Resiliency Engineering: Integrating Security, IT Operations, and Business Continuity Transcript

Part 1: The Resiliency Engineering Model

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 introduce Lisa Young, a senior member of CERT's Resiliency Engineering Team. We'll be continuing the conversation we started with Rich Caralli on how to tackle security from the perspective of operational resilience. So, Lisa, welcome. Great to have you here today.

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

Julia Allen: So, in the reading that I've done and in your research, you advise business leaders to take an engineering approach to security based on operational resilience. So I have kind of a three-parter for you, and I'll help if we forget parts.

Lisa Young: Okay.

Julia Allen: So what does this mean, an engineering approach to security based on operational resilience, what does this mean, how does it differ from traditional approaches, and why is it important?

Lisa Young: Well, I think today the problem with security management is that it's often seen as a technical problem, it's usually bolted on as an afterthought, and it has poorly defined and measured goals.

An engineering approach provides a way to align all of the different aspects of your business, so for instance, security, business continuity, IT operations. An engineering approach provides a way to align the activities so that they help the organization meet its strategic objectives, and it also gives a level of control over the outcome. Really what we're talking about is trying to take a proactive approach, a more proactive approach, and a more strategic approach, to security, business continuity and IT operations, and elevate those to the enterprise level.

Julia Allen: So maybe an analogy would help here. Can you give me an example of how an engineering approach would work in other fields, and maybe we can make some connections here?

Lisa Young: Yes, engineering – for instance, if you want to build a bridge, one of the things that has to happen is it's a coordination of many different skill sets. You have the requirements, you have the funding, you have all of the disparate skills, and it's a multi-disciplinary approach to achieving the objective of building a bridge.

And what we see is that organizational resiliency or managing this operational resiliency and operational risk needs the same disciplined and systematic approach. The organization has to

perform these security, business continuity tasks under the constraints of changing requirements, limited funding, regulatory demands, accounting and budgeting rules. So disparate parts of the organization have to coordinate their work in order to achieve security for the enterprise. And what this means is that the enterprise has the ability to sustain itself in the event of disruption or some other event that's out of their control.

Julia Allen: So if I take your bridge analogy a little bit further, you've got all kinds of roles, all kinds of perspectives, you both decompose and compartmentalize the different disciplines that have to be brought together, but then you have this integrating function that the general contractor performs or that someone performs – I'm not an expert on building bridges – to tie all the pieces together, to make sure that it happens as designed, and most importantly that every time a vehicle goes across the bridge that the bridge stays standing.

Lisa Young: Yes.

Julia Allen: So, can you tie that together a little bit for us with operational resilience and security, because clearly resilience has to do with continuity – that might be equivalent to the bridge remaining standing – but is that what you're saying, is you have to just bring all these disciplines together in a holistic way?

Lisa Young: Absolutely, and I think it's really important because security contributes to the organizational resiliency, because it's about confidentiality, availability, and integrity of organizational assets. And an organization cannot be resilient without security, and to be effective security must be built into the fabric of the organization, so it requires that security-related processes are engineered in the context of the organization's requirements. And it also requires that security be owned and that the culture of the organization is aware of the risks.

Julia Allen: Okay, so you started talking about assets a little bit. So how are business services, business processes, other types of organizational assets, how are they addressed by operational resilience, and what are some of the main ones that operational resilience targets or focuses on?

Lisa Young: Well, we take a services view of operational resiliency, and what that means is that each organization has key services that it performs, who it is and what it does. So, for instance, in the banking environment a key service might be retail banking or investment banking or some other line of business. So we feel that taking a service approach – and service could mean product, but a service approach – has you look at the organization from a top-down risk perspective. And what that means is those services are supported by business processes, and any organization can have hundreds or even thousands of business processes that support services. And underlying those business processes are assets, and typically right now security is focused at the asset level, and making assets resilient.

And what we say is that if we take a service approach, so in order for the service to be resilient the business processes have to be resilient. In order for the business processes to be resilient the services and assets have to be resilient. So each of these assets, and we classify them as people, information, technology, and facilities, contributes and creates business processes, which helps the organization meet its goal of what it does for a living.

Julia Allen: So, would it be fair to say that I have a mission, that as an organization I'm trying to perform, or I have critical success factors that are key to my success. Then would it be fair to say that the assets, the services, the processes, the information, the people, the facilities, all have a role to play in ensuring mission success or in ensuring I meet my critical success factors? Is that what I hear you saying?

Lisa Young: Right, so just to give you an example [of] what we mean by this, to keep a credit card operation running you might have hundreds of thousands of business processes. One of those processes might be receiving credit card payments. For many banks, this process might be something that they outsource to another vendor. And what we're advocating is that if you take a service view, if you look at the services and where all of the business processes and the actions take place and elevate that to an enterprise level, you start to look at it with an operational risk perspective in mind. So you can imagine that if the database where the credit card information or the customer information lives, if that becomes unavailable, that service, those business processes can't be executed and that service becomes unavailable.

Part 2: Applying the Model to Operations

Julia Allen: Let's take a little example and, if you could, identify the assets and identify maybe where an impact would be to operational risk or operational resilience. Something bad happens.

And then if you had a resiliency approach in mind or a framework in mind, how that might help mitigate the bad thing happening, how the organization might behave or respond differently if it had that framework in place.

Lisa Young: Okay, well, one of the things that we say is that assets have a protection component and a sustainability component. And the protections are generally things that you would put in place, and they could be internal controls, they could be a variety of things, but they're a protection mechanism that you put in place. The sustainability factor is what it is that you would put in place to sustain it in the event of a disruption or a bad event.

Julia Allen: So something bad happens and then these either countermeasures or controls would help you mitigate against the impact?

Lisa Young: Correct.

Julia Allen: Okay, so how about, why don't we work through a little example here?

Lisa Young: Okay.

Julia Allen: Do you have one in mind?

Lisa Young: Well, like you mean like a customer database, or?

Julia Allen: Yeah, like the customer database – everything's running along fine, you've got your baseline protection strategies in place, and then either a disgruntled employee, an insider ends up compromising part of that, or some kind of an attack occurs where part of that data is compromised or breached. If you had operational resiliency as your mode of operation in the organization, what might happen in the face of that breach or compromise?

Lisa Young: Well, I think one of the things that we advocate is taking an enterprise-level view, and what that means is coordinating all of your resources. So things that are in place for protection would be coordinated with things in place for sustainability. So in the event that there was some sort of impact to your business, I think what resiliency engineering is, it's not so much an operational approach. What it is is it's a way of looking at things so that you optimize the protection and the sustainability at the right cost of protecting the assets, okay? Because all assets are not created equal, and some are more important to the mission of the organization than others, and in

order for a business leader to know what those are, he or she has to understand what the underlying assets are that support the services and business processes, and apply the appropriate preventative measures and the appropriate sustainability measures in the context of what that asset means to the business.

Julia Allen: Okay, so what I hear you saying is those that are more critical, those that are more essential –

Lisa Young: Yes.

Julia Allen: – for business success will clearly have a higher level of investment.

Lisa Young: Yes.

Julia Allen: In terms of controls and protection strategies and sustainability.

Lisa Young: And the purpose of having resiliency engineering is to help you determine what those are. Because right now what happens is we see a deficient funding model. So we see that compliance is funded, but how do you know how much to fund for security, okay, how do you know how much to fund? And oftentimes the funding model, what drives this is out of balance with the value of the assets and the value of what it means to the organization.

So having a resiliency engineering approach means that you look at the assets in the context of what it is that they do for you – how do they deliver services, what it is that they do – and then you decide as a business leader how much money to spend, or how much resource to spend on protecting them versus sustaining them. But you do that – our goal is that if you implement the resiliency engineering, what you're doing is you're looking at the processes and you're taking a way to measure, a way to improve, a way to achieve your goals and objectives, and as a side benefit we're also looking at being able to sustain compliance with things that you're already doing.

Because many executives now are trying to derive value from sustainable compliance. They spend a lot of money on compliance, but they're not getting any other business value out of those. So how do you take an approach to have your organization be more secure, have it have the ability to continue operations in the face of many different changing risks, and then –

Julia Allen: Meet your compliance requirements at the same time.

Lisa Young: Absolutely, as a by-product.

Julia Allen: Right, yeah, so what I hear you saying is in the normal course of business, if I'm doing, let's say, business continuity correctly, and if I'm doing security correctly, and if I'm putting my investments into my high-priority services and the processes and assets that support those services, then I should get compliance as a result, if I've kind of, particularly if I've thought about that all in advance.

Lisa Young: Yes, absolutely, and also the funding model, you're not funding based on a reactionary scenario, right? You're actually trying to get a proactive approach to improving the way you manage security, right? So it's about security management, business continuity management, ahead of time, okay, not after the fact and not funding security because you had an incident of some sort.

Julia Allen: Yes, which we've all I think observed and heard enough about trying to get in front of this problem, and the things that you do proactively in advance of an occurrence end up costing you a lot less than trying to deal with it after the fact.

Lisa Young: Absolutely.

Part 3: Resiliency and Risk

Julia Allen: Okay, so let's turn our attention just a little bit, if you will, to resiliency engineering and risk management. You've talked about the aspect of trying to tie this together or have this be driven from an operational risk management perspective, but how do those two ideas tie together, resiliency engineering and risk management?

Lisa Young: Well, I think executives have a whole arsenal of tools that helps them manage credit risk, finance risk, market risk, a lot of other risk factors. What's missing is the ability to manage operational risk. Now, the resiliency engineering framework is not an operational risk management model, but what it does do is it bites off a huge chunk: the chunk of security, the chunk of business continuity, the chunk of IT operations. So it says, “These are operational risks. This is where a tremendous amount of your risk occurs day in and day out no matter what your business. And if you can get your arms around managing the risk of this environment it goes a long way towards managing your overall enterprise risk.”

Julia Allen: So this would be a contribution, taking a resiliency engineering approach would be a significant contribution to your overall risk management strategy?

Lisa Young: Absolutely yes, very much so.

Julia Allen: But there would still be clearly more to do. It doesn't do everything, right?

Lisa Young: It does not do everything, yes.

Julia Allen: Okay, so let's try and make this a little more tangible for our listeners, and I know that this is a research and development activity and you're in the early stages. But what would or what might resiliency engineering look like in practice? And how would a business leader know if they're on the right path?

Lisa Young: Well, that's a good question, and what it means is that an organization has smooth-running processes with regard to security, business continuity. But what that really means in a tangible sense is that you are working on preventing outages, preventing breaches, preventing data loss and other disruptions from happening.

Conversely, it also improves your capability to respond in the event that these things do occur, so you enhance your capabilities for managing the impact. And so really what we're talking about here is active management and control, to keep your services, business processes, and assets up and operational.

Julia Allen: Well, we all know, from a security perspective, that return on investment or cost-benefit analysis is a tough proposition, and this seems to fall into that same category. So it sounds like you're talking about cost and loss avoidance perhaps. Is that what you mean?

Lisa Young: Well, certainly by getting a handle on security, the collaboration between security and business continuity will optimize the amount of resources that you spend on protection of assets,

but also in the amount of controls, right? Controls are generally what's tested for compliance purposes. So if you can have more effective controls, right, but lower number of controls, then you also have cost avoidance from reducing the amount of controls that you have to test for compliance.

Julia Allen: Well, that makes sense, that makes sense, because if I can actually combine some of these traditionally stove-piped efforts – security, business continuity, IT operations – and I can develop from a resilience approach a control framework or a control strategy, that allows me to eliminate some of the redundancy or maybe get dual use out of some of my controls?

Lisa Young: Yes, absolutely.

Julia Allen: You're saying there can be some savings there?

Lisa Young: Quite a bit of savings, yes, absolutely.

Julia Allen: Are you able to say anything bout the work that you have been doing with FSTC and why they believe that this is a promising direction to go?

Lisa Young: The FSTC is [the] Financial Services Technology Consortium, and it's some of the largest banks in the country. And we've been working with them for the past two years building this framework. Originally, they came to us and asked for a maturity model for business continuity, because they wanted to be able to benchmark their suppliers.

Julia Allen: Okay.

Lisa Young: And through the work that we were doing with them, we discovered that you can't just look at business continuity unless you look at security, and you can't just look at security unless you look at IT ops and business continuity, because all of the bodies of work that are out there overlap one another. And so eventually what we'd like to do is we're working on an assessment methodology right now, to be able to benchmark suppliers.

So, therefore, if you're an executive and you want to outsource some of your functions to a third-party supplier, you know you have an objective benchmark to say you know how to handle security, you know how to handle business continuity, and that gives you some comfort, because you can outsource the service but you can't outsource the –

Julia Allen: The risk.

Lisa Young: The risk, or the liability.

Julia Allen: Right, right, because it still comes back to whoever owns the fundamental business service.

Lisa Young: Right.

Julia Allen: Great. Well, I really appreciate your time and your perspective on this important topic, and I'm looking forward to your development activities so that we can start to let people know when they can actually roll up their sleeves and get to work.

Lisa Young: Thank you very much.