based on your observation, your work with customers, what do you see as to why relationships such as these are becoming more and more important?

David White: Well, in business today, we've really developed a complex web of relationships that allow us to make good use of - or engage special skills from - other organizations that we don't necessarily have in our own organization or to engage special equipment or systems or data. There are all kinds of relationships that organizations developing today, both with vendors and in some cases with customers, where the technology interfaces are so elaborate and so rich that sometimes the organizational boundaries get a little bit blurred. So as organizations find that they are increasingly dependent on a larger and larger number of external party services or products or activities, then there are a lot of these (as we call them in the model, "external dependencies") that have to be managed in order to address the organization's operational resiliency.

Julia Allen: Right. And it seems to me that that's also compatible with the increase of outsourcing, global supply chain, acquisitions of various types, partnerships that are formed for a specific purpose and then disappear - those are all kinds of examples, right?

David White: Exactly.

Part 2: Set Priorities; Manage Risks

Julia Allen: So as we talk about managing operational resiliency and we take into account this complicating aspect of all these external relationships, what are - from the model's point of view - what are some of the top-level goals described in the model for managing these types of relationships?

David White: There are four high-level goals in the external dependencies process area that address the kinds of things an organization should do to manage these dependencies. So, let me just go through them one by one.

The first goal is to identify the external dependencies and to prioritize them, so that's a compound goal. But you really need to understand what your external dependencies are before you can manage them. So, that makes sense. The second goal is to manage risks associated with the external dependencies. And the third goal is to establish formal binding relationships with those external - the external parties that are - that form the dependencies. And the fourth goal is to manage the performance of the external party.

Julia Allen: OK. So, now that you've introduced each of those, I'd like to take them in turn and we can drill down and discuss them in a little bit more detail. So, when I think about – we discussed it briefly - all the various ways in which you can have these kinds of relationships, clearly some relationships are more important than others. So we have to invest in maybe greater attention, greater oversight, more resources, more stringent performance measures. So what are some ways

Copyright 2009 by Carnegie Mellon University

to pick and choose, to characterize and prioritize all the relationships with whom an organization does business?

David White: Well, that's a really good question because there are - even a midsize organization might have tens of thousands of these external relationships to prioritize, and you certainly don't want to bring the same level of attention to all of them. So one of the things that a lot of organizations do that I - let me start with something that I don't think is the best idea, OK?

Julia Allen: OK.

David White: OK. A lot of organizations are prioritizing these relationships based on cost, just based on simple dollar figure numbers around the relationship.

Julia Allen: So, you're saying the the ones that you spend the most money on are the highest priority.

David White: Right, right. And my favorite example of why not to do that is that a friend of mine works for a midsize company and he was involved in revamping their vendor management process. Turns out that their largest vendor, so the vendor that was - then they were largest by a substantial margin - was the company that provides paper products for all of the bathrooms in their facilities around the country because they have one contract for paper products. Well, clearly, if all of a sudden they run out of paper towels in the bathroom, I mean it's a problem and you have to deal with that, but managing that relationship is not quite the same as managing the key back office service provider that's doing - that's doing a lot of outsourced work related to the core business of the organization, right? So if they - and they had been prioritizing everything based on cost, so this paper products vendor was getting a great deal of attention and some other vendors that were providing services in support of mainline business processes were not getting nearly enough attention. So the first thing is you might want to - don't just prioritize based on cost. That's probably not the best approach.

Now in the Resiliency Management Model, we often talk about something that we call high-value services, which are just the critical services of the organization. The services or functions of the organization that if they stopped running would really diminish the organization's ability to achieve its mission. So one of the ways to prioritize your external dependencies is to understand the relationship between an external dependency and the provision of these or the operation of the organization's key or high-value services. So that's one of the ways that's a really good way to prioritize them. I also think from a structural perspective, most organizations will find that it's helpful to prioritize them in tiers. So you might have all of the external dependencies that achieve some threshold go into the top tier, and then you have several tiers under that so that you can cluster them and start thinking about how to manage them as a small set of tiers as opposed to a big set of thousands of external parties. So does that make sense?

Julia Allen: Well, that makes sense because here we are - we're talking about operational resilience and we're talking about high-value or critical services that are essential to the mission. So it seems that, as you're saying, that prioritizing based on how important it is – the mainstream support that the provider gives to mission success should be kind of paramount, right?

David White: It is paramount. And one thing to keep in mind as you do that is that the extent to which you might depend on that external party might change based on the situation that you're in, OK?

Copyright 2009 by Carnegie Mellon University

So, for example, in day-to-day sort of unstressed operation, then the external parties that appear to be most important might be people who are providing outsourced business services or they might be running some financial operation for you or something like that. But if the organization is under great stress, then all of a sudden, you might find that the people that you're most dependent on are those that are providing backup services or that provide failover data center support or other things like that. So it's important to keep in mind the various phases or modes of operation for the organization as you consider that prioritization.

Julia Allen: That's actually an excellent point that - yes, I hadn't considered before, which is day-to-day is one thing, but if there's a natural disaster, if there's a major business outage, if there's some other kind of market factor that significantly impacts what I need from a particular partner, then in that scenario, that becomes much more important, right?

David White: Right, exactly.

Julia Allen: So with respect to the second goal about managing risks, what are some of the issues that the model recommends need to be considered when an organization is looking at the risks that could arise when you're contracting with an outside party?

David White: Well, the one I'm going to start by just pointing out something that's very timely, which is financial condition. So financial condition is a characteristic of an external party that can have an enormous impact on their ability to provide you the services that you're counting on. And given the current economic climate, that's something that organizations should be paying acute attention to - risks associated with financial condition of external parties. Some of the other risks that we suggest that organizations pay attention to are risks to the availability of key personnel. So you might be hiring an external party because they've got this really fantastically smart or skilled workforce, but if that workforce changes, that's a risk that you should be attending to. You also should pay attention to the extent to which that external party might be dependent on third parties of their own, right? So if they're outsourcing any part of the business that they're providing to - or any of the service that they're providing to you, then their reliance on subcontractors is a risk that you inherit. So any risks associated with their management of those subcontractors are important for you to pay attention to. So those are just a couple of examples of risks that are important to manage. Oh, let me mention one more.

Julia Allen: OK.

David White: So another thing - so in an ideal world, we would all have the luxury of choosing these external parties from a set of completely capable external parties that could meet all of our requirements and we would simply go in and choose the very best, right? That would be ideal.

Julia Allen: Right. But obviously that never happens, right?

David White: Exactly. So there are always compromises when you're selecting an external party. So you ideally have developed a set of requirements and then you go out and you're selecting parties based on that set of requirements. The party that you ultimately select might not be able to meet all of your requirements, so unmet resiliency requirements are a key source of risk. And so you should treat any requirements that can't be met by the supplier you end up with as risks in managing the relationship with that supplier.

Julia Allen: Excellent, excellent. Those are all really good things that I wouldn't ordinarily think of, so thank you for those examples.

Copyright 2009 by Carnegie Mellon University

Part 3: Build Robust Contracts; Manage Partner Performance; Use a Process Approach

Julia Allen: So with respect to the third goal, and this may get into some of the residual risks that you just identified that you need to attend to, what are some of the key ideas or key practices for ensuring that resiliency requirements are reflected in contracts and service level agreements that you enter into with outside parties?

David White: I guess my first recommendation there would be to really understand the requirements. And in the model, we recommend kind of a two-pronged approach to establishing the requirements for a relationship. And the first prong is to understand what kind of blanket requirements you might have. So examples of that are you might have certain compliance requirements because of the business that you're operating in or you might have requirements for background checks on any of your employees that have access to certain types of data in your operation. So those requirements are blanket requirements that it may be appropriate to apply to any external party, right? So that's the first branch of understanding the requirements. The second prong is to understand the resiliency requirements that are specific to that external party. And to do that, you really have to understand exactly how dependent you are on the service or whatever they happen to be providing to you in support of your business. And that's where a lot of the - what are typically called service level agreement requirements come from, like how far could they - or how quickly could they get back up and running in the event that they had an issue of a certain type; like they had a power outage or they had another kind of disruption in their business, how quickly are they able to restore their business in order to continue satisfying the obligations that they have to you?

So those are examples of two takes on requirements. And then once you understand those requirements, you really want them to be documented in the contract agreement. And in a lot of organizations, in today that I'm finding anyway, that in a lot of organizations today, that might take some training of your acquisition organization or your contracts organization, whoever is responsible in your company for contracts. Because a lot of times, people who write contracts for organizations, they don't want to put more material in those contracts. But if your business is really dependent on this external party being able to perform, then those performance requirements really need to be written into the agreement along with what kind of abilities you have under the contract to correct their performance under certain scenarios. So did that answer your question?

Julia Allen: Yes, it did. And it kind of ties back to the first goal where we talked about identifying and prioritizing external dependencies or the parties that you depend on, and that is, it seems to me that when you're writing contracts, when your service level agreements - you mentioned sometimes the contract staff either isn't knowledgeable or doesn't want to go through the extra effort - so it seems to me you could also use that identification, prioritization criteria to determine how much energy, how comprehensive to make a particular contract based on the criticality of the service. Is that right?

David White: Absolutely. If I'm buying printer toner, it's very different than if I'm buying outsourced data center management, right? So ...

Julia Allen: Right, right.

David White: ... the higher tiers should get more attention in the contracting process than the lower tiers in terms of your prioritization.

Julia Allen: OK. So as we come to our close, let's talk about managing performance. You talked a little bit about this in crafting the contract and certainly that's the place to start. But how as a

Copyright 2009 by Carnegie Mellon University

business leader in the organizations that you've worked with, how do you find that they're able to ensure that their suppliers are performing as expected and when it's time to step in maybe and take some remedial action?

David White: So the number 1 recommendation I would make relative to how to make sure that the suppliers are performing as expected is to establish a standard procedure and make somebody responsible. And this too, is something that might vary base on your prioritization scheme because you might have different monitoring processes. So you have to monitor the performance of the external party in order to make sure that they're meeting the requirements, right? And so you might have different processes and different frequencies based on the prioritization you established back in the first goal we talked about. So establish a process or a procedure and make somebody responsible. And the person you make responsible might be the same person you make responsible - or the internal business owner of that relationship might be the right person to make responsible. So you have to monitor. And then when you monitor, you have to correct things that you find that are not meeting your requirements. And monitoring might take the form of inspecting deliverables if they're providing you with some deliverable artifact or like a software product or a data product, for example. But oftentimes when service is the deliverable, those inspections are harder to make. So you may have to consider testing, so you might test various scenarios in the service level agreement to make sure that the supplier can achieve what they signed up to achieve. But I guess the bottom line is establish a procedure and follow the procedure and make somebody responsible for it.

Julia Allen: What have you - in this particular arena, David, what have you found to be the role of things like assessments or audits or either self-assessments or maybe independent assessments or audits? Do you find those are useful in an ongoing relationship or are they really only useful as part of your due diligence before you enter into the relationship.

David White: Well, I'm glad you mentioned that because they can be very valuable in monitoring the highest tier of your external parties, the ones that are most important. So ongoing or regular audits should be a part of your monitoring process for really critical suppliers, as well as part of the due diligence process you go through when you're selecting them or establishing a contract with them in the first place. I think a lot of organizations are starting to imagine that maybe there's a way for organizations to provide one another with sufficient transparencies that those audits are no longer necessary. But in today's environments with the tools that we have right now, that's a really good practice.

Julia Allen: Great, great. Thank you. So you mentioned at the beginning of our conversation that the Resiliency Management Model is a maturity model, is a process model. So particularly when it comes to managing your external relationships, what have you observed are the advantages of having a defined process or some type of a process model versus a checklist or something more ad hoc? What do you see to be the benefits because clearly, investing in putting that kind of process in place takes time and money?

David White: It does take time and money. And I think the biggest value of taking a process approach is that the focus of improving the processes that are described in the Resiliency Management Model is really about institutionalizing those processes. Now what does that mean? Well institutionalizing them simply means that you build them into the way the organization does business so that the organization can count on those processes running, even in times of stress, right? And that's really what institutionalizing these processes really mean. And these processes are – the processes like the one we've been talking about today relative to managing these external dependencies - these are the processes that you're counting on being in place to make sure that all of the value-producing or mission-focused business processes of the organization continue to

Copyright 2009 by Carnegie Mellon University

operate. So to do the best job that we can to make sure that the organization stays in business and continues to achieve its mission, we have to attend to what we call resiliency processes which are all about keeping the business processes running.

Julia Allen: Yes, and I keep coming back to your tag line about “in times of stress.” So you can probably get away with something simpler, maybe more check-listy in nature if things are running smoothly, but the real test is when you're under attack, under an Internet-based security attack, when you're dealing with some type of a natural disaster or a disruption in continuity, when a big part of your network goes down, those are the times where, as you said, having these processes in place are - that's really when you call upon them to perform, right?

David White: Absolutely, absolutely.

Julia Allen: OK. Well listen David, do you have some places that you'd recommend where our listeners can learn more about what we've been discussing today?

David White: Well, as you can probably guess, I'm a big fan of the Resiliency Management Model so I would definitely consult our model and I'm sure you can provide the listeners with a place to access that. I also found relative to managing external dependencies, there's a publication by the Federal Financial Institutions Examination Council, also called FFIEC. And the FFIEC Handbook for Outsourcing Technologies is a great resource for managing the kind of relationships that we're talking about today.

Julia Allen: Well I thank you, David, so much for your time, expertise, for a great introduction to a very complex and difficult subject, and I look forward to another conversation.

David White: Thank you Julia.

Copyright 2009 by Carnegie Mellon University