Title: Global Value Chain – An Expanded View of the ICT Supply Chain
Transcript

Part 1: Eight Stages, Threats and Exposures, Eleven Security Domains

Lisa Young: Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT Division 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.

I'm Lisa Young. I'm a member of CERT's Cyber Risk and Resilience Management team. I am pleased to welcome Edna Conway, Chief Security Officer, Global Value Chain at Cisco Systems, and my colleague, John Haller, a member of CERT's Cyber Assurance team. So welcome to the podcast series, Edna.

Edna Conway: Great to be here.

Lisa Young: Thank you so much. And welcome to you too, John.

John Haller: Thanks, Lisa. Appreciate it.

Lisa Young: All right. So I'm so happy that you guys could be with me today. Edna, I saw you earlier this year speak at RSA on the Global Value Chain. Can you tell our listeners, what do you see as the value chain?

Edna Conway: Yeah. It's a great question, Lisa, because so many people are a little bit confused by the term. And what we really intend to do is to set the stage for something that's bigger than just supply chain. So the value chain really is that end-to-end lifecycle for anything that delivers value, whether that anything is a tangible product, whether it's intangible, electronic software, or whether it's something like a service offering, even, shall we say, a cloud service offering.

Lisa Young: Oh, that's good, okay, alright. So then can you talk about some of the activities that take place in the value chain?

Edna Conway: I think what we're trying to do is embrace that end-to- end lifecycle, so let's just think about it for a minute. Obviously, every industry is going to have a little bit of variability in the particular stages or nodes of the value chain for them. But let me respond to you by walking through what the value chain is for an information communications technology company such as Cisco.

So for us, we really see a number of what we call stages. And it starts really with that first spark of an idea, whether it's an idea for a new feature set in something that exists, or a totally new innovation. And we call that the design and develop stage.

The next stage that we really want to embrace when we think about value chain and before we even drive security across it and understand it is the plan stage. And what I really mean by that is begin to question, "Gee, who's going to use this? How are they going to want to use it? How are they going to want to receive it? How might we deliver it?"

The next node or stage is the source stage, and that really forces us to think about the activity of what is the third-party ecosystem for us in that value chain, which ironically enough is its own ecosystem, but who else are we going to use? Are there code providers who are going to give us modules of code if they're open source? Are we using platforms for cloud service providers upon which we're going to build an offering? Are there traditional hardware components like an ASIC (application specific integrated circuit)? Or a field programmable gate array, or a printed circuit board that are going to comprise a part?

Then we move to make node. And the make node is where fabrication in whatever form happens. And then we move to quality, where we really look at something that we think is ready to go out to the end customer and say, “Is it ready?” Let's check.” We then move on to the delivery node. How are we going to get that to the customer? In what manner?

The sustained stage or node is one where we ask ourselves, how are customers going to use it? How are we going to expand it for them, upgrade it and service it when necessary? And then finally, the last activity in this vast array of the value chain is end of life management. How we going to shut down the capability or dispose of the product, if it's tangible?

Lisa Young: So that's quite a thought process then, all the way from design, develop, all the way to the end of the lifecycle for both tangible and intangible services, products. So then are there any overarching or prevalent threats that business leaders should be concerned about in their value chain?

Edna Conway: Absolutely. Again, from the lens of the information and communications technology industry. But I think these, in all honesty, apply across the board. So we really see some foundational threats and exposure areas. So the foundational threats are really manipulation. Is somebody utilizing the product solution -- imagine, for example, the network -- in a manner that was other than intended by the operator or owner of that network?

Espionage is a threat, whether that's industrial or nation-state. And then disruption. Is there going to be a full denial of service or disruption in the service? And in order to really understand those threats, I think you need to understand a little bit about exposures. You asked about that too.

Lisa Young: Yes, I did. So what exposures arise from some of these common threats?

Edna Conway: We try to make it meaningful because, I mean, look. We can all understand manipulation and espionage and disruption. Those are big, hairy threats. Where they manifest themselves practically, what you can get your arms around to address, are taint -- so somebody actually altering in some way the solution in a manner that you didn't intend.

Counterfeit -- it's just plain old- fashioned not genuine or authentic. And then finally, the next exposure area is intellectual property (IP) misuse. So it's unauthorized access to IP, which can allow a whole host of ramifications, and certainly information security breaches are an example of a way in which folks can get access to IP that was never intended to be disclosed.

Lisa Young: So those are some pretty hairy threats, as you talked about. The taint, counterfeit, and intellectual property misuse. So then thinking about the value chain, I'll ask Edna first, you, and then John. When it comes to making decisions about expenditures for the value chain, improving traditional Information security practices or focusing on integrity areas, how would you recommend that organizations might evaluate some of these common threats or concerns?

Edna Conway: I think you need to do what we all do, right, which is take a risk-based approach. There's a funny concept that sometimes doing everything makes things better, and certainly in the security arena we're trying to build security in, not bolt it on and address these threats and exposures. But the reality is, you don't need to do everything everywhere. That may not effectively move the needle any more than doing the right security in the right place at the right time in the right way across that value chain.

For us, what we did is we came up with a value chain security architecture. And we identified 11 big categories that we call domains. So gives you a way to use a checklist and say, "Here. I'm in Oregon, and I'm trying to address this. Let's think about whether we have coverage ourselves, and with this third-party ecosystem in certain key areas." Coverage can mean a set of requirements, can mean a discussion, can mean a formal policy. And those 11 areas are pretty, pretty much things that we all think about ion a regular basis.

So first the people piece, personnel security. What are we doing with our own, right? The carbon-based units are frequently the ticket to success and security, and often we are also the problem. Third- party partner security -- understanding that your value chain partners actually have a supply chain of their own and understanding who they're utilizing or at least understanding that they know what you're worried about and they're passing that worry on.

Security engineering and architecture to the extent it's relevant to you. If you're an OEM, for example, this happens with all of us if you're a software company. Physical and environmental security -- we often forget about it. The jargon right now is all about cyber all the time, 24 by 7, and it's critical. But physical and environmental security are a foundational part of that. You don't understand where your data center is and what equipment is there, you have a problem.

Security and logistics, right, logistics and storage. Again, some of the tangible elements and some intangible -- storage of data. Where is it being housed? Who's controlling it? Asset management goes along with that. And then really understanding security incident management. We, for example, like many of our brethren in the industry, have a CSIRT and PSIRT alert, (Product Security Incident Response Team), that sends out notices about products and solutions of Cisco. Do the people on your value chain have that? How are you going to get access to that information? How swiftly you learn about incidents that may have occurred in your value chain partners' environment that impact you.

And the last three are security in manufacturing and operations to the extent it's relevant to you. And remember, operations can include development. Security and service management -- so many of us forget the service element. Are you repairing something? Are you upgrading something? And then finally, information protection. And overarching all of it is some form of security governance. And that can be if you're a small or medium business, something as simple as, "Are your senior leaders aware of it?" and embedding it into their activities. And something as sophisticated as Cisco's value chain security architecture, which has about 184 requirements built into those 11 domains that we just talked about.

Lisa Young: So the value chain security architecture. I like the structure. And definitely those requirements then, that's how you get the security and that's how you build the security in at the very beginning of every stage.

Edna Conway: Exactly. I think you just have to identify the risks that are the right risks in each one of those domains. Prioritize, quite frankly, the ones that are just critical and you have to address. And say, "I'm going to set my expectations for myself and for my community in that value chain, and here's what we're going to go after together," right? So you could, for example, look at any area of your key competitors and say, "Huh. If I have members of my value chain who are also performing services or delivering products to me and my key competitors, maybe I want to focus on that as a high priority."

That would probably lead you inevitably to establish some expectations with those third-party ecosystem partners about how they segregate things -- segregate information, maybe even segregate people. Do you want the same key engineers working on your material as are working on a key competitor's? Perhaps not.

Lisa Young: Sure. And that makes sense, because it really is, I mean, in so many ways, an interdependent and connected ecosystem. So I appreciate that regarding segregation -- people, operations, technology. So thank you for explaining that.

Part 2: Critical Infrastructure Considerations; Key Practices

Lisa Young: Alright, so backing up just one second -- John, I'll ask you a question as well. Can you say more or anything about the SEI's take on the value chain and risk-based approach to protection and then sustainment?

John Haller: Sure, Lisa. So just to lay the stage, the team that I'm on, the Cyber Assurance Team, we're very involved in assessing how critical infrastructure organizations in the United States handle this problem as part of work that we do for the Department of Homeland Security. And we look at third-party risks where the value chain goes from the perspective of information and communications technology that an organization would buy and implement or deploy internally, but also those service relationships and third-party risks, right?

The relationship -- Edna mentioned cloud services or business partner relationships, even relationships where maybe your organization, you're not explicitly contracting to have data processed or transported or stored, but in most cases any time your organization contracts with an outside party, you're probably contracting for something that's supported by information and communications technology.

These are broadly external dependencies, right? And I think to dovetail and amplify what Edna said we really look at understanding the need for an organization to understand how technology supports their operations -- specifically how third parties support their operations. And for that, I mean, that process of developing requirements and having those requirements go through technology and through your service relationships is really important.

And it's something that should not necessarily always be top-down. As an example, certain defense, the Defense Department and a lot of defense organizations right now are very, very concerned about the intellectual property angle, the possibility that in my value chain there might be an information security breach of important information that maybe I shared.

However, in many cases, things like service availability and other concerns may be really important. So we would urge organizations to empower the leaders that really understand those relationships and really understand the business or the mission function and how technology supports it to be really driving what the requirement actually is for the technology and for the third- party relationships.

And I think one of the things that's -- you asked a question about, "Well, how do you make this balance between information security practices and the integrity of stuff that you buy or deploy what's in your organization?" And I would argue that they're really linked, right? They definitely should not be thought of as a silo. And I'll give you an example. A lot of the work that we do involves assessing critical infrastructure organizations like the electric company, the water company -- things that people rely on in their everyday lives for how they deal with some of these issues.

And in many cases organizations don't have the luxury or may not have the luxury of buying technology from companies like Cisco that already have extremely mature practices in place. I mean, we've been in situations where we've talked to, for example, a critical infrastructure provider in smaller areas, where because certain pieces of SCADA (supervisory control and data acquisition) equipment, for example, may not be supported anymore or may not be available anymore.

There are cases where they have no choice but to literally go out on eBay, for example, and buy equipment, right? Because they have to continue the mission, they have to continue providing services. Well, if you're in a situation like that in a small organization, how do you manage that risk? I mean, really you have to think about what are the linkages to the other cybersecurity things or activities I would do in my organization, right?

Like, maybe my CERT, my CSIRT or my incident management folks, rather than have a more vanilla incident management plan, they really have to understand what the potential risks or even the types of activity you would see on a network are in some of those networks to be sensitive to that type of risk. So I would argue that they're really linked activities and should be thought of as in terms of the whole package of cybersecurity in an organization, if that makes any sense.

Lisa Young: Sure. And it increases in my mind this ecosystem view, right? We're not just part of one ecosystem but we're part of one, and our suppliers are part of one, and then there's a whole value chain down the line. So thank you for that, John.

Alright. So Edna, back to you then. John brought up critical infrastructure organizations. Are there any most important or practices, important practices for critical infrastructure organizations when it comes to countering these types of threat that you mentioned?

Edna Conway: It's a great question but it's a dangerous question and here's why. I think you want to always take a risk-based approach, but the risk in saying, "This is the most important" anything, whenever you're talking about security, is one that I think we need to be mindful of. So for me, I think we have to always go back to, and John hit on it really, in order to deploy the right security in the right stage of the value chain at the right time, you need to partner with your enterprise.

So go to the electric industry for example, right? I mean, not so long ago NERC (North American Electric Reliability Corporation) asked for testimony because they were thinking about expanding the CIP (critical infrastructure protection) to address cybersecurity in the supply chain. And I was privileged to actually be part of that testimony and there were a number of unbelievably expert folks in the industry there. And what we all said to NERC was, "There's a host of requirements that are already out there," right?

“Let's not rewrite something," number one. "Let's fully appreciate that not everything needs to be done everywhere. And let's see if we can try and partner via either an architecture approach or an understanding of --" and I'll go back to the 11 domains and say, "Look, what are you doing?" I mean, one of those really is physical and environmental security. If you are a substation or a nuclear facility or a distribution house in the electric sector, you need to be thinking about that in a very different way than other members of critical infrastructure might think about it.

And so it's this ability to say, "Here's 5, 10, and for us 11 things that we think you need to think about." But we want to go to the woman who runs facility operations. And then we want to go to the gentleman who is dealing with the network. And then we want to go talk to the next partner who is dealing with the reality of, "Well, we have to have materials delivered on a regular basis. He's handling logistics."

And teaching them what to think about so they embed it in their processes, their people and their technology. That I think is the ticket to success for critical infrastructure, because you leverage the already robust existing operational practices and knowledge that are there, and you slip in security so that it feeds in as a fundamental element now that -- rather than bolting it on saying, "Okay, here's my checklist of five. Those are the most important. I'm good, I'm done."

Lisa Young: No, I like that approach.

Edna Conway: They could've picked a few things, right, that -- new things that only they would know in their operations.

Lisa Young: Sure. Because they're the eyes on the ground, they're the front line, and they know whether something's an operational issue or perhaps sabotage of some sort. So they can discern that right there as they're doing their regular work. So that's actually a great point. Thank you for that.

Alright. So then John, can I ask you the same question? Are there any important or most important practices or anything you'd like to say for critical infrastructure organizations when it comes to countering some of these threats?

John Haller: Well, I like what Edna said about taking advantage of capabilities and practices that your organization already does or already has, right? And, I mean, I'm thinking about the length between, for instance, in a given organization, usually the business continuity folks have already done some basic activities like BIAs (business impact analyses) and so forth where they would look at what third parties really support the mission or the services or business functions, right?

So anything you do with respect to third-party or service relationships should take advantage of existing capabilities like that, right? And then as far as specific practices, I mean, that's potentially a toughie. I mean, Lisa, you know from the work that we've done together and that our organization does together with resilience management that we frequently talk first about asset management, right? In other words, what are the assets?

And we look at it really broadly -- people, information technology and facilities. What are the assets that you really rely on in your organization to help you do whatever it is that you do, right? Because that should -- they're not all equal. They don't all support your organization in the same way. And that is -- at least we frequently look at that as a very fundamental practice that an organization should have to determine from a technology point of view, "Well, what technology do we really care about?" Can we really prioritize our concerns?

In the old days, asset management was more about making sure that stuff does not walk off. That was years ago, right? Now, I mean, it's important to know what you're protecting, right? And then I think in terms of, in terms of practices, I mean, I would look to some of those governance and maturity practices, I think. And what I mean is getting different silos in the organization to talk to one another and to understand that they play a role.

I mean, I've been -I've lost count of the number of times that someone has told me, "Well, procurement or acquisition, the people that actually buy the stuff, never listen to us, and they don't understand the actual risks when they go out and either buy technology or enter into certain relationships," right, service relationships or third-party relationships. I mean, it really is common. And the funny thing is we think, well, maybe small organizations don't have as much capability, or we're actually starting to look at like size and sophistication of organizations just based on demographics, right.

This is something you hear at all levels. I mean, you hear it from very large government organizations and you hear it from, very small organizations out in rural America that provide critical infrastructure services. It's really interesting. And you would think that in 2016 it might have evolved a little bit, but it hasn't necessarily, right. So some of that starting at the top and setting the tone and how you govern it is really important.

Lisa Young: Well, I like that too. And I think I heard both of you say that taking a risk-based approach also helps align the business concerns and the value chain.

Part 3: Useful Sources to Consult

Lisa Young: So Edna, back to you then. Can I ask, thinking about what we've talked about today, aligning the mission, the business concerns, the value chain, are there standards or industry efforts that our listeners can look to for some assistance in this space?

Edna Conway: I think there are a number of them. We probably can't go through all of them, but I think there are a core set, to be honest with you, that will really help. And particularly for information and communications technology, looking at ISO 20243, which is a recently adopted ISO standard that went in for approval from the Open Group trusted partner group.

And what we had was something that we came together as industry, as OEMs, as acquirers, and said, "What could we do that would articulate something meaningfully about development practices, secure engineering practices and supply chain practices all in one compendium that gives people at least a checklist of what you ought to be considering and gives them flexibility on some of those practices to be able to deploy them in a manner that best fits their environment?"

You know about NIST's Cybersecurity Framework. It's very comprehensive. A bit daunting for smaller organizations, but there are mappings too, for example, the Open Group trusted technology partner standard or provider standard. And what we really have done is try to look at some of the other things that are out there like NIST best practices and cyber supply chain risk management, which also leverages information that are information that's located in other standards.

I'm going to take a deviation for a minute. I think there are some voluntary programs that a lot of people have forgotten about that don't necessarily look like they're related but there's a lot going on, on customs trade partnerships to focus on terrorism. And ironically enough, some of the best standards and practices are articulated in those programs.

Now, they're regional. So the U.S. has one. It's C-TPAT (Customs Trade Partnership Against Terrorism). The European Union has one. They call theirs the AEO, I think, Authorized Economic Operator. Mexico just came up with one. It's all in Spanish, and forgive me, that's not my first language, but it's basically a new program of certified companies is the translation. It's NEEC. Even Canada has one called Partners in Protection. You might say, "Well, why are we talking about customs and trade?"

Again, look at some of the things that are listed there as best practices that voluntarily are adhered to by members of the industry communities to meet those standards. And you will learn that there's a vast array of things that can help you. And the last thing I think I would point out is don't miss out on some of the benefit in NIST Special Pub 800-161 on Supply Chain Risk Management as well.

Lisa Young: Okay. Great. And for our listeners, we will have those references in the show notes. So thank you for that. And I like the idea of the voluntary programs because, most of the time we have enough regulation to comply with. So it's nice that folks see the importance of this and choose to follow some of these practices.

John, anything from you on standards or industry efforts that you'd like to point out here to our listeners?

John Haller: Well, I think Edna certainly hit a lot of them. And frankly, before this conversation I was really unaware of the customs and trade partnership stuff. I think the NIST CSF -- it does look a little daunting at first, but it is really valuable as a way for organizations to understand their capability and to be able to communicate with one another and with their leadership about cybersecurity.

I would just mention that we are actually on Version 3 now of the DHS Cyber Resilience Review (CRR). It's available on US CERT's website. I'm sure there's a link that will be posted in the show notes. But Version 3 will -- you take the questions, there's lots of guidance in there to help organizations, and it automatically builds out a picture against the NIST Cybersecurity Framework.

Lisa Young: I think we all know, there's a plethora of standards, guidelines and things, and it's nice to be able to have those at your disposal and pick and choose the ones that meet the business concerns for the value chain.

All right. So Edna, any further thoughts on the subject you'd like to share with our listeners before we close today?

Edna Conway: I think the only thing I'd add is that, we're in this together and this is a time where quite frankly the concept of what I like to call pervasive security in the new digital economy is something that requires all of us to sit down, take our competitive hats off for a moment and work on it to raise the bar as an industry, and at the end of the day as a planet. So here's our chance to collaborate, to do good for all.

Lisa Young: Well, I can appreciate that. And actually, the theme this year for RSA was "Connect to Protect." So I think it just shows that we certainly are all in this together. So thank you, Edna. I appreciate you being here today. John, any final thoughts for our listeners before we close up shop today?

John Haller: No. I mean, I think the theme that I hear and that we strongly espouse is it's an ecosystem, right? It's an ecosystem of good things within your organization and it's also an ecosystem of third-party relationships. And relationships with business partners, suppliers, and as Edna highlighted, we're all in it together. So we hope to add value, add value to critical infrastructure, and help organizations understand how they do in this regard. So other than that, that's about it.

Lisa Young: All right. Well, Edna and John, I can't thank you enough, both of you, for being here today. Edna we welcome, and we're so happy to have had you. And John, thank you for returning to my podcast series. Thank you both very much.

John Haller: Sure.

Lisa Young: My pleasure.